FOLIO 1

BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ORDINARIA 50/2018
DEL 23 DE NOVIEMBRE DE 2018

En la Ciudad de México, a las doce horas con treinta minutos del veintitrés de noviembre de dos mil dieciocho, en el edificio ubicado en avenida Cinco de Mayo, número seis, colonia Centro, delegación Cuauhtémoc, se reunieron Erik Mauricio Sánchez Medina, Director Jurídico, Víctor Manuel De La Luz Puebla, Director de Seguridad y Organización de la Información, y Carlos Eduardo Cicero Lebrija, Gerente de Gestión de Transparencia, suplente del Titular de la Unidad de Transparencia, todos integrantes del Comité de Transparencia de este Instituto Central, así como Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, en su carácter de Secretario de dicho órgano colegiado. ----------

También estuvieron presentes, como invitados de este Comité, en términos de los artículos 4o. y 31, fracción XIV, del Reglamento Interior del Banco de México, así como la Tercera, de las Reglas de Operación del Comité de Transparencia del Banco de México, publicadas en el Diario Oficial de la Federación el dos de junio de dos mil dieciséis, las personas que se indican en la lista de asistencia que se adjunta a la presente como **ANEXO "A"**, quienes también son servidores públicos del Banco de México. ----------

Erik Mauricio Sánchez Medina, quien preside dicho órgano colegiado, en términos del artículo 4o. del Reglamento Interior del Banco de México, y Quinta, de las Reglas de Operación del Comité de Transparencia del Banco de México, publicadas en el Diario Oficial de la Federación el dos de junio de dos mil dieciséis, solicitó al Secretario verificara si existía quórum para la sesión. Al estar presentes los integrantes mencionados, el Secretario manifestó que existe quórum para la celebración de dicha sesión, de conformidad con lo previsto en los artículos 43 de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos segundo y tercero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 83 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 4o. del Reglamento Interior del Banco de México; así como Quinta y Sexta, de las Reglas de Operación del Comité de Transparencia del Banco de México, publicadas en el Diario Oficial de la Federación el dos de junio de dos mil dieciséis. Por lo anterior, se procedió en los términos siguientes: ----------

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

El Secretario del Comité 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 4o. y 31, fracción XIV, del Reglamento Interior del Banco de México; 43, párrafo segundo, y 44, fracción IX, de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafo segundo, y 65, fracción IX, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como la Quinta, de las Reglas de Operación del Comité de Transparencia del Banco de México, aprobó por unanimidad el orden del día en los términos del documento que se adjunta a la presente como **ANEXO "B"** y procedió a su desahogo, conforme a lo siguiente:

PRIMERO. SOLICITUD DE CONFIRMACIÓN DE CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN; LA DIRECCIÓN DE SISTEMAS DE PAGOS; LA DIRECCIÓN DE OPERACIONES INTERNACIONALES, Y DE LA GERENCIA DE OPERACIONES NACIONALES, EN SUPLENCIA POR AUSENCIA DEL DIRECTOR DE OPERACIONES NACIONALES; Y POR EL GERENTE DE GESTIÓN DE LA DIRECCIÓN GENERAL DE EMISIÓN, EN SUPLENCIA POR AUSENCIA DE LA DIRECTORA DE ADMINISTRACIÓN DE EMISIÓN, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000057718.----------

El Secretario dio lectura al oficio con referencia DGTI-267/2018, suscrito por el titular de la Dirección General de Tecnologías de la Información; al oficio con referencia D01/C388/2018, suscrito por el titular de la Dirección de Sistemas de Pagos; al oficio de dieciséis de noviembre de dos mil dieciocho, suscrito por los titulares de la Dirección de Operaciones Internacionales, y de la Gerencia de Operaciones Nacionales, en suplencia por ausencia del Director de Operaciones Nacionales; y al oficio de dieciséis de noviembre de dos mil dieciocho,

BANCO DE MÉXICO

suscrito por el Gerente de Gestión de la Dirección General de Emisión, en suplencia por ausencia de la Directora de Administración de Emisión, los cuales se agregan en un solo legajo a la presente acta como **ANEXO "C"**, por medio de los cuales hicieron del conocimiento de este Comité de Transparencia la determinación de clasificar como confidencial y como reservada diversa información que se indica en dichos oficios, en términos de la motivación y fundamentación señaladas en dichos documentos, así como en las correspondientes pruebas de daño, y solicitaron a este órgano colegiado confirmar dicha clasificación. --------
Después de un amplio intercambio de opiniones, se resolvió lo siguiente:----------
Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43 y 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 9, 64 y 65 fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Quinta de las Reglas de Operación del Comité de Transparencia, vigentes, resolvió confirmar la clasificación de la información realizada por las unidades administrativas citadas, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "D"**. ----------

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE SISTEMAS DE PAGOS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000057918.----------

El Secretario dio lectura al oficio con referencia D01/C387/2018, suscrito por el titular de la Dirección de Sistemas de Pagos, el cual se agrega a la presente acta como **ANEXO "E"**, por medio del cual hizo del conocimiento de este Comité de Transparencia su determinación de clasificar como reservada la información que se indica en dicho oficio, en términos de la motivación y fundamentación señaladas en dicho oficio, así como en la correspondiente prueba de daño, y solicitó a este órgano colegiado confirmar dicha clasificación.
Después de un amplio intercambio de opiniones, se resolvió lo siguiente:----------
Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43 y 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 9, 64 y 65 fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Quinta de las Reglas de Operación del Comité de Transparencia, vigentes, resolvió confirmar la clasificación de la información realizada por la unidad administrativa citada, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "F"**. ----------

TERCERO. SOLICITUD DE CONFIRMACIÓN DE CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA DIRECCIÓN DE REGULACIÓN Y SUPERVISIÓN Y DE LA DIRECCIÓN DE SISTEMAS DE PAGOS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000060218.----------

El Secretario dio lectura al oficio de quince de noviembre de dos mil dieciocho, suscrito por los titulares de la Dirección de Regulación y Supervisión, y de la Dirección de Sistemas de Pagos, el cual se agrega a la presente acta como **ANEXO "G"**, por medio del cual hicieron del conocimiento de este Comité de Transparencia su determinación de clasificar como reservada la información que se indica en dicho oficio, en términos de la motivación y fundamentación señaladas en dicho oficio, así como en la correspondiente prueba de daño, y solicitaron a este órgano colegiado confirmar dicha clasificación. ----------
Después de un amplio intercambio de opiniones, se resolvió lo siguiente:----------
Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43 y 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 9, 64 y 65 fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Quinta de las Reglas de Operación del Comité de Transparencia, vigentes, resolvió confirmar la clasificación de la información realizada por las unidades administrativas citadas, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "H"**. ----------

CUARTO. SOLICITUD DE CONFIRMACIÓN DE CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA SUBGERENCIA DE GESTIÓN DE OBLIGACIONES DE TRANSPARENCIA Y SOLICITUDES DE

BANCO DE MÉXICO

INFORMACIÓN Y DE LA SUBGERENCIA DE ANÁLISIS JURÍDICO Y PROMOCIÓN DE TRANSPARENCIA, Y APROBACIÓN DE UNA VERSIÓN PÚBLICA, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000062118. ----------

El Secretario dio lectura al oficio de catorce de noviembre de dos mil dieciocho, suscrito por los titulares de la Subgerencia de Gestión de Obligaciones de Transparencia y Solicitudes de Información, y de la Subgerencia de Análisis Jurídico y Promoción de Transparencia, el cual se agrega a la presente acta como **ANEXO "I"**, por medio del cual hicieron del conocimiento de este Comité de Transparencia su determinación de clasificar como reservada diversa información contenida en el documento señalado en dicho oficio, en términos de la motivación y fundamentación señaladas en la correspondiente prueba de daño, y solicitaron a este órgano colegiado confirmar dicha clasificación y aprobar la versión pública respectiva, en sus términos. ----------

Después de un amplio intercambio de opiniones, se resolvió lo siguiente:----------

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43 y 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 9, 64 y 65 fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Quinta de las Reglas de Operación del Comité de Transparencia, vigentes, resolvió confirmar la clasificación de la información realizada por las unidades administrativas citadas y aprobar la versión pública respectiva, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "J"**.----------

Al no haber más asuntos que tratar, se dio por terminada la sesión, en la misma fecha y lugar de su celebración. La presente acta se firma por los integrantes presentes del Comité de Transparencia, así como por su Secretario. Conste.----------

COMITÉ DE TRANSPARENCIA

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

CARLOS EDUARDO CICERO LEBRIJA
Integrante Suplente

RODRIGO VILLA COLLINS
Secretario

ANEXO "A"

BANCO DE MÉXICO

LISTA DE ASISTENCIA

SESIÓN ORDINARIA 50/2018

23 DE NOVIEMBRE DE 2018

COMITÉ DE TRANSPARENCIA

JUAN MANUEL SÁNCHEZ RAMÍREZ Titular de la Unidad de Transparencia	
ERIK MAURICIO SÁNCHEZ MEDINA Director Jurídico	
VICTOR MANUEL DE LA LUZ PUEBLA Director de Seguridad y Organización de la Información	
JOSÉ RAMÓN RODRÍGUEZ MANCILLA Gerente de Organización de la Información	
ENRIQUE ALCÁNTAR MENDOZA Abogado Especialista nivel Gerente	
CARLOS EDUARDO CICERO LEBRIJA Gerente de Gestión de Transparencia	
RODRIGO VILLA COLLINS Secretario del Comité de Transparencia	

INVITADOS PERMANENTES

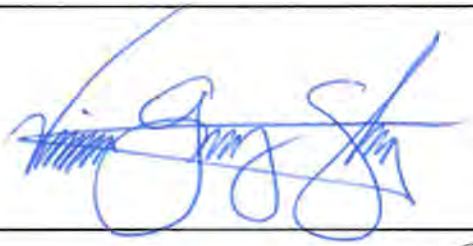
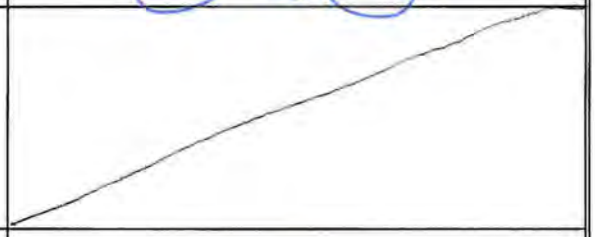
OSCAR JORGE DURÁN DÍAZ Dirección de Vinculación Institucional y Comunicación	
FRANCISCO CHAMÚ MORALES Director de Administración de Riesgos	

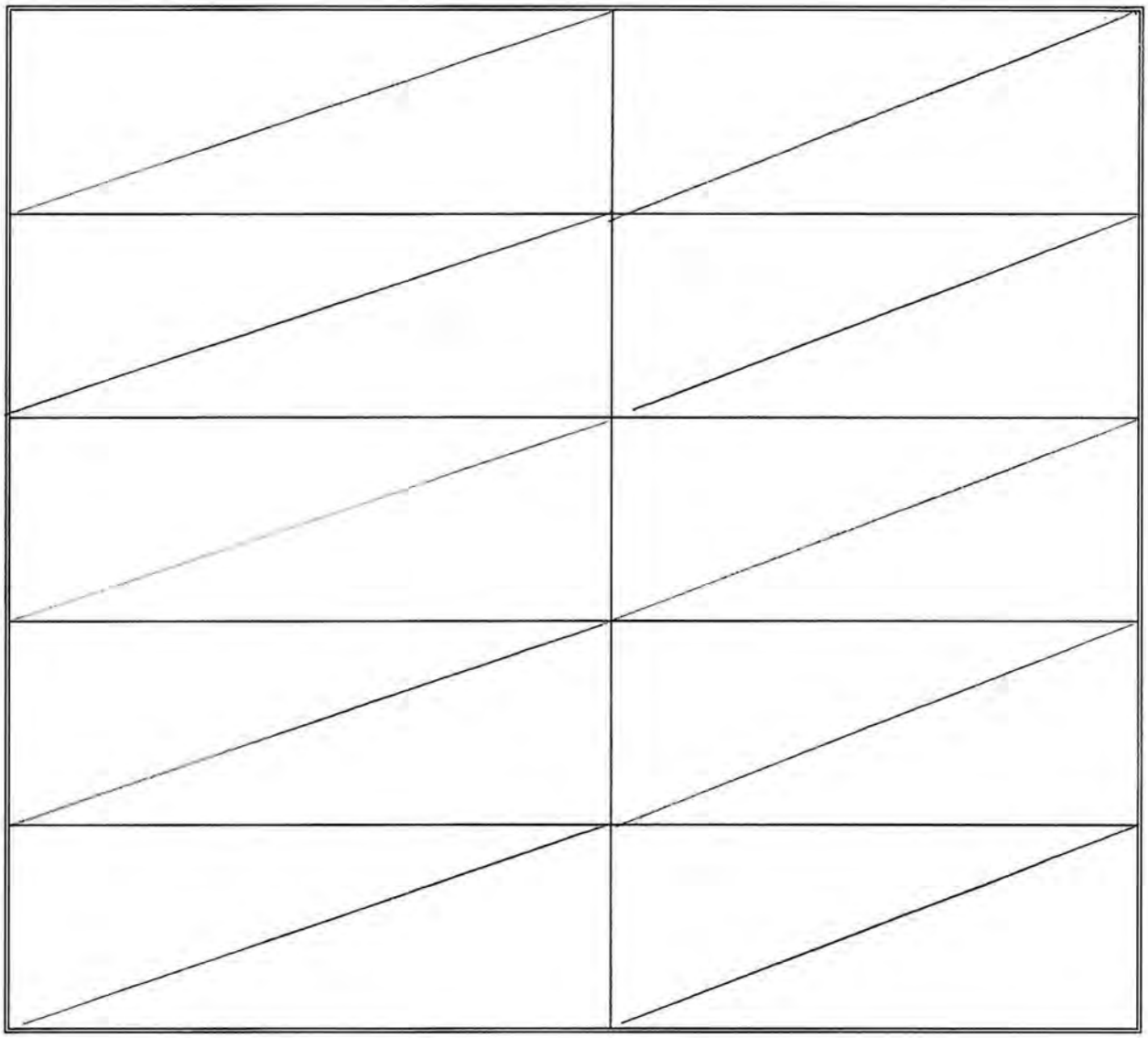
INVITADOS

RODRIGO MÉNDEZ PRECIADO Gerente de Enlace Institucional y Relaciones Públicas	
EDGAR MIGUEL SALAS ORTEGA Gerente Jurídico Consultivo	
JONATHAN NAVARRO VILLEGAS Abogado en Jefe en la Subgerencia de Apoyo Jurídico a la Transparencia	

MARGARITA LISSETE PONCE GUARNEROS Gerente de Riesgos No Financieros	
MIRNA ESPERANZA CORTÉS CAMPOS Directora de Administración de Emisión	
CARLOS GUTIÉRREZ CAPPELLO Gerente de Gestión de la Dirección General de Emisión	En medios de comunicación (Videoconferencia)
GERARDO ISRAEL GARCÍA LÓPEZ Director de Operaciones Internacionales	
JUAN RAFAEL GARCÍA PADILLA Director de Operaciones Nacionales	
MAYTE RICO FERNÁNDEZ Gerente de Operaciones Nacionales	
CLAUDIA TAPIA RANGEL Especialista Investigadora	

MARTÍN CAMPOS FERNÁNDEZ Analista de Información	
MIGUEL ÁNGEL DÍAZ DÍAZ MANUEL Director de Sistemas de Pagos	
OTHÓN MARTINO MORENO GONZÁLEZ Gerente de Política y Vigilancia de los Sistemas de Pagos	
LILIANA GARCÍA OCHOA Líder de Especialidad	
XIMENA AIDEE DOMÍNGUEZ HERNÁNDEZ Investigadora	
OCTAVIO BERGÉS BASTIDA Director General de Tecnologías de la Información	
ALICIA ADRIANA AYALA ROMERO Subgerente de Planeación y Regulación	

RICARDO ALFREDO GONZÁLEZ FRAGOSO Líder de Especialidad	
VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión	
RICARDO GARCÍA BENÍTEZ Estudios y Proyectos Especiales	
JORGE ERIK QUIROZ ROBLES Analista de Estudios y Proyectos Especiales	
ELIZABETH CASILLAS TREJO Subgerente de Gestión de Obligaciones de Transparencia y Solicitudes de Información	
SERGIO ZAMBRANO HERRERA Subgerente de Análisis Jurídico y Promoción de Transparencia	
HÉCTOR GARCÍA MONDRAGÓN Jefe de la Oficina de Análisis Jurídico y Promoción de Transparencia	



ANEXO "B"

BANCO DE MÉXICO

Comité de Transparencia

ORDEN DEL DÍA
Sesión Ordinaria 50/2018
23 de noviembre de 2018

PRIMERO. SOLICITUD DE CONFIRMACIÓN DE CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN; LA DIRECCIÓN DE SISTEMAS DE PAGOS; LA DIRECCIÓN DE OPERACIONES INTERNACIONALES, Y DE LA GERENCIA DE OPERACIONES NACIONALES, EN SUPLENCIA POR AUSENCIA DEL DIRECTOR DE OPERACIONES NACIONALES; Y POR EL GERENTE DE GESTIÓN DE LA DIRECCIÓN GENERAL DE EMISIÓN, EN SUPLENCIA POR AUSENCIA DE LA DIRECTORA DE ADMINISTRACIÓN DE EMISIÓN, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000057718.

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE SISTEMAS DE PAGOS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000057918.

TERCERO. SOLICITUD DE CONFIRMACIÓN DE CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA DIRECCIÓN DE REGULACIÓN Y SUPERVISIÓN Y DE LA DIRECCIÓN DE SISTEMAS DE PAGOS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000060218.

CUARTO. SOLICITUD DE CONFIRMACIÓN DE CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA SUBGERENCIA DE GESTIÓN DE OBLIGACIONES DE TRANSPARENCIA Y SOLICITUDES DE INFORMACIÓN Y DE LA SUBGERENCIA DE ANÁLISIS JURÍDICO Y PROMOCIÓN DE TRANSPARENCIA, Y APROBACIÓN DE UNA VERSIÓN PÚBLICA, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000062118.

ANEXO "C"

BANCO DE MÉXICO

Ciudad de México, a 31 de octubre de 2018

REF: DGTI-267/2018

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Me refiero a la solicitud de acceso a la información, identificada con el número de folio **6110000057718**, que nos turnó la Unidad de Transparencia el 16 de octubre de 2018, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

> *"Necesito de todos los servidores públicos los registros de las llamas recibidas y realizadas del mes de septiembre a la fecha, y en caso de grabarlas las de las última semana a la fecha de la presentación de esta solicitud, desde luego de linea oficial asignada."*

Al respecto, me permito hacer de su conocimiento que esta unidad administrativa **ha clasificado como confidencial la información en posesión del Banco de México relativa a los números telefónicos de las llamadas entrantes y salientes de los servidores públicos del Banco de México**, en razón de lo siguiente:

1. Al amparo de lo dispuesto por el artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos, el Banco de México, como todas las demás autoridades, tiene la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad.

   Entre los derechos humanos que reconoce la misma Constitución Política, esta establece, en el artículo 16, segundo párrafo, que toda persona tiene derecho a la protección de sus datos personales en los términos que fije la ley. En el mismo sentido, el artículo 6o., apartado A, de la propia Constitución Política, relativo al derecho de acceso a la información, señala en su fracción II que la información que se refiere a la vida privada y a los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

2. Por su parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece en su artículo 3, fracción IX, lo siguiente:

   "IX. Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información".

3. En este sentido, el número de teléfono ya sea fijo o celular se encuentra asignado a una persona determinada, la cual contrata la prestación de servicios de telecomunicaciones para poder ser localizado a través de diversos aparatos de telecomunicación.

   En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal.

En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar vía telefónica a su titular.

4. Por otro lado, si bien en el registro de llamadas se encuentran incluidos números telefónicos de dependencias públicas o proveedores del Banco de México, los cuales serían de carácter público, no se puede tener la certeza que el total de las llamadas recibidas y realizadas correspondan a este tipo de números, y al no haber modo de distinguir dentro de los registros de llamadas los números telefónicos de personas físicas de los números telefónicos de personas morales, atendiendo al principio "pro persona" esta unidad administrativa ha decidido clasificar como confidencial todos los números telefónicos de llamadas entrantes y salientes de los servidores públicos del Banco de México.

5. Adicionalmente, en términos de los artículos 120 de la Ley General de Transparencia y Acceso a la Información Pública y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública, no se actualiza ninguno de los supuestos previstos en la Ley para permitir el acceso a la información confidencial materia de la solicitud, en razón de que:

   a. No se cuenta con el consentimiento expreso y por escrito de los titulares de los datos personales para permitir el acceso a la información, en términos de los artículos 120, primer párrafo, de la Ley General de Transparencia y Acceso a la Información Pública y 117, primer párrafo, de la Ley Federal de Transparencia y Acceso a la Información Pública.

      En tal sentido, tampoco se actualiza ninguno de los supuestos previstos en el artículo 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados para tratar, en su modalidad de difusión, los datos personales de los números telefónicos de las llamadas entrantes y salientes de los servidores públicos del Banco de México, puesto que:

      i. No existe una ley así lo disponga.
      ii. La transferencia requerida no se realiza entre responsables.
      iii. No existe una orden judicial, resolución o mandato fundado y motivado de autoridad competente.
      iv. No se actualizan ni se demostraron los supuestos de reconocimiento o defensa de derechos del titular ante autoridad competente, puesto que no lo solicita el titular de los datos personales.
      v. Los datos personales solicitados no fueron requeridos para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable, ni, en caso de existir, se demostró dicha circunstancia.
      vi. No existe o no se demostró una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.
      vii. Los datos personales solicitados no son necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria y, en caso de que así fuera, no se demostró.
      viii. Los datos personales solicitados no figuran en fuentes de acceso público.

ix. Los titulares de los datos personales no son personas reportadas como desaparecidas en los términos de la ley en la materia, o no se demostró ante el Banco de México tal circunstancia.

b. La información solicitada no se encuentra en registros públicos o fuentes de acceso público, en términos de los artículos 120, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública y 117, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública.

c. La información solicitada no tiene, por ley, el carácter de pública, en términos de los artículos 120, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública y 117, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública.

d. No existe una orden judicial, en términos de los artículos 120, fracción III, de la Ley General de Transparencia y Acceso a la Información Pública y 117, fracción III, de la Ley Federal de Transparencia y Acceso a la Información Pública.

e. No existen razones de seguridad nacional y salubridad general, o de protección de derechos de terceros, que requieran de su publicación, en términos de los artículos 120, fracción IV, de la Ley General de Transparencia y Acceso a la Información Pública y 117, fracción IV, de la Ley Federal de Transparencia y Acceso a la Información Pública.

f. El peticionario no demostró ante el Banco de México su la calidad de sujeto obligado o sujeto de derecho internacional, de conformidad con los tratados y los acuerdos interinstitucionales, en términos de los artículos 120, fracción V, de la Ley General de Transparencia y Acceso a la Información Pública y 117, fracción V, de la Ley Federal de Transparencia y Acceso a la Información Pública.

6. Como consecuencia de lo anterior, no es posible divulgar los números telefónicos de donde provienen o a donde se dirigen las llamadas realizadas por los servidores públicos del Banco de México, puesto que la revelación de dicha información haría nugatoria la protección del dato personal confidencial referido.

7. En otro orden de ideas, de conformidad con el Décimo de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, informamos que el personal que por la naturaleza de sus atribuciones tiene acceso a la información clasificada, es el siguiente:

   - Gerencia de Telecomunicaciones (Gerente)
   - Subgerencia de Desarrollo de Servicios de Telecomunicaciones (Subgerente)
   - Subgerencia de Operación de Servicios de Telecomunicaciones (Subgerente)
   - Oficina de Operación de Comunicaciones Unificadas (jefe)
   - Oficina de Soporte a la Gestión Presupuestal (jefe)

   Por lo expuesto, en términos de los artículos 44, fracción II, 137, párrafo segundo, de la Ley General de Transparencia y Acceso a la información Pública; 65, fracción II, 140, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México; así como en el Vigésimo quinto de los

"Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", vigentes, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de la información aludida en el presente oficio.

Atentamente

ING. OCTAVIO BERGÉS BASTIDA
Director General de Tecnologías de la Información

BANCO DE MÉXICO

Ciudad de México, a 16 de noviembre de 2018
D01/C388/2018

COMITÉ DE TRANSPARENCIA
DEL BANCO DE MÉXICO
Presente

Nos referimos a la solicitud de acceso a la información, identificada con el número de folio **6110000057718,** de la cual se tuvo conocimiento el dieciséis de octubre del presente año, , la cual se transcribe a continuación:

> *"Necesito de todos los servidores públicos los registros de las llamas recibidas y realizadas del mes de septiembre a la fecha, y en caso de grabarlas las de las última semana a la fecha de la presentación de esta solicitud, desde luego de linea oficial asignada."*

Sobre el particular, me permito informarles que esta unidad administrativa, de conformidad con los artículos 100 y 106, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública; así como 97 y 98, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, ha determinado clasificar como reservado la ***información relacionada con los registros y grabaciones de llamadas realizadas y recibidas que soportan el funcionamiento de los sistemas de pagos,*** de conformidad con la fundamentación y motivación señaladas en la prueba de daño que se adjunta al presente.

Por lo expuesto, en términos de los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 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.

BANCO DE MÉXICO

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informo que el personal que por la naturaleza de sus atribuciones tiene acceso al referido documento clasificado es: Director, Gerentes, Subgerentes y demás personal adscrito a la Dirección de Sistemas de Pagos

Atentamente,

MANUEL MIGUEL ÁNGEL DÍAZ DÍAZ
Director de Sistemas de Pagos

BANCO DE MÉXICO
RECIBIDO
1 E MAY 2018
Comité de Transparencia
Por: BI2317 Hora: 13:51
Recibo el oficio y 4 dos páginas y una prueba de daño.

BANCO DE MÉXICO

PRUEBA DE DAÑO

GRABACIÓN DE LLAMADAS DE LA DIRECCIÓN GENERAL DE OPERACIONES Y SISTEMAS DE PAGOS

En términos de lo dispuesto en los artículos 6, apartado A, sexto párrafo, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 113, fracción IV, de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP); 110, fracción IV, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como Vigésimo segundo, fracciones I y II, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas (Lineamientos), es de clasificarse como información reservada aquella que:

- Menoscabe la efectividad de las medidas implementadas en los sistemas financiero o económico del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto;

- Ponga en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país;

- Comprometa las acciones encaminadas a proveer el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos; y

Se debe señalar que las Direcciones de Operaciones Nacionales, de Operaciones Internacionales y, de Sistemas de Pagos, tienen entre sus atribuciones las de concertar y formalizar las operaciones del Banco relacionadas con divisas, oro, plata y valores referidos a monedas extranjeras, así como las garantías vinculadas con dichas operaciones; concertar y formalizar las operaciones financieras del Banco relacionadas con moneda nacional, divisas frente a dicha moneda y valores referidos a la moneda nacional, así como las garantías vinculadas con dichas operaciones; así como concertar, ejecutar y dar seguimiento a las operaciones de los participantes en los Sistemas de Pagos administrados por el Banco respectivamente; es en el ejercicio de estas atribuciones que se graban las extensiones del personal a cargo de éstas sin distinguir si la llamada es privada o pública.

En este sentido, el dar a conocer el detalle de las llamadas del personal encargado del **análisis e instrumentación de las operaciones con propósitos de regulación monetaria**, representa un riesgo de perjuicio significativo al interés público en virtud de que dicho riesgo es:

1) **Real** ya que a través de llamadas telefónicas se intercambia información, opiniones, puntos de vista y percepciones de los participantes del sistema financiero sobre el comportamiento y condiciones de liquidez del mercado de dinero y de quienes en el intervienen, lo cual fuera de contexto, podría conducir a una lectura equivocada sobre la solidez de las instituciones

financieras que celebran operaciones de inyección de liquidez con este Instituto Central al entenderse, erróneamente, que dichas instituciones tienen problemas de liquidez lo que podría disminuir la confianza del público en éstas y por lo tanto generar un menor interés de las mismas en participar en las subastas de regulación monetaria y cualquier otro mecanismo implementado por el Banco de México en materia monetaria, lo que afectaría directamente la implementación de estas medidas.

2) **Demostrable** ya que existe gran sensibilidad tanto de inversionistas como del público en general a este tipo de información (la solvencia de las instituciones financieras) por lo que ante una incorrecta interpretación de la misma, los depositantes podrían cambiar sus inversiones de institución de crédito e incluso de país, generando con ello corridas financieras que perjudiquen a la institución de crédito en cuestión. Baste recordar la rapidez con la que es perdió la confianza en las instituciones financiera durante la crisis global que inició en 2007 en donde varios bancos alrededor del mundo presentaron corridas bancarias, entre ellos el banco británico Northern Rock[1].

3) **Identificable** ya que la pérdida de confianza en las instituciones de crédito puede afectar también a aquellas consideradas sistémicamente importantes, lo que incluso podría poner en riesgo el sano desarrollo del sistema financiero y la estabilidad financiera nacional en su conjunto. En efecto, durante la crisis financiera global de 2008, la quiebra del Banco Lehman Brothers generó una desconfianza masiva en el sistema financiero estadounidense que forzó a las autoridades financieras de dicho país a "nacionalizar" a los bancos considerados sistémicamente importantes para restaurar la confianza y mantener la estabilidad de dicho sistema.[2]

En el mismo contexto de las llamadas que se realizan para instrumentar la política monetaria, se encuentran las llamadas que se realizan para **instrumentar la política cambiaria.**

El Banco de México instrumenta la política cambiaria siguiendo las directrices que determina la Comisión de Cambios, integrada por Banco de México y la Secretaría de Hacienda y Crédito Público. Dicha Comisión mantiene una constante evaluación de los distintos factores económicos, políticos y sociales del país, así como de los fundamentos macroeconómicos, de los indicadores económicos y en particular de las condiciones de operación en el mercado cambiario nacional y de los mercados financieros globales para tomar sus decisiones.

---

[1] The Bank that failed, The economist, sep 20th 2007. https://www.economist.com/node/9832838 Consultado el 15 de noviembre

[2] Wall Street humiliated by nationalisation of banks, Independent, oct 14th 2008. https://www.independent.co.uk/news/business/news/wall-street-humiliated-by-nationalisation-of-banks-961397.html Consultado el 15 de noviembre

El dar a conocer el detalle de las llamadas del personal encargado del análisis e instrumentación de las operaciones cambiarias, representa un riesgo de perjuicio significativo al interés público en virtud de que dicho riesgo es:

1) **Real**, ya que a través de llamadas telefónicas se intercambia información, opiniones, puntos de vista y percepciones de los participantes en el mercado cambiario sobre el comportamiento y condiciones de liquidez de éste y de quienes en el intervienen, lo cual fuera de contexto podría generar percepciones erróneas en el público y propiciar que los agentes económicos o incluso las instituciones financieras tomen decisiones e implementen medidas inconvenientes para el mercado que redunden en un daño para la economía nacional y que, por otra parte y de manera fundamental, puedan afectar la efectividad de la medida en el futuro.

   Es importante destacar que en la práctica internacional la puesta a disposición del público de información y documentos relativos a las operaciones realizadas por los bancos centrales en el mercado cambiario atiende al objetivo que se busque con la propia intervención y al mensaje que los bancos centrales buscan dar a los participantes y al mercado cambiario en general. En ese sentido, la clasificación, o en su caso, la divulgación de información relativa a las operaciones efectuadas puede variar según los objetivos específicos.

   En ese sentido, la Comisión de Cambios está en posibilidad de implementar operaciones, cuya información sea clasificada, o en su caso, divulgada en el mercado cambiario, de manera acorde con la práctica internacional, a fin de lograr objetivos como corregir desalineamientos en el tipo de cambio, ordenar al mercado cambiario, acumular reservas internacionales, o bien, proveer al mercado de moneda extranjera, y que, tienen como fin último procurar la estabilidad del poder adquisitivo de la moneda nacional.

   Por tal motivo, al dar a conocer las grabaciones del personal que instrumenta éstas operaciones se pueden conocer detalles como el tipo de operación que se realizó, el nombre de las instituciones que están facultadas para operar con el Banco, cuánto puede comprar cada una, en donde residen, así como información que permita la identificación de tales operaciones, afectando de manera significativa las funciones propias de la Comisión de Cambios y del Banco Central y, disminuyendo la capacidad de éste para cumplir su finalidad constitucional de procurar la estabilidad de la moneda nacional. Lo anterior, con las correspondientes consecuencias negativas para el mercado cambiario y para la economía en general de nuestro país.

   Actualmente, a nivel internacional se reconoce como una práctica bancaria la discrecionalidad por parte de los bancos centrales para realizar operaciones en el mercado

cambiario y para determinar la clasificación, o en su caso, la divulgación de la información relativa a las operaciones que en esta materia realiza, así como diversos aspectos de las mismas. Adicionalmente, se reconoce que no obstante que los bancos centrales informen sobre sus operaciones en el mercado ello no significa que deban revelar sus estrategias de mercado u otra información que pueda generar oportunidades para que los participantes obtengan ganancias sin riesgo y que puedan utilizar en su beneficio, pudiendo perjudicar la eficacia de las medidas que en el futuro los bancos centrales requieran adoptar en materia cambiaria.

En ese mismo sentido, diversos autores que han abordado el tema de la divulgación al público de los detalles de las operaciones realizadas por los bancos centrales en el mercado cambiario, señalan que existen razones en virtud de la propia operación del mercado cambiario que justifican que el público no tenga conocimiento respecto de todos los detalles de las operaciones cambiarias realizadas por los bancos centrales. Una de las principales razones que señalan tales autores es la situación estratégica que los bancos centrales tienen dentro de las economías de sus respectivos países, reconociendo que existen algunas operaciones que no son susceptibles de divulgarse al público.

En línea con la práctica bancaria a nivel internacional, la Comisión de Cambios, a través de Banco de México, ha hecho del conocimiento del público información sobre las operaciones realizadas en el mercado cambiario mediante la publicación de comunicados de prensa o reportes financieros, en determinadas ocasiones que así lo ameritan, para conseguir objetivos de política cambiaria, o bien, en los informes anuales del Banco Central.

En ese sentido, publicar las grabaciones de las llamadas que realiza el personal que instrumenta las operaciones cambiarias implica obligar al Banco Central a actuar de manera contraria a la práctica bancaria internacional con los consecuentes efectos negativos que ello podría generar al propio Banco Central, a los mecanismos de intervención cambiaria, y finalmente, de manera preponderante, al valor adquisitivo de la moneda, obligación constitucional a la que esta Institución debe dar cabal cumplimiento.

2) **Demostrable**, pues considerando las circunstancias propias de nuestro país, el grado de cultura en materia económica y financiera, la influencia de los medios de comunicación, los diferentes intereses económicos, políticos y sociales involucrados, así como el grado de desarrollo de nuestro sistema financiero, reprivatizado hace pocas décadas y cuya composición, aunque ha evolucionado, es muy similar a través de los años, junto con otros factores, la Comisión de Cambios ha determinado no divulgar los detalles de las operaciones cambiarias como los contenidos en las grabaciones que realiza el personal que las instrumenta, previendo los posibles daños que ello podría conllevar a la población mexicana en su conjunto.

Ejemplo de lo mencionado en el párrafo anterior es el estigma que se asocia a los participantes en las operaciones cambiarias. No es extraña la publicación de artículos periodísticos en los que se califica negativamente a instituciones financieras que participaron en operaciones cambiarias realizadas por este instituto central décadas antes. Como muestra podemos mencionar el artículo publicado el 18 de abril de 2008 en el periódico La Jornada titulado "México SA"[3] o el publicado el 27 de marzo de 2009 en el periódico El País titulado "La Crisis Mexicana ahora sí parece crisis"[4] que dan fe del daño que, incluso años después de realizada la operación cambiaria de compraventa de dólares de 1994, puede provocarse con la publicación de cierta información sensible sobre mecanismos de política cambiaria implementados por la Comisión de Cambios y contenida en las grabaciones del personal que instrumenta dichas operaciones.

Lo anterior podría generar que las instituciones perdieran interés en participar en las operaciones cambiarias, al saber que su nombre así como el detalle de sus operaciones y puntos de vista llegarían a ser públicos y considerando las afectaciones que ello pudiera acarrearles. Más aún, dicha perdida de interés tendría como consecuencia la disminución de efectividad de las medidas en materia cambiaria, con su consecuente afectación en el mercado cambiario y en uno de los mecanismos con que el Banco de México cuenta para dar cumplimiento a su objetivo constitucional prioritario de procurar la estabilidad del poder adquisitivo de la moneda nacional.

Por ello, la Comisión de Cambios, así como la Secretaría de Hacienda y el Banco Central, en lo individual deben asumir la responsabilidad de considerar los efectos económicos que la publicación de las grabaciones del personal que instrumenta las operaciones cambiarias puede conllevar, particularmente, la responsabilidad de evitar riesgos y efectos negativos que puedan perjudicar no solo a la política cambiaria, sino al sistema financiero y a la economía nacional en su conjunto. En ejercicio de tal responsabilidad tal organismo y autoridades están obligadas a determinar el tratamiento de la información que nos ocupa, por lo que divulgar las grabaciones del personal que instrumenta éstas operaciones puede afectar en gran medida el ejercicio de sus facultades y funciones.

Por lo expuesto anteriormente, el Banco Central, a fin de poder dar cumplimiento a su mandato constitucional, se encuentra impedido para dar a conocer los detalles respecto de las operaciones cambiarias, contenidas en las grabaciones del personal contratado para este

[3] De Fernández-Vega, Carlos. Consultado en: http://www.jornada.unam.mx/2008/04/18/index.php?section=economia&article=030o1eco, abril 2008. Consultado el 15 de noviembre

[4] De Herrera, Carlos. Consultado en: https://lacolumna.wordpress.com/2009/03/28/la-crisis-mexicana-ahora-si-parece-crisis-arturo-herrera/, febrero 2017. Consultado el 15 de noviembre

fin, tales como las instituciones participantes en las mismas, los montos que pudieran llegar a adquirir y cualquier otro dato que permita la identificación de las operaciones.

Lo anterior, toda vez que, como se mencionó, las operaciones en el mercado cambiario determinadas por la Comisión de Cambios, e implementadas por el Banco de México, tienen como propósito proveer liquidez y mejorar las condiciones de operación de la moneda nacional. Dado que alcanzar dicho objetivo no se establece de la misma forma en todas las ocasiones, al ser sólo un participante adicional dentro del mercado cambiario, el banco central debe determinar cuidadosamente el esquema operacional de intervención y las estrategias que logren influir efectivamente dentro de este mercado conformado por un grupo heterogéneo de participantes.

Algunos ejemplos de derecho comparado en dónde la propia regulación permite reserva respecto a la divulgación de información de las intervenciones cambiarias es el Código de buenas prácticas de transparencia en las políticas monetarias y financieras, declaración de principios, del Fondo Monetario Internacional, el cual reconoce, que hay circunstancias en las que no sería aconsejable que los bancos centrales revelaran sus tácticas de implementación de la política monetaria y cambiaria, así como tampoco que proporcionaran información detallada, como la contenida en las grabaciones del personal que instrumenta las operaciones en cuestión.

Moser-Boehm (2005), señala algunas de las razones por las que existen límites válidos para la transparencia en las operaciones cambiarias: la transparencia sobre el objetivo no necesita ser sinónimo de divulgación de la información de las herramientas y tácticas relacionadas. Por su parte, Holub (2005) apunta a una segunda razón: la divulgación de información al público sobre las operaciones en el mercado de divisas puede obstaculizar su efectividad, como lo es caso de información relacionada con las tácticas o estrategias seguidas por el Banco Central, como los montos operados, instituciones adquirentes y demás detalles de las operaciones. En este caso, con la divulgación de los contratos y convenios celebrados en la materia, se actualiza la premisa sobre la divulgación de tácticas o estrategia de política cambiara del banco central.

3) **Identificable**, toda vez que, si se revelan detalles de las grabaciones del personal que instrumenta las operaciones cambiarias como cuanto compró cada institución así como cuales instituciones están en el país y cuáles en el extranjero, se puede identificar el monto operado en el mercado local y el monto operado en otros mercados internacionales. Lo anterior puede afectar la efectividad de las medidas adoptadas en materia cambiaria e incrementar el costo de operaciones financieras del Banco debido a que el mercado puede predisponerse a este tipo de estrategias y contrarrestar las acciones del banco central de manera parcial o en su totalidad, nulificando los objetivos de la operación cambiaria.

En mayor detalle, si con la publicación de los contratos y convenios los participantes deducen el monto de divisa extranjera comprada o vendida en determinado mercado, en la siguiente operación del banco central en dicho mercado tratarán de probar a éste último obligándolo a vender una cantidad mayor de dólares conociendo de antemano el monto que estuvo dispuesto a vender anteriormente. Esto incrementa el costo de la operación porque el Banco Central tendrá que vender una mayor cantidad de dólares a precios mayores e incluso podría no lograr su objetivo de procurar mantener el valor adquisitivo de la moneda nacional como se mencionó con anterioridad.

Se debe notar que al decidir implementar cualquier operación de política cambiaria, la Comisión de Cambios da a conocer la información necesaria para que los agentes económicos estén en posibilidad de adoptar las medidas que estimen más convenientes y adecuadas para satisfacer sus necesidades de moneda extranjera, así como para mantener el funcionamiento ordenado del mercado cambiario y que se procure la preservación de fundamentos económicos sólidos.

Por tal motivo, la divulgación de las grabaciones del personal que instrumenta las operaciones cambiarias en los que se puede identificar información como el nombre de las instituciones que participan en las operaciones cambiarias así como otros detalles de las mismas, podría comprometer la competitividad, ejecución y la estrategia en materia cambiaria del Instituto Central y con ello afectar la utilidad de la medida o incluso eliminarla, lo que en adición a las posibles implicaciones negativas que antes se mencionaron, podría llegar a perjudicar a la economía en su conjunto y con ello al país y podría incrementar el costo de dichas operaciones en el futuro.

Al efecto, es menester considerar que las instituciones que participan en estas operaciones buscan satisfacer necesidades de moneda extranjera, las cuales responden a características particulares de su operación, balance y/o actividades con sus clientes, en un entorno específico del mercado cambiario nacional. En ese sentido, al dar publicidad a las grabaciones del personal que instrumenta éstas operaciones y por ende, revelar el nombre de las instituciones y el monto de dólares adquirido por cada una en las operaciones implementadas por la Comisión de Cambios, a través de Banco de México, se otorgaría una ventaja indebida a otras instituciones quienes podrían utilizar dicha información para establecer estrategias en su beneficio que afecten directamente a las instituciones adquirentes de dólares, generando incluso una minusvalía y con ello una afectación en el patrimonio de estas últimas.

Adicionalmente, al dar publicidad a la información que nos ocupa, se podrían generar señales erróneas al público en general sobre la solidez o debilidad de las instituciones que

reciben asignación de dólares mediante los mecanismos que celebra la Comisión de Cambios a través de Banco de México, ya que podría interpretarse que las mismas tienen problemas para obtener dólares en el mercado o para cubrir sus pasivos en dicha moneda. Esta interpretación, podría tener implicaciones importantes para las instituciones adquirentes de dólares quienes estarían en una posición de desventaja frente a sus competidores y verse afectadas en la confianza que el público inversionista tiene en ellas.

Asimismo, el mercado y el público en general podrían llegar a determinar consideraciones sobre el perfil crediticio de riesgo de las instituciones bancarias que hayan o no participado en este tipo de operaciones que pueden ser completamente erróneas en términos de dicho asesoramiento. No sobra mencionar que las posibles consecuencias negativas antes mencionadas, afectarían de manera directa a los clientes de las instituciones adquirentes de dólares, ya que los daños causados al patrimonio de tales instituciones necesariamente se verían reflejados en las operaciones y servicios que éstas celebran con sus clientes, lo cual repercutiría en una afectación de los intereses del público en general, usuario del sistema financiero.

Adicionalmente, las afectaciones al público inversionista, podrían llegar a implicar una afectación directa a la economía nacional, ya que es conocido el hecho de que el sistema financiero promueve el desarrollo económico del país a través del otorgamiento de crédito, generando empleo, riqueza y bienestar a la sociedad.

Por lo anterior, las instituciones podrían perder interés en participar en las operaciones cambiarias en el futuro, al saber que la información sobre el nombre de los adquirentes y el monto adquirido llegaría a ser pública y considerando las afectaciones que ello pudiera acarrearles.

Por tal motivo, la publicidad de las grabaciones de las llamadas del personal que instrumenta las operaciones en materia cambiaria en los que aparece el nombre de las instituciones que participan en las operaciones mencionadas y otros detalles como el monto que se asignó a cada una, podría comprometer la competitividad, ejecución y la estrategia de intervención del Instituto Central y con ello afectar la utilidad de la medida cambiaria o incluso eliminarla, lo que en adición a las posibles implicaciones negativas que antes se mencionaron, podría llegar a perjudicar a la economía en su conjunto y con ello al país y podría incrementar el costo de dichas operaciones en el futuro.

Otro de los grandes rubros que comprende la grabación de llamadas está relacionado con las que realiza el personal encargado de la **administración e inversión de la reserva de activos internacionales.** Se debe señalar que el objetivo último de la reserva internacional es coadyuvar a la estabilidad del poder adquisitivo de la moneda nacional mediante la compensación de

desequilibrios entre los ingresos y egresos de divisas del país. En este sentido, divulgar la información contenida en las grabaciones del personal que celebra las operaciones para la administración de la reserva internacional, comprometería la ejecución de las operaciones de inversión, incrementaría el costo de las citadas operaciones y, por lo tanto, pondría en riesgo el mantenimiento del valor de la reserva internacional, lo que representa un riesgo de perjuicio significativo al interés público en virtud de que dicho riesgo es:

1) **Real**, ya que con la divulgación de las grabaciones del personal que realiza las operaciones de administración de la reserva se haría publica información como el nombre de las contrapartes del Banco y el detalle de los instrumentos en los que Banco de México tiene invertidas las reservas internacionales lo que podría dificultar la ejecución de las operaciones de inversión, así como las estrategias de cobertura de riesgos que asumen las contrapartes del Banco por las operaciones que conciertan con este Instituto Central. Esto último tendría como consecuencia un posible incremento en el costo de la realización de las operaciones del Banco Central en detrimento del rendimiento y valor de la reserva internacional en su conjunto.

   Se debe recordar que el nivel de reservas de una nación se asocia con la fortaleza de su economía para enfrentar situaciones económicas y financieras adversas. Baste recordar los artículos de prensa que fueron publicados a finales de 2015 y principios de 2016 en los cuales, debido a la baja en el nivel de las reservas internacionales derivado de las subastas de dólares implementadas por la Comisión de Cambios a través del Banco de México, los analistas cuestionaron y mostraron preocupación respecto a si el nivel de reservas era el adecuado para enfrentar situaciones financieras adversas. Así, una afectación en el nivel de las reservas internacionales generaría una menor capacidad del Banco Central para intervenir en los mercados cambiarios, en caso de que así lo determine la Comisión de Cambios. Lo anterior, podría reflejarse en niveles más elevados del tipo de cambio del peso frente a otras divisas. A su vez, la depreciación del peso incrementaría las presiones a la alza en los precios de distintos bienes y servicios, primeramente de aquellos que utilizan insumos importados y, posteriormente de todo tipo de bienes de uso cotidiano en toda la población. De actualizarse este supuesto, se vería afectada la capacidad del Banco de México de cumplir con su objetivo prioritario de procurar la estabilidad del poder adquisitivo de la moneda nacional.

   En el mismo orden de ideas, una depreciación sostenida del tipo de cambio, podría aumentar los riesgos para la estabilidad financiera y económica del país, toda vez que las empresas y otros oferentes de bienes y servicios tienden a reaccionar con cautela ante estos episodios de volatilidad, disminuyendo sus niveles de inversión e incluso eliminando empleos hasta no tener mayor certeza del panorama económico. En este tipo de entorno, podría originarse un círculo vicioso en el cual las instituciones financieras podrían enfrentar

pérdidas en sus carteras de crédito, restringir las condiciones de otorgamiento de crédito y acentuar el debilitamiento de la actividad económica en el país.

2) **Demostrable,** pues no debe olvidarse que el monto de las reservas tiene un peso relativo importante en la economía nacional, por tal motivo es necesario mantener una estrategia de inversión de las mismas que minimice el impacto sobre las condiciones de los mercados financieros y, consecuentemente, el costo de ejecución de dichas estrategias. En tal virtud la divulgación de las grabaciones de las llamadas del personal que celebra las operaciones para administrar la reserva internacional y por ende de los instrumentos en los que el Banco Central invierte los recursos de dicha reserva representa un riesgo para la ejecución de las estrategias mencionadas; lo anterior, se debe a que diversas instituciones que no operan con el Banco de México, podrían utilizar la información contenida en las grabaciones como el nombre de las contrapartes o los instrumentos en los que se invierten con fines especulativos para comprar anticipadamente el mismo tipo de instrumentos financieros, elevando considerablemente el precio de los mismos al momento en que el Banco requiera comprarlos, circunstancia que podría afectar el rendimiento y el valor de los activos internacionales de Banco de México.

   La citada actividad especulativa junto con la divulgación de los nombre de las contrapartes del Banco como consecuencia de la divulgación de los contratos y convenios, también podría afectar o entorpecer las estrategias de dichas contrapartes del Banco de México para cubrir los riesgos que asumen por las operaciones concertadas con este Instituto Central. Esto último podría repercutir en un mayor costo de las operaciones de estas instituciones financieras, el cual podría transmitirse a la población a través de un incremento en el precio de sus comisiones y productos de crédito, incluyendo tarjetas de crédito, créditos para compra de automóviles, hipotecas, así como créditos al sector corporativo. De este modo, derivado de la dependencia de las economías y la interrelación de los mercados financieros, podría haber una afectación generalizada a la actividad económica, a través de un menor otorgamiento de crédito.

   Este tipo de comportamientos, anticiparse al mercado, es común entre los participantes de los mercados financieros y se puede ejemplificar con lo sucedido el 29 de marzo de 2017 en el que Banco de México anunció el traspaso de 321,653.3 millones de pesos al Gobierno Federal por concepto de su remanente de operación. Ese mismo día la Secretaría de Hacienda y Crédito Público (SHCP) señaló que utilizaría al menos el setenta por ciento del mismo para la amortización de la deuda pública del Gobierno Federal, esta decisión coincidió con la del año pasado en la que también se destinó el mismo porcentaje del remanente para la compra de deuda existente. Lo anterior dio paso a que los participantes del mercado anticiparan una re-compra de valores gubernamentales similar a la realizada en mayo del año pasado, lo que generó que los instrumentos de plazos similares a los que

recompró en esa fecha la SHCP incrementaran su valor en 0.21% respecto al cierre del día anterior (28 de marzo). En otras palabras, si el 29 de marzo la SHCP hubiera recomprado deuda con plazos similares a los que recompró en 2016 hubiera pagado un precio 0.21% mayor (aproximadamente 200 millones de pesos más si se considera un monto de recompra igual al de 2016).

3) **Identificable,** pues el dar a conocer detalles específicos y características de las operaciones de la administración de la reserva internacional como consecuencia de hacer públicos las grabaciones del personal que celebra las operaciones en esta materia, como por ejemplo detalles sobre los emisores de títulos de renta fija elegibles para la inversión de la reserva internacional, dará señales erróneas a los mercados financieros nacionales e internacionales y a sus distintos agentes sobre la percepción que el Banco de México tiene en relación con la seguridad de las operaciones que celebra y la capacidad, solidez o debilidad de los distintos emisores. Al respecto, estos últimos, en su mayoría son considerados de riesgo sistémico, al tratarse de entidades cuyo incumplimiento potencial pudiera afectar la estabilidad del sistema financiero, del sistema de pagos o de la economía del país en el que se encuentran establecidos, con el riesgo de que debido a la interrelación de los mercados y la globalización de la economía, esta afectación se materialice de igual forma en la economía nacional. Asimismo, lo expresado generará que los agentes financieros u otras empresas omitan analizar adecuadamente el riesgo de crédito de las instituciones y emisores con los que operan, al dar por sentado que al estar incluidas en el listado de contrapartes del Banco de México tienen un riesgo crediticio bajo, lo que representa un factor de riesgo adicional para la estabilidad del sistema financiero.

Como **agente financiero del Gobierno Federal** el Banco de México realiza operaciones con instituciones domiciliadas en México y de origen tanto nacional como internacional. Las operaciones en el ámbito nacional comprenden principalmente el seguimiento de la deuda bursátil, esto es la colocación, administración y redención de valores gubernamentales, las operaciones para manejo de pasivo y el seguimiento al programa de formadores de mercado. Por lo que respecta a las operaciones internacionales estas se centran en la contratación de las coberturas petroleras. El dar a conocer detalles de las grabaciones del personal que ejecuta las operaciones como agente financiero del Gobierno Federal, podría generar que instituciones financieras en general utilicen la información con fines especulativos frente a otras instituciones para comprar/vender anticipadamente el mismo tipo de instrumentos financieros que utiliza el Gobierno Federal en sus operaciones, elevando considerablemente su precio y el costo financiero que éste tiene que pagar. Esto no sólo dificultará la ejecución de las operaciones futuras sino que puede producir incertidumbre respecto a los recursos disponibles para otros fines del gasto público e incluso podrá comprometer los parámetros establecidos en el paquete económico del Gobierno Federal. Lo anterior representa un riesgo de perjuicio significativo al interés público en virtud de que dicho riesgo es:

1) **Real**, pues por lo que se refiere a las operaciones nacionales, de acuerdo con la normatividad vigente[5], sólo pueden participar en las operaciones que Banco de México realiza como agente financiero del Gobierno Federal en los mercados nacionales las instituciones de crédito, la Financiera rural, las casas de bolsa, las sociedades de inversión, las sociedades de inversión especializadas de fondos para el retiro y otros intermediarios autorizados expresamente por el Banco de México. Normalmente, tales intermediarios financieros participan en estas operaciones (como la subasta primaria de valores gubernamentales, las subastas sindicadas, las operaciones de refinanciamiento, etcétera) presentando posturas con precios previamente acordados con sus clientes. Esto permite a los postores determinar los precios con los que participarán en las operaciones para tratar de asegurar que recibirán asignación y, al mismo tiempo, mantener cierto margen de intermediación. En tal sentido, si se da a conocer detalles de las llamadas que realizan las personas que llevan a cabo estas operaciones a través de la divulgación de la grabación de dichas llamadas, como nombres y montos de participación de las contrapartes del Banco, sus clientes podrían obtener conclusiones no necesariamente correctas y exigir mejores precios a los intermediarios (entiéndase una tasa de interés mayor), quienes a su vez trasladarían esta mayor tasa al Gobierno Federal. Lo anterior podría generar un aumento en el costo de financiamiento del Gobierno Federal, pues se debe recordar que las operaciones que Banco de México realiza en nombre del Gobierno son con propósitos de financiamiento (emisión de valores gubernamentales) o de manejo de pasivos. Si el costo de financiamiento del Gobierno Federal se incrementa, éste tendrá que destinar mayores recursos de su presupuesto al pago de intereses de su deuda, disminuyendo el gasto en otros rubros que puedan generar mayores beneficios a la sociedad.

   Respecto a las operaciones de coberturas petroleras, se debe hacer notar que el programa de coberturas petroleras mexicano se encuentra dentro de los mayores a nivel global. Por tal motivo, debe cuidarse el impacto negativo que pueda tener sobre las condiciones de los mercados financieros y procurar que se reduzca su costo. El programa de coberturas petroleras que el Gobierno Federal implementa año con año tiene la finalidad de proteger los ingresos de la Federación, específicamente los ingresos petroleros, mismos que representan alrededor del 11% de los ingresos totales (equivalente al presupuesto asignado a los sectores de salud y educación para 2018), de acuerdo con las Estadísticas Oportunas de Finanzas Públicas.

   La divulgación de los datos de las entidades con las que se ha contratado, así como los plazos, cantidades, términos y condiciones pactadas, también afectará el interés público. Lo

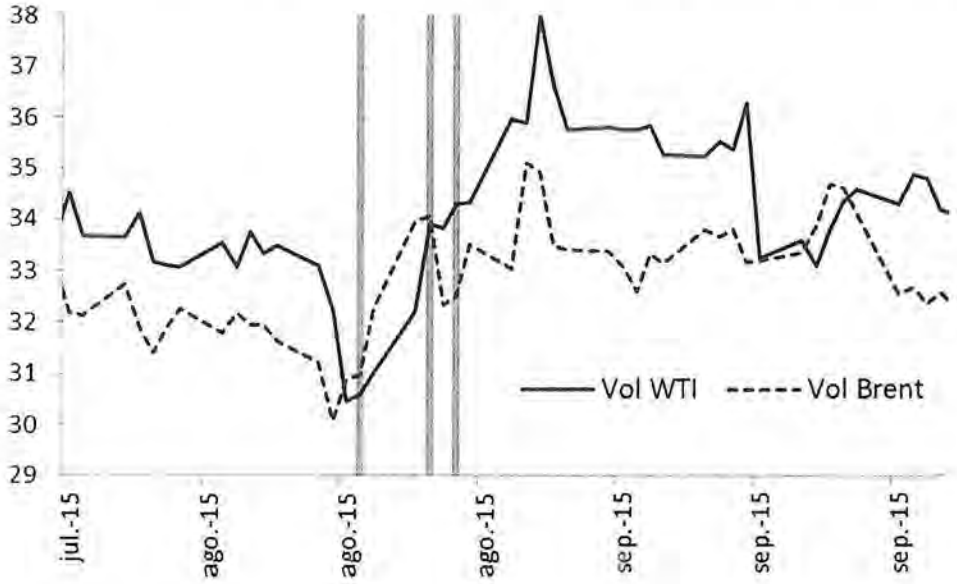
[5] Circular 5/2012 "Reglas de las subastas para la colocación de valores gubernamentales y de valores del IPAB" Consultado el 15 de noviembre

anterior, debido a que diversas instituciones ajenas al programa de coberturas podrían utilizar la información con fines especulativos para comprar anticipadamente el mismo tipo de instrumentos financieros que utiliza el Gobierno Federal, elevando considerablemente su precio. Esto ocasionará necesariamente que el costo fiscal del referido programa sea mayor, lo cual dificultará su ejecución, pues el precio de las coberturas será más alto, lo que producirá incertidumbre respecto a los recursos disponibles para otros fines del gasto público e incluso podrá comprometer los parámetros establecidos en el paquete económico del Gobierno Federal, ya que se tendrán que destinar mayores recursos públicos en la compra de las referidas coberturas, con la correlativa disminución de otros rubros del gasto público.

Además, debe señalarse que en el caso que ocurra un cambio en la rentabilidad o riesgo esperado de las contrapartes con las que se contratan las coberturas petroleras por hacer pública la información de las mismas a través de la divulgación de las grabaciones de las llamadas del personal que las instrumenta, éstas pudieran negarse a contratar coberturas con el Gobierno Federal.

En efecto, como se ilustra en la Gráfica 1, después de darse a conocer un serie de artículos sobre la cobertura petrolera de México en agosto de 2015, a través del sistema de noticias Bloomberg, la volatilidad en el precio de los crudos de referencia "West Texas Intermediate (WTI)" y "Brent" se incrementó generando también un aumento en el costo ofrecido por las contrapartes para cubrir las operaciones concertadas con el Banco de México.

Gráfica 1: Volatilidad del petróleo en términos porcentuales



Fuente: Datos de Bloomberg

La volatilidad es un componente muy importante del precio de las coberturas debido a que esta refleja el ritmo al que el precio de un activo -en este caso del WTI o Brent - puede subir o bajar. Al aumentar la volatilidad, aumenta la probabilidad de que los precios suban o caigan en mayor grado y a mayor velocidad: es decir, se acrecienta la incertidumbre de cuál será el precio de un activo a una fecha futura. Y como con cualquier seguro, al incrementar la incertidumbre sobre un evento aumenta el costo de su cobertura. Adicionalmente, este último costo no solamente lo absorbe el Gobierno Federal, al destinar mayores recursos públicos en la compra de las referidas coberturas, sino que las mismas contrapartes que ofrecen estos instrumentos tienen a su vez que realizar operaciones en el mercado para cubrirse y prevenir la posibilidad de que pierdan dinero a raíz del programa -tal y como sucedió durante los programas de 2015 y 2016, en los que el precio del petróleo cayó de manera importante, beneficiando al cumplimiento de los compromisos señalados en el Presupuesto de Egresos de la Federación, toda vez que las contrapartes tuvieron que honrar las coberturas - mismas que también incrementan en precio al aumentar la volatilidad, creando un círculo vicioso de aumentos en el precio. A manera de ejemplo, bajo las condiciones de mercado del primer trimestre del año, un incremento de 1 punto porcentual de la volatilidad -es decir, que por ejemplo ésta se incremente de 30 a 31% - equivale a que el precio de cobertura de 1 barril de petróleo aumente en 15 centavos. Si esto se traduce a un Programa de, por ejemplo, 200 millones de barriles, y donde el aumento en la volatilidad no es de solamente 1 punto porcentual sino de 8 como se observa en la Gráfica 1, se obtiene que el costo de la cobertura sería de $240 millones de dólares adicionales a lo que hubiera sido de no haber aumentado la volatilidad.

Las entidades con las que se contratan las coberturas compiten entre sí en un mercado muy especializado y en el que participan pocas contrapartes. En consecuencia, la divulgación de la información contenida en las grabaciones afectará necesariamente la determinación de los precios de los derivados. Al respecto, ha de tomarse en cuenta que la mayor parte del programa de cobertura se concentra en cubrir el crudo tipo Maya, al ser el que México produce. Sin embargo este es más susceptible de ser distorsionado, debido a lo reducido de su mercado en comparación con otros crudos de referencia como es el caso del tipo Brent.

En relación con lo anterior es importante considerar que no existe un mercado desarrollado de los instrumentos financieros necesarios para cubrir los ingresos petroleros del Gobierno Federal, por lo que el Gobierno solo puede adquirir estas coberturas con pocas instituciones financieras internacionales especializadas (contrapartes del programa). Dichas contrapartes, a su vez, se ven obligadas a comprar coberturas con otros operadores de

materias primas para diversificar su riesgo, lo cual resulta complicado debido a las pocas contrapartes que existen para este tipo de instrumentos.

Las entidades con las que se contratan las coberturas buscan a su vez celebrar operaciones en el mercado con otras instituciones financieras, en las que se consideran todos los componentes de dichas coberturas, con el fin de cubrir los riesgos que asumen. En consecuencia, instituciones ajenas al programa respectivo tendrán ventaja comparativa frente a las contrapartes del Banco Central, al conocer las necesidades de cobertura que estas requieren llevar a cabo.

2) **Demostrable**, pues por lo que se refiere a las operaciones en los mercados financieros nacionales, existe gran sensibilidad a la información que se proporciona. El hecho de dar a conocer detalles contenidos en las grabaciones del personal que instrumenta las operaciones en comento como el nombre de las instituciones participantes en las operaciones de agente financiero que Banco de México lleva a cabo a nombre del Gobierno Federal, podría conducir a conclusiones erróneas sobre su posición o inclusive su estrategia de inversión, lo que podría dar lugar a una percepción equivocada sobre la solidez o debilidad de distintas instituciones financieras. Cabe recordar que varias de las instituciones financieras que participan en éstas operaciones son o pueden ser consideradas de riesgo sistémico, por lo que al tratarse de entidades cuyo potencial incumplimiento pudiera afectar la estabilidad del sistema financiero o de los sistemas de pagos, existe el riesgo de que esta afectación se materialice en la economía nacional.

   La publicación de esta información podría traducirse en un menor interés por parte de los intermediarios financieros en participar en este tipo de operaciones, lo que derivaría potencialmente en un incremento en el costo de financiamiento del Gobierno Federal y podría comprometer la adecuada implementación de la política fiscal del país.
   En el mismo sentido, el dar a conocer los nombres de las instituciones con las que se han celebrado las operaciones de coberturas petroleras y las especificaciones de las mismas, dará señales erróneas a los mercados financieros nacionales e internacionales y a sus distintos agentes sobre la percepción que el Banco de México tiene en relación con la seguridad de las operaciones que celebra y la capacidad, solidez o debilidad de distintas instituciones financieras, en específico, de aquellas con las que se han celebrado las mencionadas operaciones. Dichas instituciones, en su mayoría son consideradas de riesgo sistémico, al tratarse de entidades cuyo incumplimiento potencial pudiera afectar la estabilidad del sistema financiero, del sistema de pagos o de la economía del país en el que se encuentran establecidas, con el riesgo de que debido a la interrelación de los mercados y la globalización de la economía, esta afectación se materialice de igual forma en la economía nacional. Esto además tendrá implicaciones sobre la competencia en el sector financiero, al poner en una posición ventajosa o incluso beneficiar a las instituciones

incluidas en la lista de instituciones autorizadas para operar las coberturas de petróleo y potencialmente perjudicar a aquellas que no lo están.

Lo expresado generará que los agentes financieros u otras empresas omitan analizar adecuadamente el riesgo de crédito de las instituciones con las que operan, al dar por sentado que al estar incluidas en dicho listado tienen un riesgo crediticio bajo, lo que representa un factor de riesgo para la estabilidad del sistema financiero.

Por otra parte, al ocurrir lo mencionado en los párrafos anteriores, tanto para las operaciones realizadas en los mercados nacionales como internacionales, el Banco de México no establecería los incentivos para una sana competencia entre las instituciones financieras, en contravención a una de sus finalidades previstas en el artículo 2o. de su Ley, que es precisamente promover el sano desarrollo del sistema financiero. El divulgar las grabaciones del personal que celebra las operaciones que realiza este Instituto central como como agente financiero del Gobierno Federal, impedirá el cumplimiento de dicha finalidad, pues afecta la debida competencia entre las instituciones financieras y debilita la confianza en algunas de ellas. Este argumento es incluso válido para el programa de coberturas petroleras que, si bien se realiza en mercados financieros internacionales de primer orden, debido a la interconexión y dependencia que existe entre las economías, la afectación a cualquiera de las entidades financieras que integran los mercados financieros se traduce en una afectación al mercado nacional y a las entidades financieras que están establecidas en nuestro país.

El debilitamiento de la confianza en algunas instituciones incrementa su costo de financiamiento que, a su vez, encarece el crédito a hogares y empresas, con implicaciones adversas sobre el desarrollo y dinamismo de la actividad económica. Esto último a través de mayores comisiones y tasas de interés en créditos al consumo, hipotecarios, refaccionarios, de habilitación y avío, entre otros.

En caso de ponerse en riesgo la realización de cualquiera de las operaciones de agente financiero del Gobierno Federal, esto tendrá implicaciones directas sobre las finanzas públicas del país y la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero mexicano al ponerse en duda la capacidad de pago del Gobierno Federal. En efecto, un incremento en el costo de financiamiento del Gobierno Federal por una menor participación de las instituciones financieras en las operaciones que Banco de México realiza en su nombre en los mercados nacionales, o el no contar con un programa de cobertura petrolera podría poner en riesgo las finanzas públicas.

Una debilidad en las finanzas públicas genera incertidumbre respecto de la capacidad crediticia del Gobierno Federal, ejemplo de ello es el cambio en la perspectiva de la calificación crediticia de la deuda del Estado Mexicano, de estable a negativa, por parte de la calificadora Fitch Ratings el pasado 31 de octubre. En el comunicado que acompañó la decisión, la calificadora argumentó que "...Aunque Fitch espera que la próxima administración continúe apoyando los aspectos fundamentales del marco de política macroeconómica –disciplina presupuestaria y autonomía del Banco de México (Banxico)–, persisten los riesgos relacionados con la postura fiscal del gobierno entrante". La revisión en la perspectiva de riesgo crediticio del país desencadenó una serie de revisiones a la perspectiva de riesgo crediticio de los emisores nacionales, entre ellos, algunas instituciones financieras mexicanas. En el comunicado de fecha 6 de noviembre de 2018, la calificadora señaló: "...Fitch Ratings has conducted a portfolio review of selected Mexican Financial Institutions (FIs) following the revision of Mexico's sovereign rating Outlook to Negative from Stable on Oct. 31, 2018 (Fitch Ratings realizó una revisión de la cartera de instituciones financieras mexicanas (IF) seleccionadas luego de la revisión de la calificación de la calificación soberana de México a Negativo desde Estable el 31 de octubre de 2018)".

3) **Identificable**, toda vez que revelar la información contenida en las grabaciones del personal del Banco de México que celebra las operaciones como agente financiero del Gobierno Federal, puede derivar en conclusiones erróneas sobre el riesgo de los intermediarios financieros, en particular en el caso de las instituciones que participan en las operaciones llevadas a cabo en los mercados nacionales, y generarles pérdidas potenciales a los mismos y, en un caso extremo, una corrida bancaria en su contra. Cuando una institución sufre una corrida bancaria se produce una oleada especulativa, que bien puede definirse como un sentimiento de desconfianza generalizada y especulación poco fundamentada sobre la solidez de las instituciones de crédito por parte de los depositantes de todo el sistema financiero. Este hecho incrementa en forma considerable la probabilidad de contagio a clientes de otras instituciones y de un retiro masivo de los depositantes de las instituciones que no quieren perder sus ahorros, poniendo en riesgo la estabilidad financiera y la economía nacional en su conjunto. Adicionalmente, si como resultado de una corrida bancaria una institución de crédito se declara en bancarrota, es muy probable que ese participante no pueda cumplir con sus obligaciones en los sistemas de pagos, provocando con ello que otros participantes también incumplan, generando lo que se conoce como riesgo sistémico. Si además la institución de crédito en bancarrota es sistémicamente importante, el contagio podría esparcirse rápidamente a todo el sistema financiero, incrementando los riesgos para el sano desarrollo del mismo y para la estabilidad financiera, con el consecuente daño grave a la economía nacional.

En relación con la revisión a la baja de las calificaciones a algunos bancos mexicanos que ocurren normalmente cuando existen dudas respecto a la solidez de las finanzas públicas

del país, es importante resaltar que un deterioro en la calificación de dichas entidades puede restringir su acceso a financiamiento e incrementar el costo del mismo, dificultando el cumplimiento de sus obligaciones con los potenciales riesgos que esto implica para los sistemas de pagos y la estabilidad financiera del país. Más aún, siendo los bancos mexicanos de los principales tenedores de deuda emitida por el Gobierno de México, la baja calificación de dichos títulos afecta la liquidez de las instituciones financieras tenedoras, colocándose en una situación de riesgo que, dependiendo de la institución financiera afectada, podría representar un riesgo al sistema financiero en su conjunto. Adicionalmente, una percepción de mayor riesgo en las finanzas públicas podría generar desconfianza y la salida de los títulos emitidos por el Gobierno Mexicano de varios índices de referencia de inversión y por ende una redistribución de las carteras de inversión de participantes extranjeros, que también son de los principales tenedores de estos valores, generando una venta importante de títulos y un incremento en el costo de financiamiento del Gobierno Federal.

En el caso particular de las coberturas petroleras, debe señalarse que en el caso de no poder cubrir íntegramente los ingresos petroleros del Gobierno, un ajuste a la baja en los precios internacionales del petróleo implicaría una disminución en los ingresos del Gobierno Federal, lo que a su vez requeriría un mayor endeudamiento para cubrir dicha disminución. Lo anterior representaría un cambio en la política fiscal del Gobierno Federal (proceso de consolidación fiscal), lo que podría afectar la percepción de riesgo de la deuda del Gobierno con su consecuente aumento en el costo de financiamiento del mismo.

Finalmente, el dar a conocer detalles de las llamadas y grabaciones del personal encargado del **soporte del funcionamiento de los Sistemas de Pagos** representa un riesgo de perjuicio significativo al interés público en virtud de que dicho riesgo es:

1) **Real**, en razón de revelar o divulgar la información relacionada con los registros y grabaciones de llamadas realizadas y recibidas que soportan el funcionamiento de los Sistemas de Pagos, facilita a una persona o grupo de personas con intenciones delincuenciales distinguir las comunicaciones de los Servidores Públicos que están relacionadas con aspectos de seguridad informática, especificaciones técnicas en materia de seguridad, procesos de continuidad operativa y de contingencia; así mismo permitiría identificar los tiempos de respuesta de los Participantes ante presuntas vulneraciones, protocolos de comunicación y, en general, información relacionada con la infraestructura de los sistemas de pago administrados por este Instituto Central, lo cual posibilita la realización de acciones hostiles en contra de las tecnologías de la información de este Banco Central, así como de las infraestructuras que éste administra, opera y supervisa, lo cual, podría menoscabar la efectividad de las infraestructuras a tal grado, que su destrucción o inhabilitación afectaría seriamente la efectividad de las medidas implementadas en los sistemas financiero y económico, del país, arriesgando el

funcionamiento de esos sistemas y, en consecuencia, de la economía nacional en su conjunto.

Asimismo, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se fundamentan en descubrir y aprovechar vulnerabilidades de dichos sistemas, así como brechas de seguridad en los procesos y protocolos de operación, 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, la infraestructura informática y sus procesos operativos.

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.[6]

En el caso en concreto, los registros y grabaciones de llamadas realizadas y recibidas que soportan el funcionamiento de los Sistemas de Pagos contiene información relacionada con especificaciones técnicas en materia de seguridad, procesos de continuidad operativa, información sobre los componentes de los sistemas informáticos así como especificaciones de equipos de cómputo y telecomunicaciones, especificaciones en materia de seguridad informática, protocolos de actuación para la operación de los sistemas de pagos así como las condiciones de operación de los mismos, entre otros, por lo que su divulgación proporcionaría elementos de información que facilitarían a los cibercriminales aprovechar los puntos débiles de las infraestructuras de los mercados financieros, entre ellas, los sistemas de pagos, 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 infraestructuras.

2) **Demostrable**, ya que es un hecho notorio que los sistemas de pagos de Bancos Centrales han sufrido ataques cibernéticos a través de los participantes de estas infraestructuras de

[6] 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.

forma constante y organizada. Dichos ataques tienen por objeto el robo de recursos económicos a través del empleo de vulnerabilidades en las instituciones, aplicativos e infraestructura tecnológica de los sistemas.

Adicionalmente, está documentado que durante los últimos años se ha observado un incremento sostenido de ataques informáticos en el sector financiero a nivel mundial, incluyendo Bancos Centrales y diversas instituciones financieras. Las investigaciones realizadas señalan que estos ataques han sido orquestados por organizaciones criminales internacionales con herramientas y técnicas sofisticadas que, además de dañar la reputación de las instituciones afectadas, han generado cuantiosas pérdidas económicas.[7]

En relación con lo anterior, es importante señalar que México ocupa el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica[8] y que tan sólo en México, el costo causado por el cibercrimen ascendió a $5,500 millones de dólares y afectó alrededor de 22.4 millones de personas; mientras que a nivel mundial, el costo ascendió a $125,900 millones de dólares y afectó a 689.4 millones de personas.[9] Por lo anterior, este Instituto Central[10] y autoridades como la Secretaría de Hacienda y Crédito Público[11] se han pronunciado sobre la importancia de fortalecer la ciberseguridad para la estabilidad del sistema financiero.

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

i) El ataque de tipo "Watering hole" en Polonia, que permitió utilizar un servidor de la Autoridad de Supervisión Financiera para distribuir código malicioso a más de 20 bancos

---

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

8 Arreola Javier. "Ciberseguridad (casi) a prueba del enemigo 'invisible'". Forbes México. http://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/ consultado el 13 de noviembre de 2018.

9 Informe Norton sobre Ciberseguridad 2016 - Comparaciones Globales https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf consultado el 13 de noviembre de 2018.

10 En septiembre de 2016, el Banco de México publicó el documento "Política y funciones del Banco de México respecto a las infraestructuras de los mercados financieros" en el cual dedica una sección especial al tema de seguridad informática. Este documento se encuentra disponible en la siguiente dirección electrónica: http://www.banxico.org.mx/sistemas-de-pago/informacion-general/politica-del-banco-de-mexico-respecto-de-las-infra/%7B2EAC65D2-21F4-AB2D-D250-06926EE796F8%7D.pdf, consultado el 13 de noviembre de 2018.

11 Secretaría de Hacienda y Crédito Público. "Fortalecer la ciberseguridad, relevante para el desarrollo de México." 29 de octubre de 2017. https://www.gob.mx/shcp/prensa/informe-semanal-del-vocero-132251?idiom=es consultado el 13 de noviembre de 2018.

polacos[12] , el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada;[13]

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;[14]

iii) El ataque mediante el código malicioso "Petya", enfocado en borrar archivos y discos duros completos, que paralizó las actividades de aerolíneas, bancos y bufetes de abogados en Europa;[15]

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;[16]

v) 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;[17]

vi) Los cibertataques reportados por la empresa de ciberseguridad S21sec realizados por el grupo cibercriminal llamado 'Cobalt', el cual consistió en un ataque realizado a los cajero

---

12 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 13 de noviembre de 2018.

13 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 13 de noviembre de 2018.

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

15 Marín, Eduardo. "Descubren Que Petya, El Ataque Que Paralizó Empresas De Toda Europa, No Secuestraba Archivos Sino Que Los Borraba." Gizmodo En Español, Es.gizmodo.com, 28 de junio de 2017, http://es.gizmodo.com/descubren-que-petya-el-ataque-que-paralizo-empresas-de-1796492938 consultado el 13 de noviembre de 2018.

16 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 13 de noviembre de 2018.

17 Nussman, Chris. "DHS Bulletin on Denial of Service (TDoS) Attacks on PSAPs." NENA The 911 Association, 17 de marzo de 2013, www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm, consultado el 13 de noviembre de 2018.

automáticos basado en red, es decir que no se requiere acceso físico al cajero para perpetrarlos, sino que la infección se lleva a cabo desde la propia red interna del banco; [18]

vii) El ciberataque basado en la modalidad de denegación de servicio distribuido (DDoS) en Holanda, en el cual diez millones de holandeses se quedaron sin firma digital por el bloqueo del portal como consecuencia de una avalancha de solicitudes; [19]

viii) Los ciberataques a los que fue víctima Delta Air Lines, entre el 26 de septiembre al 12 de octubre de 2017, los cuales fueron informados a través de un comunicado que la compañía [24]7.ai, proveedora de servicios informáticos de ésta y otras compañías, suceso que causó que los datos bancarios de algunos de los usuarios de la aerolínea se hayan visto comprometidos durante ese periodo. [20]

ix) Los ataques cibernéticos que han sufrido otros Bancos Centrales a través de la infraestructura de sistemas de pagos conocida como SWIFT, la cual ha sido utilizada para realizar robos de capital, uno de estos casos es el del Banco Central de Bangladesh, que sufrió un robo de 81 millones de dólares. [21] 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. [22] 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. [23]

x) El ataque ocurrido a las instituciones financieras participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI®), el cual consistió en la alteración de sus aplicativos para conectarse a esta Infraestructura de Mercado Financiera (IMF), mediante código malicioso, el cual distribuyó dinero desde las cuentas concentradoras de los participantes

---

18 S21Sec. "COBALT: EL CIBERCRIMEN ORGANIZADO GOLPEA LOS CAJEROS AUTOMÁTICOS EUROPEOS." S21Sec, 23 de noviembre de 2016, www.s21sec.com/es/blog/2016/11/cobalt-cibercrimen-organizado-que-ataca-a-los-cajeros-automaticos-europeos consultado el 13 de noviembre de 2018.

19 Recalde, Luis. EL CIBERESPACIO: EL NUEVO TEATRO DE GUERRA GLOBAL. Revista De Ciencias De Seguridad y Defensa, http://geo1.espe.edu.ec/wp-content/uploads/2016/07/art15.pdf consultado el 13 de noviembre de 2018.

20 Delta Airlines. "INFORMATION ON [24]7.AI CYBER INCIDENT." Information on [24]7.Ai Cyber Incident, 7 de abril de 2018, www.delta.com/content/www/en_US/response.html consultado el 13 de noviembre de 2018.

21 Michael Riley, Alan Katz. "Swift Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh". Bloomberg. 26 de Mayo de 2016. https://www.bloomberg.com/news/articles/2016-05-26/swift-hack-probe-expands-to-up-to-dozen-banks-beyond-bangladesh consultado el 13 de noviembre de 2018.

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

23 Antony Peyton. "Symantec reveals more hack attempts on Swift network". Banking Technology. 11 de octubre de 2016. https://www.bankingtech.com/2016/10/symantec-reveals-more-hack-attempts-on-swift-network/ consultado el 13 de noviembre de 2018.

a cuentas de usuarios específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero. [24] 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. [25]

Inclusive, uno de los modus operandi de los ciberataques es precisamente a través de la obtención de información pública, información fácilmente accesible o información inaccesible, lo cual puede ocurrir mediante solicitudes de acceso a la información, o bien, a través de las organizaciones que operan o tienen acceso a los sistemas, en complicidad o no, con el único objeto de conocer las vulnerabilidades en las instituciones, empresas, sistemas, protocolos y procedimientos de operación e infraestructura de tecnologías de la información. [26]

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. [27]

Por lo anterior, los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar cualquier tipo de información asociada a los sistemas o los procesos en los que intervienen así como las especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuyo rol no esté autorizado[28], entre otros, en el entendido de que dicha información, al

---

[24] Banco de México. "Información sobre los ataques a los Participantes del SPEI". http://www.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/%7B2B9BB8C6-D66B-38C4-CC90-F72A7BC335C9%7D.pdf, consultado el 13 de noviembre de 2018.

[25] Acorde con los "Puntos importantes sobre la situación actual del SPEI" publicados en la página de internet del Banco de México. http://www.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/%7B022CD9D7-11A9-68E6-D1A5-965F57A23F60%7D.pdf, consultados el 13 de noviembre de 2018

[26] El Economista, *El sistema financiero mexicano fue víctima de una campaña de ciberataques*, 15 de mayo de 2018. https://www.eleconomista.com.mx/sectorfinanciero/El-sistema-financiero-mexicano-fue-victima-de-una-campana-de-ciberataques-20180515-0097.html consultado el 13 de noviembre de 2018.

[27] 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 13 de noviembre de 2018.

[28] 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

estar en posesión de personas no autorizadas, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central de la Nación, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

3) **Identificable,** ya que a la fecha de realización de la presente prueba de daño, es un hecho notorio que los sistemas de pagos están siendo objeto de ciberataques a gran escala, como quedó demostrado en la sección anterior. Si bien dichos ataques no han logrado irrumpir en los sistemas del Banco de México, resulta claramente identificable que el objeto final de dichos ataques son los sistemas de pagos que maneja el Banco de México, cuya seguridad depende de la reserva de la información materia de la presente prueba de daño.

En ese sentido, un ataque informático derivado de proporcionar la información materia de la presente prueba de daño, podría resultar en la afectación de las órdenes de transferencia en las cuentas bancarias de los distintos participantes y de los usuarios del sistema en comento. A su vez, estas afectaciones en las órdenes de transferencia podrían derivar en una pérdida de patrimonio no sólo para las instituciones financieras del país y demás participantes de los sistemas de pagos, sino en perjuicio de la población usuaria de los pagos electrónicos interbancarios, es decir millones de personas físicas y morales, incluyendo aquellos empleados del sector público o privado que reciben su pago de salario vía transferencia electrónica que realizan sus patrones.

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

---

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 13 de noviembre de 2018.

Por lo anterior, un ataque perpetrado directamente al SPEI o a sus participantes, ocasionado por dar a conocer información, representa un perjuicio significativo para el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias, pues de acuerdo con la información del Banco de México, de agosto de 2017 a agosto de 2018, se realizaron aproximadamente 603 millones de pagos electrónicos interbancarios por un monto de 293 billones de pesos; lo anterior equivale a más de 63 mil operaciones por un monto de aproximadamente 31 mil millones de pesos por hora, únicamente para lo que respecta al SPEI. [29]

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

El riesgo de perjuicio que supondría la divulgación de la información, supera el interés público general de que se difunda, pues dar a conocer las grabaciones de las llamadas del personal del Banco de México que instrumenta las operaciones con propósitos de regulación monetaria, regulación cambiaria, de inversión y administración de las reservas internacionales, de agente financiero del Gobierno Federal y de soporte de los Sistemas de Pagos, no abona un beneficio a la transparencia comparable con el perjuicio de debilitar la efectividad de las medidas de política en materia monetaria, o de una oleada especulativa que afecte a las instituciones, muchas de ellas de importancia sistémica, o de debilitar la efectividad de las medidas adoptadas en relación con las políticas en materia cambiaria, las acciones encaminadas a mantener la estabilidad del poder adquisitivo de la moneda nacional, evitar distorsiones en la estabilidad de los mercados, garantizar la estabilidad del sistema financiero, de los sistemas de pagos y de la economía nacional en su conjunto, de no incrementar el costo de las operaciones financieras que realiza el Banco en sus operaciones de inversión y administración de la Reserva Internacional, de no incrementar el costo de las operaciones del Banco, en su carácter de agente financiero del Gobierno Federal, en particular de la Secretaría de Hacienda y Crédito Público como sujeto obligado del sector público federal y de proteger al sistema financiero y en consecuencia a sus usuarios, respecto de otorgar publicidad a diversa información contenida en las grabaciones de las llamadas realizadas por el personal que instrumenta las operaciones antes mencionadas. En atención a lo anterior, la reserva en la

---

[29] Banco de México. Sistemas de pago de alto valor, Sistemas de liquidación en tiempo real (CF252) – Sistema de Pagos Electrónico Interbancarios. http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es

publicidad de la información, resulta la forma menos restrictiva disponible para evitar un perjuicio mayor.

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que se debe prevalecer el interés público de proteger la efectividad de las medidas de política en materia monetaria, de no afectar la efectividad de uno de los mecanismos de política cambiaria establecidos por la Comisión de Cambios; de no incrementar el costo de las operaciones cambiarias realizadas por el Banco central a nombre propio y a nombre del Gobierno Federal, en su carácter de agente financiero, en particular de la Secretaría de Hacienda y Crédito Público como sujeto obligado del sector público federal; y de proteger los sistemas de pagos y en consecuencia al sistema financiero y sus usuarios de la perpetración de ataques cibernéticos dirigidos específicamente a los sistemas de pagos administrados por el Banco de México y a la infraestructura relacionada con estos, los cuales tengan como resultado la creación de mecanismos que faciliten el acceso indebido, la substracción de información - como datos personales referente a sus usuarios y las operaciones que realizan -, la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción en éstos; respecto de otorgar publicidad de las grabaciones del personal que celebra las operaciones con propósitos de regulación monetaria, cambiaria, de inversión y administración de la reserva internacional, de agente financiero del Gobierno Federal y de las que dan soporte a los sistemas de pagos. En atención a lo anterior, la reserva en la publicidad de la información, resulta la forma menos restrictiva disponible para evitar un perjuicio mayor.

La reserva de la información deberá mantenerse, al menos por cinco años, pues dar a conocer detalles de las grabaciones que realiza el personal encargado de instrumentas las operaciones monetarias, cambiarias y de agente financiero en los mercados nacionales, como por ejemplo el nombre de las instituciones con las que se realizan, podría generar señales erróneas al público sobre la solidez o debilidad de las instituciones que participan en las mencionadas operaciones, lo cual pondría a estas instituciones, en desventaja frente a sus competidores y las podría afectar en la confianza que el público inversionista tiene en ellas al ser el universo de participantes reducido y con pocas variaciones a lo largo del tiempo. La reserva de la información al menos por cinco años aplica también para las grabaciones que realiza el personal como agente financiero que se realizan en mercados internacionales toda vez que la realización dichas operaciones es un evento que se realiza cada año y, por las características del mercado en que se llevan a cabo (especializado y reducido en cuanto al número de contrapartes), las probabilidades de efectuar operaciones con la misma contraparte en años consecutivos son altas, lo que implicará que las instituciones ajenas a las operaciones en cuestión podrán dar seguimiento a las operaciones de las instituciones que son o han sido contrapartes del Banco de México en este tipo de operaciones y con base en dicha información determinar si participan o no en el programa, abriendo la posibilidad, como se mencionó con anterioridad, que puedan utilizar la información con fines especulativos para comprar anticipadamente el mismo tipo de instrumentos, incrementando el costo de las operaciones

financieras que nos ocupan. De la misma forma, las llamadas y grabaciones de las mismas del personal que soporta las operaciones de los sistemas de pagos deben reservarse por el plazo de cinco años toda vez que, como se ha manifestado esta acción atiende a la protección de las medidas de seguridad informática, con la finalidad de evitar proporcionar información que facilite intrusiones que puedan vulnerar los protocolos de operación e inhabilitar los sistemas de tecnologías de la información y comunicaciones, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques informáticos, no solo de las vulnerabilidades identificadas sino de aquellas que no se encuentran reconocidas provocando afectaciones a las Infraestructuras de los Mercados Financieros que opera y administra este Instituto Central, entre ellas los sistemas de pagos, menoscabaría la efectividad de las medidas implementadas en relación con las políticas en materia del sistema financiero del país, y ponga en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, así como comprometería las acciones encaminadas a propiciar el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos. Por lo antes expuesto, la divulgación de las grabaciones del personal y en su caso, el listado de llamadas que instrumenta las operaciones cambiarias, monetarias, de administración de la reserva internacional, de agente financiero del Gobierno Federal y de soporte de los sistemas de pagos, comprometería 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, se comprometerían las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero o el buen funcionamiento de los sistemas de pagos; se otorgaría una ventaja indebida, generando distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pagos, y se generaría un incumplimiento de las obligaciones de los participantes en un sistema de pagos, afectando seriamente al sistema financiero.

Por lo antes expuesto, con fundamento en los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 103, segundo párrafo, 104, 105, 106, fracciones I y III, 107, 108, último párrafo, 109, 113, fracción IV, y 114 de la Ley General de Transparencia y Acceso a la Información Pública; 97, 98, fracciones I y III, 100, 102, 103, 110, fracción IV, y 111de la Ley Federal de Transparencia y Acceso a la Información Pública; 1, 2, 3, fracciones I, II, III, y IV, de la Ley del Banco de México, 4, párrafo primero, 8, párrafos primero y tercero, 10, párrafo primero, 12, 19, 19 Bis, y 20, del Reglamento Interior del Banco de México, Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, así como Primero, Cuarto, Quinto, Sexto, párrafo segundo, Séptimo, fracción III, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I, II, III y IV, Trigésimo tercero, Trigésimo cuarto, párrafos primero y segundo, Quincuagésimo cuarto y Quincuagésimo quinto, párrafo primero, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, la información referente a la grabación de las llamadas que realizó el personal de la Dirección General de Operaciones y Sistemas

de Pagos del 8 de octubre al 16 de octubre de 2018, es de clasificarse como reservada, pues su divulgación pondrían en riesgo las funciones del Banco de México, el funcionamiento del sistema financiero y de la economía nacional en su conjunto, se dañaría el buen funcionamiento de los sistemas de pagos, se crearían distorsiones en los sistemas de pagos, se comprometerían las acciones encaminadas a propiciar el buen funcionamiento de los sistemas de pagos y se generaría el incumplimiento de obligaciones de un participante en los sistemas de pagos.

Referencia 1

Britain's bank run

The Bank that failed

The governor of the Bank of England is the biggest casualty of a financial fiasco—but far from the only one

Print edition | Leaders
Sep 20th 2007

Bloomberg/Landov

BRITAIN prides itself on its expertise in finance. The City is the brightest jewel in the economy's crown. Banks and financiers have based themselves in London because of the depth and sophistication of its markets and the sure touch with which they have been regulated.

Referencia 2

Wall Street humiliated by nationalisation of banks

By Stephen Foley in New York | Wednesday 15 October 2008 00:00 | 0 comments

The US government is set to become the largest shareholder in its national banks, pumping in $250bn (£143bn) to prop up its financial system and marking one of the most startling moments in a credit crisis that has broughtquasi-nationalisation to the home of free-market capitalism.

President George Bush appeared in the White House Rose Garden yesterday morning to declare that his government was immediately taking stakes in nine of the biggest banks in America, and would extend its hand to hundreds and possibly thousands more.

Referencia 3

La Jornada

México SA

Carlos Fernández-Vega

- Ahorro para la especulación (II)
- Cachorros zarandeados

A mediados de 1989, Carlos Salinas de Gortari puso en circulación los Bonos de la Tesorería de la Federación, Tesobonos, a disposición, decía, del "público ahorrador en general". Se trataba de valores gubernamentales, cotizados en dólares y pagaderos en pesos, con interés garantizado más el diferencial del tipo de cambio entre la fecha de compra y la de amortización. Como en el caso de los Petrobonos y los Cetes, estos nuevos títulos quedaron en pocas manos.

El resultado de los Tesobonos no rompió expectativa alguna, hasta que a mediados de noviembre de 1994 –unas semanas antes de la estrepitosa devaluación por los "errores de diciembre"– se convirtieron en pieza de colección. Más allá de su agudo olfato, algún amigo informó a los principales especuladores financieros y bursátiles lo que estaba a punto de suceder: el fin de la ilusión primer mundista machaconamente difundida por el salinato y el derrumbe económico-financiero del país.

Dos semanas antes del desplome de la moneda nacional (21 de diciembre de 1994), cinco casas de bolsa pertenecientes a igual número de grupos financieros (constituidos tras la reprivatización bancaria), incrementaron en casi 400 por ciento la adquisición de Tesobonos. Al igual que en el caso de los CAP's antes de la venta de los bancos, en esta ocasión las más movidas fueron Acciones y Valores, del Grupo Financiero Banamex-Accival (Roberto Hernández y Alfredo Harp Helú); Invermexico, del Grupo Financiero de igual nombre (Carlos Gómez y Gómez, uno de los destinatarios del correo electrónico referido en el México SA del 17 de abril); Operadora de Bolsa, del Grupo Financiero Obsa-Serfin (Adrián Sada); Probursa, del Grupo Financiero Mercantil-Probursa (José Madariaga Lomelín, en ese entonces presidente de los banqueros), y Mexival, del Grupo Financiero Mexival-Banpaís (Ángel Isidoro Rodríguez, *El Divino*).

La crisis estalló en la cara de millones de desamparados mexicanos, pero los especuladores financieros y bursátiles, no sin la contribución de sus amigos en el gobierno, ya habían tomado sus precauciones: con el grueso de los Tesobonos en sus alforjas, presionaron y obtuvieron de la administración Zedillo que esos valores les fueran pagados en dólares y no en pesos, como lo estableció el decreto presidencial (junio de 1989) para su emisión y circulación. Así, parte de la deuda interna –contratada en pesos para ser pagada en pesos, a un tipo de cambio de 3.4 pesos por dólar– simple y sencillamente se dolarizó (a un tipo de cambio de 7.63 pesos por billete verde en febrero de 1996) para favorecer a ese grupúsculo de especuladores, más los extranjeros, con muy buenos amigos en las más altas esferas del poder.

En menos de 14 meses, el gobierno zedillista amortizó, en dólares, el saldo total de Tesobonos en circulación: alrededor de 30 mil millones de billetes verdes (que legalmente debieron pagarse en pesos, al igual que los intereses por ellos generados y el diferencial en el tipo de cambio), y buena parte de ellos ingresaron a las alforjas del selecto grupo de especuladores bursátiles y financieros. Según información proporcionada por el propio ex inquilino de Los Pinos, estos valores representaron 43 por ciento del "costo de la crisis en 1995", es decir, 33 mil de los 70 mil millones por él reconocidos.

De acuerdo con información de la Secretaría de Hacienda, al cierre de 1993 los Tesobonos representaban entre 5 y 6 por ciento de la deuda interna total del gobierno federal; al finalizar 1994, más de 50 por ciento. Para justificar el beneficio a los especuladores, la dependencia aseguró que "lo único que se hizo fue cambiar deuda interna por deuda externa" (Tesobonos en pesos por Tesobonos en dólares), pero lo hizo sin autorización del Congreso.

A pesar de ello, los Tesobonos representaron el entremés de lo que ya se cocinaba: el "rescate" bancario, por medio del Fobaproa y sus 120 mil millones de dólares (también sin autorización del Congreso), que los mexicanos no terminan de pagar. Entre los beneficiarios, reiteradamente aparecen los nombres de los especuladores financieros y bursátiles que gozaron de los subsidios cambiarios del Ficorca, de la "devolución" de empresas no bancarias asociadas a las instituciones estatizadas, de los bonos de indemnización bancaria, de los certificados de aportación patrimonial de la reprivatización de los bancos, de los Tesobonos y de la impunidad que el gerente en turno de Los Pinos les brindó, les brinda.

A lo anterior agréguese los impuestos "diferidos" (causados pero nunca entregados), los voluminosos créditos fiscales que no amortizan, las exenciones y regímenes tributarios especiales y tantas otras gracias que, por falta de espacio, escapan de este breve recuento de cómo las finanzas nacionales han sido puestas al servicio de una minoría rapaz y millonaria.

Viene el festín del petróleo: los llamados "bonos petroleros ciudadanos" serían el más fresco entremés de lo que el gerente en turno pretende ponerles en charola de plata. Los manjares vienen enseguida.

Por cierto, los especuladores bursátiles organizados (*Bolsa Mexicana de Valores* y las casas de bolsa) juran que "el sector financiero del país no recibió de parte del gobierno de la República ninguna información material sobre el contenido de la reforma energética" antes de que el inquilino de Los Pinos "la presentara a la nación", es decir, el pasado 8 de abril.

Bien, no iban a decir que sí, pero sólo para ubicar va una declaración de Guillermo Prieto Treviño, presidente de la BMV, el 2 de abril de 2008 (seis días antes de que el inquilino de Los Pinos entregara su iniciativa al Congreso): "el mercado de capitales está listo para operar títulos de Pemex... La reforma energética es un objetivo en la bolsa y el sector financiero" (*La Jornada*, Antonio Castellanos, 2 de abril de 2008). Y los especuladores ya tienen las alforjas.

Las rebanadas del pastel

Si de especuladores y tráfico de influencias se trata, allí están los cachorros de Marta Sahagún, a quienes el IFAI les propinó una buena zarandeada al ordenar a la PGR entregar copia de la indagatoria ministerial en su contra.

BANCO DE MÉXICO

Referencia 4

Información política confidencial

El blog de análisis político más comentado y acertado de México

— "Las cosas antes del PRI" / Luciano Ojeda — Peña Nieto visto a su tan Felipe Calderón —

La crisis mexicana ahora sí parece crisis / Arturo Herrera

Publicado el jueves 29, 2009 por Luis Estrada

Si hay algo que sabemos los mexicanos es comer con picante, fallar penaltis y ligar las devaluaciones a las crisis económicas. Y no es para menos. La mayor parte de las crisis económicas en la historia moderna mexicana -por lo menos las más graves- han sido inauguradas con devaluaciones del peso.

En 1976, el peso pasó de 12,5 unidades por dólar, nivel en el que se había mantenido desde 1954, a 22 pesos por dólar en unas cuantas semanas. Situaciones similares ocurrieron en febrero de 1982 y en diciembre de 1994, cuando nuevamente al peso le bastaron unas cuantas semanas para perder la mitad de su valor.

En algunos de estos eventos se presume que algunos inversionistas mexicanos, usando información privilegiada, cambiaron pesos a dólares y los sacaron del país obteniendo jugosas ganancias.

Así pues, en el imaginario popular -y en el de gran número de políticos y analistas- las crisis van acompañadas de devaluaciones y tienen culpables muy precisos: el gobierno que no sabe manejar la política económica y *los sacadólares* que se enriquecen especulando contra el peso.

Por eso ésta ha sido una crisis singular para los mexicanos. De hecho el primer problema con el peso no se dio sino hasta el verano pasado, un año después de iniciada la crisis mundial, y fue un problema de ¡sobrevaluación! Sí, la moneda llegó a estar a 10 pesos por dólar y el problema de las autoridades financieras no era analizar cómo parar una devaluación (algo con lo que los funcionarios financieros mexicanos han venido lidiando durante décadas) ¡sino cómo evitar que el precio se siguiera apreciando!

Por ello, el 25 de julio la comisión de cambios, (formada de manera paritaria por funcionarios el Ministerio de Hacienda y el Banco de México, aunque con voto de calidad de la primera) anunció que el Banco de México dejaría de subastar dólares, es decir, explícitamente disminuiría la oferta de dólares para inducir una depreciación del tipo de cambio, una situación inédita.

Nuestro rating

- 2.257.405 lecturas (la mayoría de clones) no pueden estar equivocadas

La Columna en tu e-mail

Recibe las actualizaciones de **La Columna por Correo-e**

Protagonistas y protagonismos

5 de julio A/H1N1 Alfredo García Arteaga Andrés Manuel López Obrador Banco de México Carlos Ahumada Carlos Salinas de Gortari Carmen Aristegui cepa H1N1 Chihuahua Clara Brugada Cámara de Diputados derecho de réplica DF Eduardo Bours Encuestas Enrique Peña Nieto Estado de México Felipe Calderón Fernando Elizondo Fidel Herrera Fútbol Germán Martínez guardería ABC Hermosillo Hidalgo IFE influenza influenza estacional

BANCO DE MÉXICO

Referencia 5

DOF: 02/03/2012

CIRCULAR 5/2012 dirigida a las Instituciones de Crédito, Casas de Bolsa, Sociedades de Inversión, Sociedades de Inversión Especializadas de Fondos para el Retiro y a la Financiera Rural, relativa a las Subastas para la Colocación de Valores Gubernamentales y de Valores del IPAB.

Al margen un logotipo, que dice: Banco de México.

CIRCULAR 5/2012

A LAS INSTITUCIONES DE CREDITO, CASAS DE BOLSA, SOCIEDADES DE INVERSION, SOCIEDADES DE INVERSION ESPECIALIZADAS DE FONDOS PARA EL RETIRO Y A LA FINANCIERA RURAL:

ASUNTO: **SUBASTAS PARA LA COLOCACION DE VALORES GUBERNAMENTALES Y DE VALORES DEL IPAB**

El Banco de México, en su carácter de agente financiero del Gobierno Federal de los Estados Unidos Mexicanos y del Instituto para la Protección al Ahorro Bancario (IPAB), con el propósito de continuar promoviendo el sano desarrollo del sistema financiero considera conveniente uniformar y compilar en un solo ordenamiento la regulación relativa a las subastas para la colocación de valores gubernamentales y de valores del IPAB, aplicable a las instituciones de crédito y a la Financiera Rural, así como a las casas de bolsa, sociedades de inversión y sociedades de inversión especializadas de fondos para el retiro, contenida actualmente, entre otras disposiciones, en el Anexo 6 de la Circular 2019/95, dirigida a las instituciones de banca múltiple, en el Anexo 3 de la Circular 1/2000, dirigida a las instituciones de banca de desarrollo y a la Financiera Rural, en los Apéndices 1 y 2 del Anexo 3 de la Circular 115/2002, dirigida a las casas de bolsa, y en la Circular 2/2002, dirigida a las sociedades de inversión y sociedades de inversión especializadas de fondos para el retiro.

Adicionalmente, para facilitar la consulta de la Circular se incluyen títulos para cada uno de los artículos con la intención de que sirvan como guía para la pronta identificación de su contenido, no obstante que tales títulos no forman parte de los artículos.

Por lo anterior, con fundamento en los artículos 28 de la Constitución Política de los Estados Unidos Mexicanos, párrafos sexto y séptimo; 3o. fracción II, 7o. fracción I, 8o., 10, 14 y 24 de la Ley del Banco de México; 9o. de la Ley Orgánica de Nacional Financiera; 6o. de la Ley Orgánica de Sociedad Hipotecaria Federal; 9o. de la Ley Orgánica del Banco del Ahorro Nacional y Servicios Financieros; 9o. de la Ley Orgánica del Banco Nacional de Comercio Exterior; 10 de la Ley Orgánica del Banco Nacional de Obras y Servicios Públicos; 8o. de la Ley Orgánica del Banco Nacional del Ejército, Fuerza Aérea y Armada; 18 y 19 de la Ley Orgánica de la Financiera Rural; 2o. de la Ley de Ingresos de la Federación para el Ejercicio Fiscal de 2012; 22 de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros; 4o. párrafo primero, 8o. párrafos cuarto y séptimo, 10 párrafo primero, 12 párrafo primero en relación con el 19 fracciones II y VII, y 14 Bis párrafo primero en relación con el 17 fracción I del Reglamento Interior del Banco de México, que le otorgan la atribución de expedir disposiciones a través de la Dirección General de Operaciones de Banca Central y de la Dirección General Jurídica, respectivamente, así como en el artículo Segundo fracciones VII y XI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, ha resuelto expedir las siguientes

REGLAS DE LAS SUBASTAS PARA LA COLOCACION DE VALORES GUBERNAMENTALES Y DE VALORES DEL IPAB

CAPITULO I

DISPOSICIONES PRELIMINARES

Definiciones

Artículo 1o.- Para fines de brevedad, en singular o plural, en estas Reglas se entenderá por:

Banco:	al Banco de México, actuando en su carácter de agente financiero.
BONDES:	a los Bonos de Desarrollo del Gobierno Federal de los Estados Unidos Mexicanos, denominados en moneda nacional y en UDIS, tanto a tasa de interés fija como a tasa de interés variable.
CETES:	a los Certificados de la Tesorería de la Federación emitidos por el Gobierno Federal de los Estados Unidos Mexicanos.
Días Hábiles Bancarios:	a los días en que las entidades financieras no estén obligadas a cerrar sus puertas ni a suspender operaciones, en términos de las disposiciones de carácter general que, para tal efecto, emite la Comisión Nacional Bancaria y de Valores.
IPAB:	al Instituto para la Protección al Ahorro Bancario.
SIAC-BANXICO:	al Sistema de Atención a Cuentahabientes de Banco de México.
UDIS:	a las unidades de cuenta cuyo valor en moneda nacional publica el

BANCO DE MÉXICO

Referencia 6

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

Order Code RL32331

CRS Report for Congress
Received through the CRS Web

The Economic Impact of Cyber-Attacks

April 1, 2004

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

Forbes
(/)

Portada (Https://Www.Forbes.Com.Mx/) / Últimas Noticias (Https://Www.Forbes.Com.Mx/_ultimas-Noticias_/) /

Javier Arreola (https://www.forbes.com.mx/author/javier-arreola/)

Ciberseguridad (casi) a prueba del enemigo 'invisible'

Ni las compañías más grandes del mundo ni los gobiernos han podido evitar los ataques cibernéticos, y aun así es posible que tengas una ciberseguridad casi al 100% si sigues las recomendaciones de los expertos.

Donald Rumsfeld, ex secretario de Defensa de Estados Unidos, quiso decir –en una famosa conferencia de prensa– que hay riesgos altos y riesgos bajos, y que hay riesgos que se ven y otros que no se ven. (Graham, 2014) Pero al combinar estos conceptos encontramos un cuadrante muy útil para tratar los temas de seguridad.

Por ejemplo, las personas saben que dejar abierta la puerta de su casa es un riesgo alto y visible. También podemos encontrar riesgos bajos que aún alcanzamos a ver, como la posibilidad de cruzar la calle cuando el semáforo está en rojo y que un vehículo "se lo pase" y te atropelle. Y hay riesgos bajos que no alcanzamos a ver, como que te roben la cartera en un lugar público y que al llegar a tu casa la busques y concluyas que la perdiste.

Sin embargo, los riesgos altos que no alcanzamos a ver son el tema de este artículo. Por ejemplo, la posibilidad de que alguien entre a tu casa, extraiga algo que tengas guardado, y salga de ella sin que te des cuenta. En temas cibernéticos, esto es más común de lo que parece: hackers entran a tu correo, cibercriminales que

MÁS COBERTURA

Equipo de López Obrador presenta la segunda parte de Pejenomics (https://www.forbes.com.mx/equip de-lopez-obrador-presenta-la-segunda-parte-de-pejenomics/)

ONU condena uso excesivo de la fuerza de Israel contra palestinos (https://www.forbes.com.mx/onu-condena-uso-excesivo-de-la-fuerza-de-israel-contra-palestinos/)

SCJN otorga amparo a Ríos Piter para consumo recreativo de mariguana (https://www.forbes.com.mx/scjn-otorga-amparo-a-rios-piter-para-consumo-recreativo-de-mariguana/)

REFERENCIA 9

Informe Norton sobre Ciberseguridad 2016

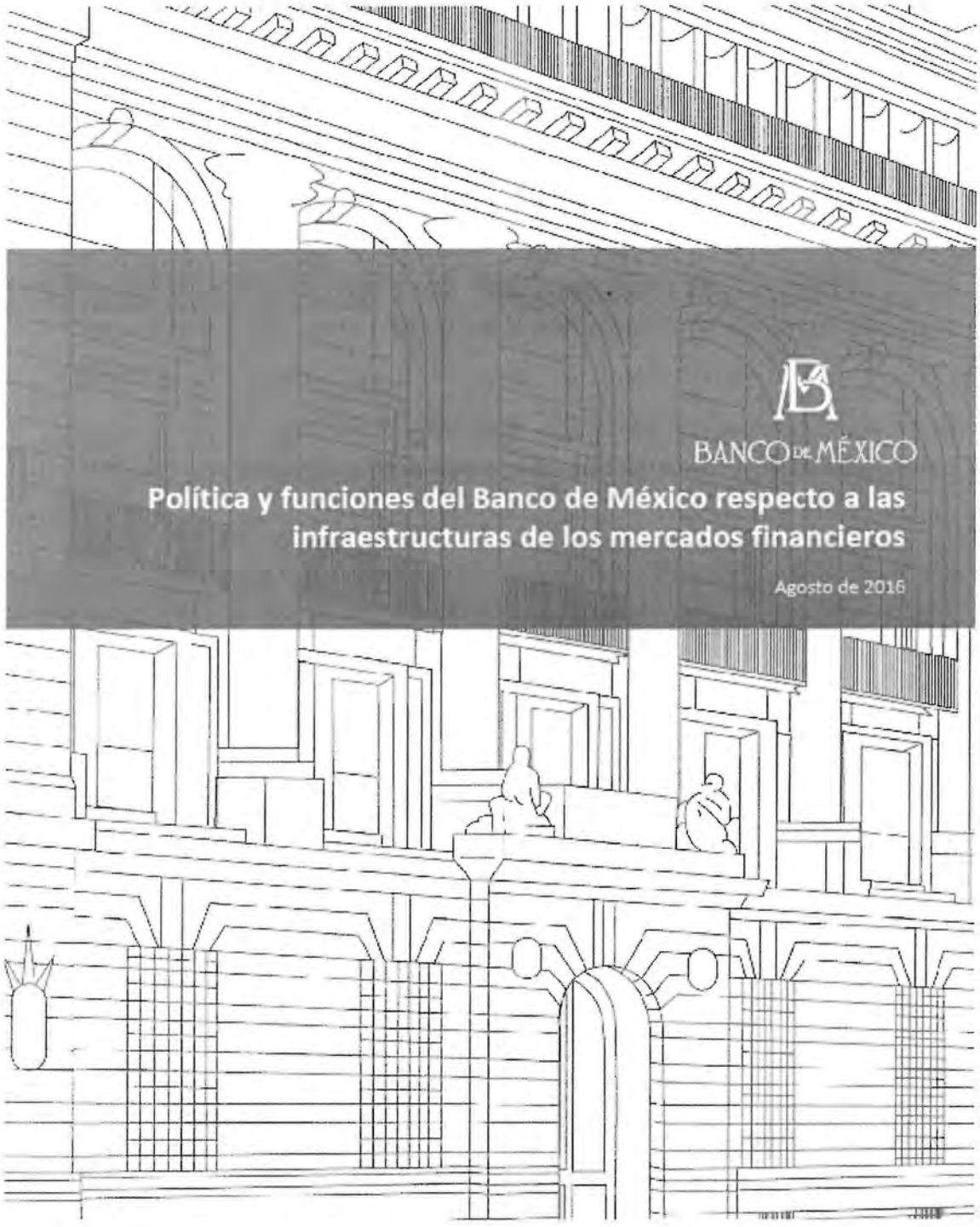
Comparaciones Globales

PRINCIPALES CONCLUSIONES	MÉXICO	GLOBAL (24 países)
Total de consumidores afectados por el cibercrimen en el último año	**22.4 millones (45%)**	689.4 millones (31%)
Total de costos financieros causados por el cibercrimen en el último año	**$5,500 millones (USD)**	$125,900 millones (USD)
Total de tiempo perdido por el cibercrimen en el último año	**28.8 horas**	19.7 horas
Los crímenes cibernéticos más comunes que han experimentado los consumidores	**Robo de dispositivo móvil: 33% Robo de contraseña:26% Correo electrónico hackeado: 20%**	Robo de contraseña: 18% Correo electrónico hackeado: 16% Robo de dispositivo móvil: 15%
Porcentaje de usuarios que no pueden identificar un correo electrónico "phishing" o suponen que es legítimo	**30%**	41%
Porcentaje de usuarios que han experimentado una consecuencia negativa después de responder a un correo electrónico "phishing"	**68%**	80%
Porcentaje de personas que se consideran capaces de determinar si usan una red de Wi-Fi segura	**61%**	48%
Dispositivo doméstico con mayor probabilidad de ser protegido por los encuestados	**Sistema de seguridad en casa: 79%**	Sistema de seguridad en casa: 76%
Porcentaje que piensa que los dispositivos domésticos conectados ofrecen a los hackers nuevas formas de robar datos	**71%**	72%
Porcentaje de personas que piensan que los dispositivos domésticos conectados están diseñados considerando la seguridad	**64%**	62%
Porcentaje con al menos un dispositivo no protegido	**39%**	35%
Porcentaje que confía en su capacidad para mantener segura la información personal en línea	**43%**	40%
Porcentaje que cree que es más difícil mantenerse a salvo y seguro en línea en los últimos 5 años	**65%**	63%
Porcentaje de padres que creen que sus hijos son más propensos a ser intimidados en línea que en un patio de recreo	**48%**	48%
Porcentaje que cree que los niños están expuestos a más peligros en línea ahora que hace 5 años	**86%**	78%

Norton

BANCO DE MÉXICO

REFERENCIA 10



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

(http://

Informe Semanal del Vocero

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

Informe Semanal del Vocero

Autor
Secretaría de Hacienda y Crédito Público

Fecha de publicación
29 de octubre de 2017

Categoría
Comunicado

BadCyber

Making infosec journalism great again!

Several Polish banks hacked, information stolen by unknown attackers

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

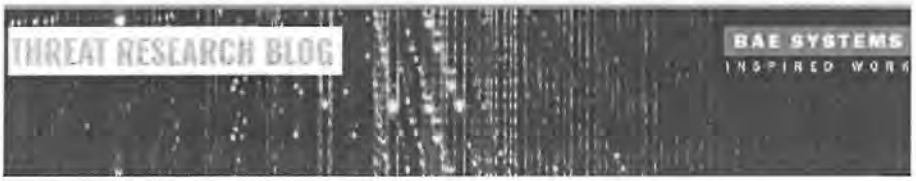
241 Share Tweet

REFERENCIA 13

Más

BAE SYSTEMS THREAT RESEARCH BLOG

Home Products Solutions News & Events Partners About Us Careers



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.

POPULAR POSTS


TWO BYTES TO $953N


RANSOMWARE


CYBER HEIST ATTRIBUTION

CONTACT

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

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

Article · World Neurosurgery · June 2017

CITATION
1

READS
142

1 author:

Eastern Maine Medical Center

164 PUBLICATIONS 604 CITATIONS

SEE PROFILE

REFERENCIA 15

Descubren que Petya, el ataque que paralizó empresas de toda Europa, no secuestraba archivos sino que los borraba

Eduardo Marín
6/28/17 3:17pm •

Imagen: Björn Olsson, bajo licencia Creative Commons.

Un nuevo ataque de ransomware, conocido como Petya, hizo que se paralizaran las actividades en un gran número de oficinas de compañías importantes en Europa, incluyendo aerolíneas, bancos y bufetes de abogados. Sin embargo, un nuevo análisis asegura que este ataque era mucho peor de lo que imaginamos.

BANCO DE MÉXICO

REFERENCIA 16

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.

Telefono de Comunicación Social: 15551024

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

NENA News, Press, & Stories...: Home Page

Email to a Friend (/members/send.aspx?in=119592)

DHS Bulletin on Denial of Service (TDoS) Attacks on PSAPs

Sunday, March 17, 2013 (0 Comments)
Posted by: Chris Nussman

Share (https://www.addthis.com/bookmark.php?v=250&pub=yourmembership) |

The Department of Homeland Security (DHS) NCCIC - National Coordinating Center for Communications – the DHS Office of Emergency Communications, DHS - Office of Infrastructure Protection, Federal Communications Commission, the National Cyber and Forensics Training Alliance, the FBI-National Cyber Investigative Joint Task Force working in coordination with the National Emergency Number Association (NENA), the Association of Public Safety Communications Officials (APCO) International, Louisiana Fusion Center, Mansfield Police Department and telecommunications service providers to identify and mitigate the effects of a criminal Telephony Denial of Service (TDoS) against public safety communications, hospitals and ambulance services. This is for immediate dissemination to public safety answering points (PSAPs) and emergency communications centers and personnel.

Background: Information received from multiple jurisdictions indicates the possibility of attacks targeting the telephone systems of public sector entities. Dozens of such attacks have targeted the administrative PSAP lines (not the 911 emergency line). The perpetrators of the attack have launched high volume of calls against the target network, tying up the system from receiving legitimate calls. This type of attack is referred to as a TDoS or Telephony Denial of Service attack. These attacks are ongoing. Many similar attacks have occurred targeting various businesses and public entities, including the financial sector and other public emergency operations interests, including air ambulance, ambulance and hospital communications.

COBALT: EL CIBERCRIMEN ORGANIZADO GOLPEA LOS CAJEROS AUTOMÁTICOS EUROPEOS

By S21sec Posted 2016/11/23 In Ciberseguridad

El malware en cajeros automáticos (ATMs) es un asunto de gran actualidad y que genera una gran preocupación en el sector bancario. El número de ataques está creciendo muy rápidamente y **está afectando a toda clase de países y regiones.**

En julio de 2016, los cibercriminales consiguieron extraer un total de **2 millones de dólares** de 34 cajeros automáticos del banco taiwanés First Bank. En agosto de 2016, consiguieron atacar el banco estatal tailandés Government Savings Bank, permitiendo así a los cibercriminales hacerse con un botín de **350.000 dólares** en metálico y forzando al banco a desactivar **3300 cajeros** automáticos, o lo que es lo mismo, cerca de la mitad de su red. Tal y como ya anticipamos en un post anterior, era altamente probable que estos ataques se extendiesen a otros países y regiones, y ahora le ha tocado el **turno a Europa**.

Revista de Ciencias de Seguridad y Defensa (Vol. 1, No. 2, 2016)

EL CIBERESPACIO: EL NUEVO TEATRO DE GUERRA GLOBAL

Luis Recalde H.,
Universidad de las Fuerzas Armadas - ESPE

Resumen

Finalizada o controlada la tradicional guerra convencional, el mundo tiene un nuevo teatro de operaciones llamado ciberespacio. De allí se han desprendido diversos ataques que traspasaron las fronteras virtuales; así, la tecnología de vanguardia ha formulado el nuevo campo de batalla global, desarrollado por los nuevos sistemas cibernéticos.

Palabras clave: ciberespacio, fronteras virtuales, espacio tridimensional, ciberguerras

Introducción

El teatro de guerra es una zona del globo terráqueo relativamente extensa, compuesta por los espacios terrestres, marítimos y aéreos que están - o estarían - potencialmente implicados en operaciones de guerra. Bajo esta perspectiva, estaríamos hablando de una determinada zona geográfica "tangible" de la tierra compuesta por los dominios tridimensionales de las operaciones militares convencionales, y que puede estar involucrada en una acción bélica determinada.

Hace algunos siglos, cuando se comenzaron a estudiar las guerras, generalmente se analizaban las formas de enfrentamientos básicos, por ejemplo la falange griega o la romana, éstas se enfocaban en el empleo táctico de las fuerzas en un determinado teatro de operaciones, hasta que Jomini (1838) pensó que, siguiendo una serie de leyes, un contingente militar podría estar en condiciones de vencer más fácilmente. Estas leyes se referían no solo al enfrentamiento y al combate en sí (es decir, la táctica de la que todos se habían ocupado hasta ese entonces), sino también a la maniobra de aproximación y retirada y a la logística de sostenimiento de las operaciones. A la combinación sincronizada en el terreno de estos aspectos previos al hecho táctico se lo conoce hoy como el "arte operacional" (Vergara, 2003).

Mientras Clausewitz (1831), concebía que la guerra era demasiado compleja, impredecible y un arte muy especial, porque se ejercía sobre elementos que reaccionan en función de su empleo y conducción. Pero lo más importante es que quería probar la naturaleza fundamental de la guerra y su lugar en el espectro de la actividad humana, por lo que la guerra fue orientada a una sistematización en el pensamiento de la conducción militar que, para una mejor interpretación, la guerra podía definirse en tres niveles:

- El que fijaba las causas por las que se debía ir a la guerra, al que llamaron nivel estratégico
- El que entendía los movimientos (maniobras) y la logística de las tropas en el terreno, al que llamaron nivel operacional
- El de los enfrentamientos en sí, al que llamaron nivel táctico (Vergara, 2003).

Por lo tanto en la guerra tradicionalmente visualizada, las fuerzas militares beligerantes emplean sus medios en un espacio tridimensional definido (aire, mar y tierra), y que es uno de los elementos decisivos para la consecución de un objetivo preestablecido en el nivel estratégico militar.

DELTA

MY TRIPS BOOK A TRIP FLIGHT STATUS CHECK IN

INFORMATION ON [24]7.AI CYBER INCIDENT

OVERVIEW

Last updated on April 7, 2018 at 9:00 ET

Last week, on March 28, Delta was notified by [24]7.ai, a company that provides online chat services for Delta and many other companies, that [24]7.ai had been involved in a cyber incident. It is our understanding that the incident occurred at [24]7.ai from Sept. 26 to Oct. 12, 2017 and that during this time certain customer payment information for [24]7.ai clients, including Delta, may have been accessed – no other customer personal information, such as passport, government ID, security or SkyMiles information was impacted. Delta customers who believe they could be impacted, should visit https://delta.arkadium.com to enroll in the free protection services being offered.

Upon being notified of [24]7.ai's incident last week, Delta immediately began working with [24]7.ai to understand any potential impact the incident had on Delta customers, delta.com, or any Delta computer system. We also engaged federal law enforcement and forensic teams, and have confirmed that the incident was resolved by [24]7.ai last October. At this point, even though only a small subset of our customers would have been accessed, we cannot say definitively whether any of our customers' information was actually accessed or subsequently compromised.

We appreciate and understand that this information is concerning to our customers. The security and confidentiality of our customers' information is of critical importance to us and a responsibility we take extremely seriously. We will be updating http://www.delta.com/response regularly to address customer questions and concerns. We will also be directly contacting customers who may have been impacted by the [24]7.ai cyber incident. In the event any of our customers' payment cards were used fraudulently as a result of the [24]7.ai cyber incident, we will ensure our customers are not responsible for that activity.

• Click to enlarge

FREQUENTLY ASKED QUESTIONS

1. How did [24]7.ai's cyber incident occur?
   - [24]7.ai is a company that provides online chat services for many companies, including Delta.
   - We understand malware present in [24]7.ai's software between Sept. 26 and Oct. 12, 2017, made unauthorized access possible for the following fields of information when manually completing a payment card purchase on any page of the delta.com desktop platform during the same timeframe: name, address, payment card number, CVV number, and expiration date.
   - *All other customer personal information, such as passport, government ID, security or SkyMiles information was impacted.*
2. What customers were impacted?
   - At this point, we understand that the malware was present for a short period of time and potentially exposed several hundred thousand customers.
   - While we believe we have identified with some precision the transactions that could have been impacted, we cannot say definitively whether any of our customers' information was actually accessed or subsequently compromised.
   - There was no impact to the fly.Delta app, mobile.delta.com or any other Delta computer system. Payment card information for those customers who used Delta Wallet to complete transactions was not compromised. The malware could only collect the information shown on the screen, so credit card information automatically populated by Delta Wallet functionality would have remained masked and not useable.
   - Customers did not have to interact with the online chat tool to be impacted.
3. What is Delta doing to make this right for customers?
   - Delta launched www.delta.com/response, a dedicated website, on April 5 at noon ET, which we will be updating regularly to address customer questions and concerns.
   - Delta will be working diligently to directly contact customers, including by first-class postal mail, who may have been impacted by the [24]7.ai cyber incident.

Technology

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

By Michael Riley and Alan Katz
26 de mayo de 2016 8:36 GMT-5
Updated on 26 de mayo de 2016 15:21 GMT-5

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

Swift Hack Investigation Expands to Southeast Asia

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

Recuadro 7

RIESGO CIBERNÉTICO: RELEVANCIA Y ENFOQUES PARA SU REGULACIÓN Y SUPERVISIÓN

Felipe Clavijo Ramírez
Daniel Osorio
Eduardo Yanquen*

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

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

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

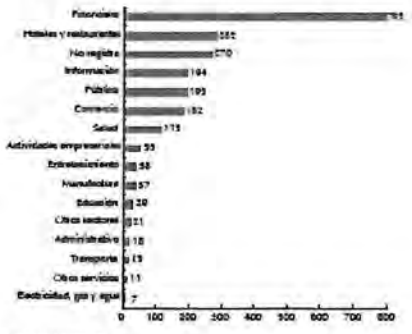
La forma más común como se ha materializado el riesgo cibernético en años recientes ha sido mediante lo que se conoce como ataques cibernéticos. En esencia, estos son acciones ilegales realizadas por *hackers*, con el objetivo principal de obtener cierto beneficio, al generar daños en los sistemas tecnológicos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

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

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

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

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



Fuente: Verizon (2016).

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

News

Symantec reveals more hack attempts on Swift network

Written by Antony Peyton (https://www.bankingtech.com/author/antonypeyton/) 11 Oct 2016

Symantec has found evidence that the Odinaff group has mounted attacks on Swift users, using malware to hide customers' own records of Swift messages relating to fraudulent transactions.

The tools used are designed to monitor customers' local message logs for keywords relating to certain transactions. They will then move these logs out of customers' local Swift software environment. Symantec says it has no indication that Swift network was itself compromised.

(https://www.bankingtech.com/file 1.png)
Odinaff attacks by region (IMAGE: Symantec) Click to enlarge

Symantec says these Odinaff attacks are an example of another group believed to be involved in this kind of activity, following the Bangladesh central bank heist (https://www.bankingtech.com/455732/typo-spells-confusion-in-101m-cyber-bank-heist/) linked to the Lazarus group.

There are no apparent links between Odinaff's attacks and the attacks on banks' Swift environments attributed to Lazarus and the Swift-related malware used by the Odinaff group bears no resemblance to Trojan.Banswift, the malware used in the Lazarus-linked attacks.

But Symantec notes that the attacks involving Odinaff share some links to the Carbanak group, whose activities became public in late 2014. Carbanak also specialises in high-value attacks against financial institutions and has been implicated in a string of attacks against banks in addition to point of sale (PoS) intrusions.

This is bad news for Swift but its fight back against these attacks has been extensive and ongoing. It has spoken strongly (https://www.bankingtech.com/595372/swift-issues-plea-to-collaborate-in-fight-against-cybercrime/) on the subject and recently unveiled SwiftSmart (https://www.bankingtech.com/602332/swift-smart-modules-seek-stronger-security/) modules to help its customers operate their Swift environment "securely and in-line with best practice". This move is also a "critical part" of its Customer Security Programme

BANCO DE MÉXICO

REFERENCIA 24

BANCO DE MÉXICO

REFERENCIA 25

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 extraido 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.**

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

+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/1236241)

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 28

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.

BANCO DE MÉXICO

REFERENCIA 29

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real.

Fecha de consulta: 26/09/2018 12:59:39

Título	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios SPEI®, Número de operaciones	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios SPEI®, Importe (millones de pesos)
Periodo disponible	Ene 1992 - Ago 2018	Ene 1992 - Ago 2018
Periodicidad	Mensual	Mensual
Cifra	Volumen	Flujos
Unidad	Operaciones	Millones de Pesos
Base		
Aviso		
Tipo de información	Niveles	Niveles
Fecha	SF46188	SF46189
Ene 2017	35,016,703	23,877,271
Feb 2017	34,817,472	21,505,024
Mar 2017	40,016,546	26,180,217
Abr 2017	35,954,794	20,494,020
May 2017	37,831,714	21,984,690
Jun 2017	43,806,037	23,093,365
Jul 2017	35,242,331	21,576,446
Ago 2017	42,207,091	22,005,722
Sep 2017	42,473,998	21,881,177
Oct 2017	40,172,877	22,509,386
Nov 2017	43,888,894	21,719,416
Dic 2017	48,576,208	23,658,129
Ene 2018	43,696,159	24,177,775
Feb 2018	43,392,790	20,965,410
Mar 2018	46,956,342	23,580,617
Abr 2018	49,608,372	23,993,595
May 2018	46,106,472	22,005,913
Jun 2018	53,607,479	23,215,548
Jul 2018	46,293,171	21,428,148
Ago 2018	56,288,104	22,102,662

BANCO DE MÉXICO

Ciudad de México, a 16 de noviembre de 2018.

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

Nos referimos a la solicitud de acceso a la información identificada con el número de folio **6110000057718,** que nos turnó la Unidad de Transparencia el dieciséis de octubre del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

> *"Necesito de todos los servidores públicos los registros de las llamas recibidas y realizadas del mes de septiembre a la fecha, y en caso de grabarlas las de las última semana a la fecha de la presentación de esta solicitud, desde luego de linea oficial asignada."*

Al respecto, nos permitimos informarles que, en términos de lo dispuesto por los artículos 100 y 106, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública; así como 97 y 98, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, estas unidades administrativas han determinado clasificar la información relativa a la totalidad de **las grabaciones de las llamadas realizadas o recibidas a través de las Extensiones Telefónicas Seleccionadas, del personal de la Dirección de Operaciones Internacionales, de la Dirección de Operaciones Nacionales y de la Dirección de Sistemas de Pagos,** en términos de los siguientes fundamentos y motivos:

1. INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL

Conforme a la disposición Sexta de la Norma Administrativa Interna "Administración del sistema de seguimiento de extensiones telefónicas" (NAI), las Extensiones Telefónicas Seleccionadas (ETS) serán aquellas extensiones que se ubiquen en las instalaciones del Banco, destinadas a hacer y recibir llamadas para:

a. La negociación, concertación, celebración, conciliación, trámite, formalización o ejecución de actos u operaciones, cuyo registro y conservación sean necesarios para acreditar y, en su caso revisar, los términos y condiciones en que fueron realizadas.

b. Reportar emergencias o hechos que deban ser atendidos con urgencia, relacionados con temas de protección civil y seguridad interna en las instalaciones del "Banco".

Por su parte, la disposición Quinta, de la NAI en comento, señala que la grabación de las llamadas realizadas o recibidas a través de las ETS, así como la consulta de dichas

grabaciones, son parte de las operaciones del Sistema de Seguimiento de Extensiones Telefónicas (SSET).

Asimismo, la disposición Décima de la NAI referida señala que las actividades de supervisión de la correcta operación de la infraestructura del SSET, se realizarán **sin consultar las grabaciones de las llamadas.**

La Décima cuarta disposición de la citada NAI, señala que la consulta de las grabaciones podrá realizarse tanto por los titulares de la Dirección General de Emisión, de la Dirección General de Operaciones y Sistemas de Pagos y la Coordinación Administrativa del Fondo Mexicano del Petróleo para la Estabilización y el Desarrollo, así como por los trabajadores especificados en la solicitud de la consulta. En relación con lo anterior, la disposición Décima quinta de la citada NAI, establece que serán los titulares de las unidades administrativas señaladas, los responsables del uso adecuado de la información obtenida a través de las grabaciones de las llamadas; y que la Dirección General de Tecnologías de la Información (DGTI) será responsable del debido resguardo de dicha información.

En adición a lo anterior, la disposición Décimo sexta de la NAI en comento, señala que las unidades administrativas referidas en el párrafo precedente, deberán salvaguardar el derecho a la **intimidad o privacidad** de las personas que intervengan en las conversaciones grabadas.

De conformidad con lo dispuesto en los artículos 116, párrafos primero y cuarto, de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracciones I y III, de la Ley Federal de Transparencia y Acceso a la Información Pública: Trigésimo octavo, fracciones I y II, y Cuadragésimo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, es confidencial la información que contenga datos personales concernientes a una persona identificada o identificable, así como aquella que los particulares presenten a los sujetos obligados, siempre que tengan derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales, respectivamente.

En este sentido se hace notar la **confidencialidad** de las grabaciones de las llamadas realizadas y recibidas por los trabajadores de la Dirección de Operaciones Nacionales, la Dirección de Operaciones Internacionales, y la Dirección de Sistemas de Pagos, a través de las ETS, en virtud de los datos personales que pudieran contener dichas llamadas, así como la información que comprenda hechos y actos de carácter económico, contable, jurídico o administrativo relativos a una persona, que pudiera ser útil para un competidor, información de la cual son titulares los interlocutores con quienes interactúan los servidores públicos adscritos a las unidades administrativas descritas.

En efecto, las llamadas que reciben o efectúan los servidores públicos de las unidades administrativas en cuestión, a través de las extensiones destinadas para los fines descritos en el inciso a. disposición Sexta de la NAI, pueden contender datos personales, así como información que comprende hechos y actos de carácter económico, contable, jurídico o administrativo relativos a una persona, que pudiera ser útil para un competidor, mismos que no pueden ser disociados de las grabaciones de llamadas telefónicas en los formatos en que se encuentran.

Lo anterior, máxime que la autodeterminación informativa de los titulares de la información contenida en las llamadas telefónicas grabadas en virtud de la NAI, no se pierde en función de la naturaleza y características del equipo telefónico del que recibieron las llamadas en su momento, ni porque en las mismas intervengan servidores públicos.

En ese sentido, se observa una imposibilidad para los sujetos obligados de identificar y disociar el contenido en concreto de las llamadas telefónicas en cuestión que tenga el carácter de público y cuál debe ser protegido.

En adición a lo anterior, considerando que la fecha de ingreso de la misma fue el dieciséis de octubre del presente año, y que las grabaciones de las llamadas requeridas, corresponden al periodo del 8 al 16 de octubre del presente año, y tienen una duración en total, de 185.78 horas. En tal sentido, resulta evidente que existe una incapacidad material y técnica para la revisión de cada una de las llamadas para determinar su naturaleza, así como para la elaboración de versiones públicas en virtud del formato en que se encuentra la información solicitada.

Atento a lo expuesto, fundado y motivado, estas unidades administrativas determinan clasificar como **confidencial** la información relativa a la totalidad de **las grabaciones de las llamadas realizadas o recibidas a través de las Extensiones Telefónicas Seleccionadas, del personal de la Dirección de Operaciones Internacionales, de la Dirección de Operaciones Nacionales y de la Dirección de Sistemas de Pagos.**

2. INFORMACIÓN CLASIFICADA COMO RESERVADA

Se debe señalar que la Dirección de Operaciones Nacionales, de la Dirección de Operaciones Internacionales y de la Dirección de Sistemas de Pagos, tienen entre sus atribuciones las de concertar y formalizar las operaciones del Banco relacionadas con divisas, oro, plata y valores referidos a monedas extranjeras, así como las garantías vinculadas con dichas operaciones; concertar y formalizar las operaciones financieras del Banco relacionadas con moneda nacional, divisas frente a dicha moneda y valores referidos a la moneda nacional, así como las garantías vinculadas con dichas operaciones; así como concertar, ejecutar y dar seguimiento a las operaciones de los participantes en los Sistemas de Pagos

administrados por el Banco respectivamente, es en el ejercicio de estas atribuciones que se graban las extensiones de todo el personal a cargo de éstas.

En ese sentido, y en virtud de la imposibilidad de identificar y disociar el contenido en concreto de las llamadas telefónicas en cuestión que tenga el carácter de público y cuál debe ser protegido, a efecto de determinar la naturaleza de dichas llamadas, estas unidades administrativas determinan clasificar como **reservada** la información relativa a la totalidad de **las grabaciones de las llamadas realizadas a través de las Extensiones Telefónicas Seleccionadas, del personal de la Dirección de Operaciones Internacionales, de la Dirección de Operaciones Nacionales y de la Dirección de Sistemas de Pagos,** en términos de la fundamentación y motivación expuestos en la prueba de daño que se adjunta al presente oficio.

Quedamos a sus órdenes, para cualquier aclaración o comentario adicional.

Atentamente,

Gerardo I García L

LIC. GERARDO ISRAEL GARCÍA LÓPEZ
Director de Operaciones Internacionales

LIC. MAYTE RICO FERNÁNDEZ
Gerente de Operaciones Nacionales
En suplencia por ausencia del Director de Operaciones Nacionales
en términos del Art. 66 del Reglamento Interior del Banco de México

BANCO DE MÉXICO
RECIBIDO
Comité de Transparencia
Por: BI7327 Hora: 13:30
Recibo este oficio en cuatro páginas y una prueba de daño.

BANCO DE MÉXICO

PRUEBA DE DAÑO

GRABACIÓN DE LLAMADAS DE LA DIRECCIÓN GENERAL DE OPERACIONES Y SISTEMAS DE PAGOS

En términos de lo dispuesto en los artículos 6, apartado A, sexto párrafo, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 113, fracción IV, de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP); 110, fracción IV, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como Vigésimo segundo, fracciones I y II, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas (Lineamientos), es de clasificarse como información reservada aquella que:

- Menoscabe la efectividad de las medidas implementadas en los sistemas financiero o económico del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto;

- Ponga en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país;

- Comprometa las acciones encaminadas a proveer el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos; y

Se debe señalar que las Direcciones de Operaciones Nacionales, de Operaciones Internacionales y, de Sistemas de Pagos, tienen entre sus atribuciones las de concertar y formalizar las operaciones del Banco relacionadas con divisas, oro, plata y valores referidos a monedas extranjeras, así como las garantías vinculadas con dichas operaciones; concertar y formalizar las operaciones financieras del Banco relacionadas con moneda nacional, divisas frente a dicha moneda y valores referidos a la moneda nacional, así como las garantías vinculadas con dichas operaciones; así como concertar, ejecutar y dar seguimiento a las operaciones de los participantes en los Sistemas de Pagos administrados por el Banco respectivamente; es en el ejercicio de estas atribuciones que se graban las extensiones del personal a cargo de éstas sin distinguir si la llamada es privada o pública.

En este sentido, el dar a conocer el detalle de las llamadas del personal encargado del **análisis e instrumentación de las operaciones con propósitos de regulación monetaria**, representa un riesgo de perjuicio significativo al interés público en virtud de que dicho riesgo es:

1) **Real** ya que a través de llamadas telefónicas se intercambia información, opiniones, puntos de vista y percepciones de los participantes del sistema financiero sobre el comportamiento y condiciones de liquidez del mercado de dinero y de quienes en el intervienen, lo cual fuera de contexto, podría conducir a una lectura equivocada sobre la solidez de las instituciones

financieras que celebran operaciones de inyección de liquidez con este Instituto Central al entenderse, erróneamente, que dichas instituciones tienen problemas de liquidez lo que podría disminuir la confianza del público en éstas y por lo tanto generar un menor interés de las mismas en participar en las subastas de regulación monetaria y cualquier otro mecanismo implementado por el Banco de México en materia monetaria, lo que afectaría directamente la implementación de estas medidas.

2) **Demostrable** ya que existe gran sensibilidad tanto de inversionistas como del público en general a este tipo de información (la solvencia de las instituciones financieras) por lo que ante una incorrecta interpretación de la misma, los depositantes podrían cambiar sus inversiones de institución de crédito e incluso de país, generando con ello corridas financieras que perjudiquen a la institución de crédito en cuestión. Baste recordar la rapidez con la que es perdió la confianza en las instituciones financiera durante la crisis global que inició en 2007 en donde varios bancos alrededor del mundo presentaron corridas bancarias, entre ellos el banco británico Northern Rock[1].

3) **Identificable** ya que la pérdida de confianza en las instituciones de crédito puede afectar también a aquellas consideradas sistémicamente importantes, lo que incluso podría poner en riesgo el sano desarrollo del sistema financiero y la estabilidad financiera nacional en su conjunto. En efecto, durante la crisis financiera global de 2008, la quiebra del Banco Lehman Brothers generó una desconfianza masiva en el sistema financiero estadounidense que forzó a las autoridades financieras de dicho país a "nacionalizar" a los bancos considerados sistémicamente importantes para restaurar la confianza y mantener la estabilidad de dicho sistema.[2]

En el mismo contexto de las llamadas que se realizan para instrumentar la política monetaria, se encuentran las llamadas que se realizan para **instrumentar la política cambiaria.**

El Banco de México instrumenta la política cambiaria siguiendo las directrices que determina la Comisión de Cambios, integrada por Banco de México y la Secretaría de Hacienda y Crédito Público. Dicha Comisión mantiene una constante evaluación de los distintos factores económicos, políticos y sociales del país, así como de los fundamentos macroeconómicos, de los indicadores económicos y en particular de las condiciones de operación en el mercado cambiario nacional y de los mercados financieros globales para tomar sus decisiones.

---

[1] The Bank that failed, The economist, sep 20th 2007. https://www.economist.com/node/9832838 Consultado el 15 de noviembre

[2] Wall Street humiliated by nationalisation of banks, Independent, oct 14th 2008. https://www.independent.co.uk/news/business/news/wall-street-humiliated-by-nationalisation-of-banks-961397.html Consultado el 15 de noviembre

El dar a conocer el detalle de las llamadas del personal encargado del análisis e instrumentación de las operaciones cambiarias, representa un riesgo de perjuicio significativo al interés público en virtud de que dicho riesgo es:

1) **Real**, ya que a través de llamadas telefónicas se intercambia información, opiniones, puntos de vista y percepciones de los participantes en el mercado cambiario sobre el comportamiento y condiciones de liquidez de éste y de quienes en el intervienen, lo cual fuera de contexto podría generar percepciones erróneas en el público y propiciar que los agentes económicos o incluso las instituciones financieras tomen decisiones e implementen medidas inconvenientes para el mercado que redunden en un daño para la economía nacional y que, por otra parte y de manera fundamental, puedan afectar la efectividad de la medida en el futuro.

   Es importante destacar que en la práctica internacional la puesta a disposición del público de información y documentos relativos a las operaciones realizadas por los bancos centrales en el mercado cambiario atiende al objetivo que se busque con la propia intervención y al mensaje que los bancos centrales buscan dar a los participantes y al mercado cambiario en general. En ese sentido, la clasificación, o en su caso, la divulgación de información relativa a las operaciones efectuadas puede variar según los objetivos específicos.

   En ese sentido, la Comisión de Cambios está en posibilidad de implementar operaciones, cuya información sea clasificada, o en su caso, divulgada en el mercado cambiario, de manera acorde con la práctica internacional, a fin de lograr objetivos como corregir desalineamientos en el tipo de cambio, ordenar al mercado cambiario, acumular reservas internacionales, o bien, proveer al mercado de moneda extranjera, y que, tienen como fin último procurar la estabilidad del poder adquisitivo de la moneda nacional.

   Por tal motivo, al dar a conocer las grabaciones del personal que instrumenta éstas operaciones se pueden conocer detalles como el tipo de operación que se realizó, el nombre de las instituciones que están facultadas para operar con el Banco, cuánto puede comprar cada una, en donde residen, así como información que permita la identificación de tales operaciones, afectando de manera significativa las funciones propias de la Comisión de Cambios y del Banco Central y, disminuyendo la capacidad de éste para cumplir su finalidad constitucional de procurar la estabilidad de la moneda nacional. Lo anterior, con las correspondientes consecuencias negativas para el mercado cambiario y para la economía en general de nuestro país.

   Actualmente, a nivel internacional se reconoce como una práctica bancaria la discrecionalidad por parte de los bancos centrales para realizar operaciones en el mercado

cambiario y para determinar la clasificación, o en su caso, la divulgación de la información relativa a las operaciones que en esta materia realiza, así como diversos aspectos de las mismas. Adicionalmente, se reconoce que no obstante que los bancos centrales informen sobre sus operaciones en el mercado ello no significa que deban revelar sus estrategias de mercado u otra información que pueda generar oportunidades para que los participantes obtengan ganancias sin riesgo y que puedan utilizar en su beneficio, pudiendo perjudicar la eficacia de las medidas que en el futuro los bancos centrales requieran adoptar en materia cambiaria.

En ese mismo sentido, diversos autores que han abordado el tema de la divulgación al público de los detalles de las operaciones realizadas por los bancos centrales en el mercado cambiario, señalan que existen razones en virtud de la propia operación del mercado cambiario que justifican que el público no tenga conocimiento respecto de todos los detalles de las operaciones cambiarias realizadas por los bancos centrales. Una de las principales razones que señalan tales autores es la situación estratégica que los bancos centrales tienen dentro de las economías de sus respectivos países, reconociendo que existen algunas operaciones que no son susceptibles de divulgarse al público.

En línea con la práctica bancaria a nivel internacional, la Comisión de Cambios, a través de Banco de México, ha hecho del conocimiento del público información sobre las operaciones realizadas en el mercado cambiario mediante la publicación de comunicados de prensa o reportes financieros, en determinadas ocasiones que así lo ameritan, para conseguir objetivos de política cambiaria, o bien, en los informes anuales del Banco Central.

En ese sentido, publicar las grabaciones de las llamadas que realiza el personal que instrumenta las operaciones cambiarias implica obligar al Banco Central a actuar de manera contraria a la práctica bancaria internacional con los consecuentes efectos negativos que ello podría generar al propio Banco Central, a los mecanismos de intervención cambiaria, y finalmente, de manera preponderante, al valor adquisitivo de la moneda, obligación constitucional a la que esta Institución debe dar cabal cumplimiento.

2) **Demostrable**, pues considerando las circunstancias propias de nuestro país, el grado de cultura en materia económica y financiera, la influencia de los medios de comunicación, los diferentes intereses económicos, políticos y sociales involucrados, así como el grado de desarrollo de nuestro sistema financiero, reprivatizado hace pocas décadas y cuya composición, aunque ha evolucionado, es muy similar a través de los años, junto con otros factores, la Comisión de Cambios ha determinado no divulgar los detalles de las operaciones cambiarias como los contenidos en las grabaciones que realiza el personal que las instrumenta, previendo los posibles daños que ello podría conllevar a la población mexicana en su conjunto.

Ejemplo de lo mencionado en el párrafo anterior es el estigma que se asocia a los participantes en las operaciones cambiarias. No es extraña la publicación de artículos periodísticos en los que se califica negativamente a instituciones financieras que participaron en operaciones cambiarias realizadas por este instituto central décadas antes. Como muestra podemos mencionar el artículo publicado el 18 de abril de 2008 en el periódico La Jornada titulado "México SA"[3] o el publicado el 27 de marzo de 2009 en el periódico El País titulado "La Crisis Mexicana ahora sí parece crisis"[4] que dan fe del daño que, incluso años después de realizada la operación cambiaria de compraventa de dólares de 1994, puede provocarse con la publicación de cierta información sensible sobre mecanismos de política cambiaria implementados por la Comisión de Cambios y contenida en las grabaciones del personal que instrumenta dichas operaciones.

Lo anterior podría generar que las instituciones perdieran interés en participar en las operaciones cambiarias, al saber que su nombre así como el detalle de sus operaciones y puntos de vista llegarían a ser públicos y considerando las afectaciones que ello pudiera acarrearles. Más aún, dicha perdida de interés tendría como consecuencia la disminución de efectividad de las medidas en materia cambiaria, con su consecuente afectación en el mercado cambiario y en uno de los mecanismos con que el Banco de México cuenta para dar cumplimiento a su objetivo constitucional prioritario de procurar la estabilidad del poder adquisitivo de la moneda nacional.

Por ello, la Comisión de Cambios, así como la Secretaría de Hacienda y el Banco Central, en lo individual deben asumir la responsabilidad de considerar los efectos económicos que la publicación de las grabaciones del personal que instrumenta las operaciones cambiarias puede conllevar, particularmente, la responsabilidad de evitar riesgos y efectos negativos que puedan perjudicar no solo a la política cambiaria, sino al sistema financiero y a la economía nacional en su conjunto. En ejercicio de tal responsabilidad tal organismo y autoridades están obligadas a determinar el tratamiento de la información que nos ocupa, por lo que divulgar las grabaciones del personal que instrumenta éstas operaciones puede afectar en gran medida el ejercicio de sus facultades y funciones.

Por lo expuesto anteriormente, el Banco Central, a fin de poder dar cumplimiento a su mandato constitucional, se encuentra impedido para dar a conocer los detalles respecto de las operaciones cambiarias, contenidas en las grabaciones del personal contratado para este

---

[3] De Fernández-Vega, Carlos. Consultado en: http://www.jornada.unam.mx/2008/04/18/index.php?section=economia&article=030o1eco, abril 2008. Consultado el 15 de noviembre

[4] De Herrera, Carlos. Consultado en: https://lacolumna.wordpress.com/2009/03/28/la-crisis-mexicana-ahora-si-parece-crisis-arturo-herrera/, febrero 2017. Consultado el 15 de noviembre

fin, tales como las instituciones participantes en las mismas, los montos que pudieran llegar a adquirir y cualquier otro dato que permita la identificación de las operaciones.

Lo anterior, toda vez que, como se mencionó, las operaciones en el mercado cambiario determinadas por la Comisión de Cambios, e implementadas por el Banco de México, tienen como propósito proveer liquidez y mejorar las condiciones de operación de la moneda nacional. Dado que alcanzar dicho objetivo no se establece de la misma forma en todas las ocasiones, al ser sólo un participante adicional dentro del mercado cambiario, el banco central debe determinar cuidadosamente el esquema operacional de intervención y las estrategias que logren influir efectivamente dentro de este mercado conformado por un grupo heterogéneo de participantes.

Algunos ejemplos de derecho comparado en dónde la propia regulación permite reserva respecto a la divulgación de información de las intervenciones cambiarias es el Código de buenas prácticas de transparencia en las políticas monetarias y financieras, declaración de principios, del Fondo Monetario Internacional, el cual reconoce, que hay circunstancias en las que no sería aconsejable que los bancos centrales revelaran sus tácticas de implementación de la política monetaria y cambiaria, así como tampoco que proporcionaran información detallada, como la contenida en las grabaciones del personal que instrumenta las operaciones en cuestión.

Moser-Boehm (2005), señala algunas de las razones por las que existen límites válidos para la transparencia en las operaciones cambiarias: la transparencia sobre el objetivo no necesita ser sinónimo de divulgación de la información de las herramientas y tácticas relacionadas. Por su parte, Holub (2005) apunta a una segunda razón: la divulgación de información al público sobre las operaciones en el mercado de divisas puede obstaculizar su efectividad, como lo es caso de información relacionada con las tácticas o estrategias seguidas por el Banco Central, como los montos operados, instituciones adquirentes y demás detalles de las operaciones. En este caso, con la divulgación de los contratos y convenios celebrados en la materia, se actualiza la premisa sobre la divulgación de tácticas o estrategia de política cambiara del banco central.

3) **Identificable**, toda vez que, si se revelan detalles de las grabaciones del personal que instrumenta las operaciones cambiarias como cuanto compró cada institución así como cuales instituciones están en el país y cuáles en el extranjero, se puede identificar el monto operado en el mercado local y el monto operado en otros mercados internacionales. Lo anterior puede afectar la efectividad de las medidas adoptadas en materia cambiaria e incrementar el costo de operaciones financieras del Banco debido a que el mercado puede predisponerse a este tipo de estrategias y contrarrestar las acciones del banco central de manera parcial o en su totalidad, nulificando los objetivos de la operación cambiaria.

En mayor detalle, si con la publicación de los contratos y convenios los participantes deducen el monto de divisa extranjera comprada o vendida en determinado mercado, en la siguiente operación del banco central en dicho mercado tratarán de probar a éste último obligándolo a vender una cantidad mayor de dólares conociendo de antemano el monto que estuvo dispuesto a vender anteriormente. Esto incrementa el costo de la operación porque el Banco Central tendrá que vender una mayor cantidad de dólares a precios mayores e incluso podría no lograr su objetivo de procurar mantener el valor adquisitivo de la moneda nacional como se mencionó con anterioridad.

Se debe notar que al decidir implementar cualquier operación de política cambiaria, la Comisión de Cambios da a conocer la información necesaria para que los agentes económicos estén en posibilidad de adoptar las medidas que estimen más convenientes y adecuadas para satisfacer sus necesidades de moneda extranjera, así como para mantener el funcionamiento ordenado del mercado cambiario y que se procure la preservación de fundamentos económicos sólidos.

Por tal motivo, la divulgación de las grabaciones del personal que instrumenta las operaciones cambiarias en los que se puede identificar información como el nombre de las instituciones que participan en las operaciones cambiarias así como otros detalles de las mismas, podría comprometer la competitividad, ejecución y la estrategia en materia cambiaria del Instituto Central y con ello afectar la utilidad de la medida o incluso eliminarla, lo que en adición a las posibles implicaciones negativas que antes se mencionaron, podría llegar a perjudicar a la economía en su conjunto y con ello al país y podría incrementar el costo de dichas operaciones en el futuro.

Al efecto, es menester considerar que las instituciones que participan en estas operaciones buscan satisfacer necesidades de moneda extranjera, las cuales responden a características particulares de su operación, balance y/o actividades con sus clientes, en un entorno específico del mercado cambiario nacional. En ese sentido, al dar publicidad a las grabaciones del personal que instrumenta éstas operaciones y por ende, revelar el nombre de las instituciones y el monto de dólares adquirido por cada una en las operaciones implementadas por la Comisión de Cambios, a través de Banco de México, se otorgaría una ventaja indebida a otras instituciones quienes podrían utilizar dicha información para establecer estrategias en su beneficio que afecten directamente a las instituciones adquirentes de dólares, generando incluso una minusvalía y con ello una afectación en el patrimonio de estas últimas.

Adicionalmente, al dar publicidad a la información que nos ocupa, se podrían generar señales erróneas al público en general sobre la solidez o debilidad de las instituciones que

reciben asignación de dólares mediante los mecanismos que celebra la Comisión de Cambios a través de Banco de México, ya que podría interpretarse que las mismas tienen problemas para obtener dólares en el mercado o para cubrir sus pasivos en dicha moneda. Esta interpretación, podría tener implicaciones importantes para las instituciones adquirentes de dólares quienes estarían en una posición de desventaja frente a sus competidores y verse afectadas en la confianza que el público inversionista tiene en ellas.

Asimismo, el mercado y el público en general podrían llegar a determinar consideraciones sobre el perfil crediticio de riesgo de las instituciones bancarias que hayan o no participado en este tipo de operaciones que pueden ser completamente erróneas en términos de dicho asesoramiento. No sobra mencionar que las posibles consecuencias negativas antes mencionadas, afectarían de manera directa a los clientes de las instituciones adquirentes de dólares, ya que los daños causados al patrimonio de tales instituciones necesariamente se verían reflejados en las operaciones y servicios que éstas celebran con sus clientes, lo cual repercutiría en una afectación de los intereses del público en general, usuario del sistema financiero.

Adicionalmente, las afectaciones al público inversionista, podrían llegar a implicar una afectación directa a la economía nacional, ya que es conocido el hecho de que el sistema financiero promueve el desarrollo económico del país a través del otorgamiento de crédito, generando empleo, riqueza y bienestar a la sociedad.

Por lo anterior, las instituciones podrían perder interés en participar en las operaciones cambiarias en el futuro, al saber que la información sobre el nombre de los adquirentes y el monto adquirido llegaría a ser pública y considerando las afectaciones que ello pudiera acarrearles.

Por tal motivo, la publicidad de las grabaciones de las llamadas del personal que instrumenta las operaciones en materia cambiaria en los que aparece el nombre de las instituciones que participan en las operaciones mencionadas y otros detalles como el monto que se asignó a cada una, podría comprometer la competitividad, ejecución y la estrategia de intervención del Instituto Central y con ello afectar la utilidad de la medida cambiaria o incluso eliminarla, lo que en adición a las posibles implicaciones negativas que antes se mencionaron, podría llegar a perjudicar a la economía en su conjunto y con ello al país y podría incrementar el costo de dichas operaciones en el futuro.

Otro de los grandes rubros que comprende la grabación de llamadas está relacionado con las que realiza el personal encargado de la **administración e inversión de la reserva de activos internacionales.** Se debe señalar que el objetivo último de la reserva internacional es coadyuvar a la estabilidad del poder adquisitivo de la moneda nacional mediante la compensación de

desequilibrios entre los ingresos y egresos de divisas del país. En este sentido, divulgar la información contenida en las grabaciones del personal que celebra las operaciones para la administración de la reserva internacional, comprometería la ejecución de las operaciones de inversión, incrementaría el costo de las citadas operaciones y, por lo tanto, pondría en riesgo el mantenimiento del valor de la reserva internacional, lo que representa un riesgo de perjuicio significativo al interés público en virtud de que dicho riesgo es:

1) **Real**, ya que con la divulgación de las grabaciones del personal que realiza las operaciones de administración de la reserva se haría publica información como el nombre de las contrapartes del Banco y el detalle de los instrumentos en los que Banco de México tiene invertidas las reservas internacionales lo que podría dificultar la ejecución de las operaciones de inversión, así como las estrategias de cobertura de riesgos que asumen las contrapartes del Banco por las operaciones que conciertan con este Instituto Central. Esto último tendría como consecuencia un posible incremento en el costo de la realización de las operaciones del Banco Central en detrimento del rendimiento y valor de la reserva internacional en su conjunto.

   Se debe recordar que el nivel de reservas de una nación se asocia con la fortaleza de su economía para enfrentar situaciones económicas y financieras adversas. Baste recordar los artículos de prensa que fueron publicados a finales de 2015 y principios de 2016 en los cuales, debido a la baja en el nivel de las reservas internacionales derivado de las subastas de dólares implementadas por la Comisión de Cambios a través del Banco de México, los analistas cuestionaron y mostraron preocupación respecto a si el nivel de reservas era el adecuado para enfrentar situaciones financieras adversas. Así, una afectación en el nivel de las reservas internacionales generaría una menor capacidad del Banco Central para intervenir en los mercados cambiarios, en caso de que así lo determine la Comisión de Cambios. Lo anterior, podría reflejarse en niveles más elevados del tipo de cambio del peso frente a otras divisas. A su vez, la depreciación del peso incrementaría las presiones a la alza en los precios de distintos bienes y servicios, primeramente de aquellos que utilizan insumos importados y, posteriormente de todo tipo de bienes de uso cotidiano en toda la población. De actualizarse este supuesto, se vería afectada la capacidad del Banco de México de cumplir con su objetivo prioritario de procurar la estabilidad del poder adquisitivo de la moneda nacional.

   En el mismo orden de ideas, una depreciación sostenida del tipo de cambio, podría aumentar los riesgos para la estabilidad financiera y económica del país, toda vez que las empresas y otros oferentes de bienes y servicios tienden a reaccionar con cautela ante estos episodios de volatilidad, disminuyendo sus niveles de inversión e incluso eliminando empleos hasta no tener mayor certeza del panorama económico. En este tipo de entorno, podría originarse un círculo vicioso en el cual las instituciones financieras podrían enfrentar

pérdidas en sus carteras de crédito, restringir las condiciones de otorgamiento de crédito y acentuar el debilitamiento de la actividad económica en el país.

2) **Demostrable,** pues no debe olvidarse que el monto de las reservas tiene un peso relativo importante en la economía nacional, por tal motivo es necesario mantener una estrategia de inversión de las mismas que minimice el impacto sobre las condiciones de los mercados financieros y, consecuentemente, el costo de ejecución de dichas estrategias. En tal virtud la divulgación de las grabaciones de las llamadas del personal que celebra las operaciones para administrar la reserva internacional y por ende de los instrumentos en los que el Banco Central invierte los recursos de dicha reserva representa un riesgo para la ejecución de las estrategias mencionadas; lo anterior, se debe a que diversas instituciones que no operan con el Banco de México, podrían utilizar la información contenida en las grabaciones como el nombre de las contrapartes o los instrumentos en los que se invierten con fines especulativos para comprar anticipadamente el mismo tipo de instrumentos financieros, elevando considerablemente el precio de los mismos al momento en que el Banco requiera comprarlos, circunstancia que podría afectar el rendimiento y el valor de los activos internacionales de Banco de México.

   La citada actividad especulativa junto con la divulgación de los nombre de las contrapartes del Banco como consecuencia de la divulgación de los contratos y convenios, también podría afectar o entorpecer las estrategias de dichas contrapartes del Banco de México para cubrir los riesgos que asumen por las operaciones concertadas con este Instituto Central. Esto último podría repercutir en un mayor costo de las operaciones de estas instituciones financieras, el cual podría transmitirse a la población a través de un incremento en el precio de sus comisiones y productos de crédito, incluyendo tarjetas de crédito, créditos para compra de automóviles, hipotecas, así como créditos al sector corporativo. De este modo, derivado de la dependencia de las economías y la interrelación de los mercados financieros, podría haber una afectación generalizada a la actividad económica, a través de un menor otorgamiento de crédito.

   Este tipo de comportamientos, anticiparse al mercado, es común entre los participantes de los mercados financieros y se puede ejemplificar con lo sucedido el 29 de marzo de 2017 en el que Banco de México anunció el traspaso de 321,653.3 millones de pesos al Gobierno Federal por concepto de su remanente de operación. Ese mismo día la Secretaría de Hacienda y Crédito Público (SHCP) señaló que utilizaría al menos el setenta por ciento del mismo para la amortización de la deuda pública del Gobierno Federal, esta decisión coincidió con la del año pasado en la que también se destinó el mismo porcentaje del remanente para la compra de deuda existente. Lo anterior dio paso a que los participantes del mercado anticiparan una re-compra de valores gubernamentales similar a la realizada en mayo del año pasado, lo que generó que los instrumentos de plazos similares a los que

recompró en esa fecha la SHCP incrementaran su valor en 0.21% respecto al cierre del día anterior (28 de marzo). En otras palabras, si el 29 de marzo la SHCP hubiera recomprado deuda con plazos similares a los que recompró en 2016 hubiera pagado un precio 0.21% mayor (aproximadamente 200 millones de pesos más si se considera un monto de recompra igual al de 2016).

3) **Identificable,** pues el dar a conocer detalles específicos y características de las operaciones de la administración de la reserva internacional como consecuencia de hacer públicos las grabaciones del personal que celebra las operaciones en esta materia, como por ejemplo detalles sobre los emisores de títulos de renta fija elegibles para la inversión de la reserva internacional, dará señales erróneas a los mercados financieros nacionales e internacionales y a sus distintos agentes sobre la percepción que el Banco de México tiene en relación con la seguridad de las operaciones que celebra y la capacidad, solidez o debilidad de los distintos emisores. Al respecto, estos últimos, en su mayoría son considerados de riesgo sistémico, al tratarse de entidades cuyo incumplimiento potencial pudiera afectar la estabilidad del sistema financiero, del sistema de pagos o de la economía del país en el que se encuentran establecidos, con el riesgo de que debido a la interrelación de los mercados y la globalización de la economía, esta afectación se materialice de igual forma en la economía nacional. Asimismo, lo expresado generará que los agentes financieros u otras empresas omitan analizar adecuadamente el riesgo de crédito de las instituciones y emisores con los que operan, al dar por sentado que al estar incluidas en el listado de contrapartes del Banco de México tienen un riesgo crediticio bajo, lo que representa un factor de riesgo adicional para la estabilidad del sistema financiero.

Como **agente financiero del Gobierno Federal** el Banco de México realiza operaciones con instituciones domiciliadas en México y de origen tanto nacional como internacional. Las operaciones en el ámbito nacional comprenden principalmente el seguimiento de la deuda bursátil, esto es la colocación, administración y redención de valores gubernamentales, las operaciones para manejo de pasivo y el seguimiento al programa de formadores de mercado. Por lo que respecta a las operaciones internacionales estas se centran en la contratación de las coberturas petroleras. El dar a conocer detalles de las grabaciones del personal que ejecuta las operaciones como agente financiero del Gobierno Federal, podría generar que instituciones financieras en general utilicen la información con fines especulativos frente a otras instituciones para comprar/vender anticipadamente el mismo tipo de instrumentos financieros que utiliza el Gobierno Federal en sus operaciones, elevando considerablemente su precio y el costo financiero que éste tiene que pagar. Esto no sólo dificultará la ejecución de las operaciones futuras sino que puede producir incertidumbre respecto a los recursos disponibles para otros fines del gasto público e incluso podrá comprometer los parámetros establecidos en el paquete económico del Gobierno Federal. Lo anterior representa un riesgo de perjuicio significativo al interés público en virtud de que dicho riesgo es:

1) **Real**, pues por lo que se refiere a las operaciones nacionales, de acuerdo con la normatividad vigente[5], sólo pueden participar en las operaciones que Banco de México realiza como agente financiero del Gobierno Federal en los mercados nacionales las instituciones de crédito, la Financiera rural, las casas de bolsa, las sociedades de inversión, las sociedades de inversión especializadas de fondos para el retiro y otros intermediarios autorizados expresamente por el Banco de México. Normalmente, tales intermediarios financieros participan en estas operaciones (como la subasta primaria de valores gubernamentales, las subastas sindicadas, las operaciones de refinanciamiento, etcétera) presentando posturas con precios previamente acordados con sus clientes. Esto permite a los postores determinar los precios con los que participarán en las operaciones para tratar de asegurar que recibirán asignación y, al mismo tiempo, mantener cierto margen de intermediación. En tal sentido, si se da a conocer detalles de las llamadas que realizan las personas que llevan a cabo estas operaciones a través de la divulgación de la grabación de dichas llamadas, como nombres y montos de participación de las contrapartes del Banco, sus clientes podrían obtener conclusiones no necesariamente correctas y exigir mejores precios a los intermediarios (entiéndase una tasa de interés mayor), quienes a su vez trasladarían esta mayor tasa al Gobierno Federal. Lo anterior podría generar un aumento en el costo de financiamiento del Gobierno Federal, pues se debe recordar que las operaciones que Banco de México realiza en nombre del Gobierno son con propósitos de financiamiento (emisión de valores gubernamentales) o de manejo de pasivos. Si el costo de financiamiento del Gobierno Federal se incrementa, éste tendrá que destinar mayores recursos de su presupuesto al pago de intereses de su deuda, disminuyendo el gasto en otros rubros que puedan generar mayores beneficios a la sociedad.

   Respecto a las operaciones de coberturas petroleras, se debe hacer notar que el programa de coberturas petroleras mexicano se encuentra dentro de los mayores a nivel global. Por tal motivo, debe cuidarse el impacto negativo que pueda tener sobre las condiciones de los mercados financieros y procurar que se reduzca su costo. El programa de coberturas petroleras que el Gobierno Federal implementa año con año tiene la finalidad de proteger los ingresos de la Federación, específicamente los ingresos petroleros, mismos que representan alrededor del 11% de los ingresos totales (equivalente al presupuesto asignado a los sectores de salud y educación para 2018), de acuerdo con las Estadísticas Oportunas de Finanzas Públicas.

   La divulgación de los datos de las entidades con las que se ha contratado, así como los plazos, cantidades, términos y condiciones pactadas, también afectará el interés público. Lo

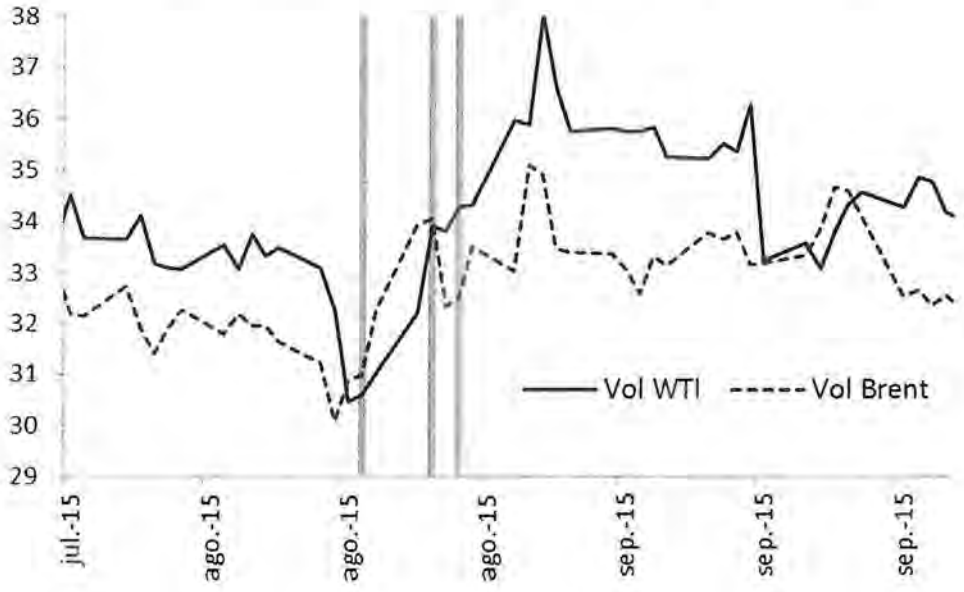
[5] Circular 5/2012 "Reglas de las subastas para la colocación de valores gubernamentales y de valores del IPAB" Consultado el 15 de noviembre

anterior, debido a que diversas instituciones ajenas al programa de coberturas podrían utilizar la información con fines especulativos para comprar anticipadamente el mismo tipo de instrumentos financieros que utiliza el Gobierno Federal, elevando considerablemente su precio. Esto ocasionará necesariamente que el costo fiscal del referido programa sea mayor, lo cual dificultará su ejecución, pues el precio de las coberturas será más alto, lo que producirá incertidumbre respecto a los recursos disponibles para otros fines del gasto público e incluso podrá comprometer los parámetros establecidos en el paquete económico del Gobierno Federal, ya que se tendrán que destinar mayores recursos públicos en la compra de las referidas coberturas, con la correlativa disminución de otros rubros del gasto público.

Además, debe señalarse que en el caso que ocurra un cambio en la rentabilidad o riesgo esperado de las contrapartes con las que se contratan las coberturas petroleras por hacer pública la información de las mismas a través de la divulgación de las grabaciones de las llamadas del personal que las instrumenta, éstas pudieran negarse a contratar coberturas con el Gobierno Federal.

En efecto, como se ilustra en la Gráfica 1, después de darse a conocer un serie de artículos sobre la cobertura petrolera de México en agosto de 2015, a través del sistema de noticias Bloomberg, la volatilidad en el precio de los crudos de referencia "West Texas Intermediate (WTI)" y "Brent" se incrementó generando también un aumento en el costo ofrecido por las contrapartes para cubrir las operaciones concertadas con el Banco de México.

Gráfica 1: Volatilidad del petróleo en términos porcentuales



Fuente: Datos de Bloomberg

La volatilidad es un componente muy importante del precio de las coberturas debido a que esta refleja el ritmo al que el precio de un activo -en este caso del WTI o Brent - puede subir o bajar. Al aumentar la volatilidad, aumenta la probabilidad de que los precios suban o caigan en mayor grado y a mayor velocidad: es decir, se acrecienta la incertidumbre de cuál será el precio de un activo a una fecha futura. Y como con cualquier seguro, al incrementar la incertidumbre sobre un evento aumenta el costo de su cobertura. Adicionalmente, este último costo no solamente lo absorbe el Gobierno Federal, al destinar mayores recursos públicos en la compra de las referidas coberturas, sino que las mismas contrapartes que ofrecen estos instrumentos tienen a su vez que realizar operaciones en el mercado para cubrirse y prevenir la posibilidad de que pierdan dinero a raíz del programa -tal y como sucedió durante los programas de 2015 y 2016, en los que el precio del petróleo cayó de manera importante, beneficiando al cumplimiento de los compromisos señalados en el Presupuesto de Egresos de la Federación, toda vez que las contrapartes tuvieron que honrar las coberturas - mismas que también incrementan en precio al aumentar la volatilidad, creando un círculo vicioso de aumentos en el precio. A manera de ejemplo, bajo las condiciones de mercado del primer trimestre del año, un incremento de 1 punto porcentual de la volatilidad -es decir, que por ejemplo ésta se incremente de 30 a 31% - equivale a que el precio de cobertura de 1 barril de petróleo aumente en 15 centavos. Si esto se traduce a un Programa de, por ejemplo, 200 millones de barriles, y donde el aumento en la volatilidad no es de solamente 1 punto porcentual sino de 8 como se observa en la Gráfica 1, se obtiene que el costo de la cobertura sería de $240 millones de dólares adicionales a lo que hubiera sido de no haber aumentado la volatilidad.

Las entidades con las que se contratan las coberturas compiten entre sí en un mercado muy especializado y en el que participan pocas contrapartes. En consecuencia, la divulgación de la información contenida en las grabaciones afectará necesariamente la determinación de los precios de los derivados. Al respecto, ha de tomarse en cuenta que la mayor parte del programa de cobertura se concentra en cubrir el crudo tipo Maya, al ser el que México produce. Sin embargo este es más susceptible de ser distorsionado, debido a lo reducido de su mercado en comparación con otros crudos de referencia como es el caso del tipo Brent.

En relación con lo anterior es importante considerar que no existe un mercado desarrollado de los instrumentos financieros necesarios para cubrir los ingresos petroleros del Gobierno Federal, por lo que el Gobierno solo puede adquirir estas coberturas con pocas instituciones financieras internacionales especializadas (contrapartes del programa). Dichas contrapartes, a su vez, se ven obligadas a comprar coberturas con otros operadores de

materias primas para diversificar su riesgo, lo cual resulta complicado debido a las pocas contrapartes que existen para este tipo de instrumentos.

Las entidades con las que se contratan las coberturas buscan a su vez celebrar operaciones en el mercado con otras instituciones financieras, en las que se consideran todos los componentes de dichas coberturas, con el fin de cubrir los riesgos que asumen. En consecuencia, instituciones ajenas al programa respectivo tendrán ventaja comparativa frente a las contrapartes del Banco Central, al conocer las necesidades de cobertura que estas requieren llevar a cabo.

2) **Demostrable**, pues por lo que se refiere a las operaciones en los mercados financieros nacionales, existe gran sensibilidad a la información que se proporciona. El hecho de dar a conocer detalles contenidos en las grabaciones del personal que instrumenta las operaciones en comento como el nombre de las instituciones participantes en las operaciones de agente financiero que Banco de México lleva a cabo a nombre del Gobierno Federal, podría conducir a conclusiones erróneas sobre su posición o inclusive su estrategia de inversión, lo que podría dar lugar a una percepción equivocada sobre la solidez o debilidad de distintas instituciones financieras. Cabe recordar que varias de las instituciones financieras que participan en éstas operaciones son o pueden ser consideradas de riesgo sistémico, por lo que al tratarse de entidades cuyo potencial incumplimiento pudiera afectar la estabilidad del sistema financiero o de los sistemas de pagos, existe el riesgo de que esta afectación se materialice en la economía nacional.

   La publicación de esta información podría traducirse en un menor interés por parte de los intermediarios financieros en participar en este tipo de operaciones, lo que derivaría potencialmente en un incremento en el costo de financiamiento del Gobierno Federal y podría comprometer la adecuada implementación de la política fiscal del país.
   En el mismo sentido, el dar a conocer los nombres de las instituciones con las que se han celebrado las operaciones de coberturas petroleras y las especificaciones de las mismas, dará señales erróneas a los mercados financieros nacionales e internacionales y a sus distintos agentes sobre la percepción que el Banco de México tiene en relación con la seguridad de las operaciones que celebra y la capacidad, solidez o debilidad de distintas instituciones financieras, en específico, de aquellas con las que se han celebrado las mencionadas operaciones. Dichas instituciones, en su mayoría son consideradas de riesgo sistémico, al tratarse de entidades cuyo incumplimiento potencial pudiera afectar la estabilidad del sistema financiero, del sistema de pagos o de la economía del país en el que se encuentran establecidas, con el riesgo de que debido a la interrelación de los mercados y la globalización de la economía, esta afectación se materialice de igual forma en la economía nacional. Esto además tendrá implicaciones sobre la competencia en el sector financiero, al poner en una posición ventajosa o incluso beneficiar a las instituciones

incluidas en la lista de instituciones autorizadas para operar las coberturas de petróleo y potencialmente perjudicar a aquellas que no lo están.

Lo expresado generará que los agentes financieros u otras empresas omitan analizar adecuadamente el riesgo de crédito de las instituciones con las que operan, al dar por sentado que al estar incluidas en dicho listado tienen un riesgo crediticio bajo, lo que representa un factor de riesgo para la estabilidad del sistema financiero.

Por otra parte, al ocurrir lo mencionado en los párrafos anteriores, tanto para las operaciones realizadas en los mercados nacionales como internacionales, el Banco de México no establecería los incentivos para una sana competencia entre las instituciones financieras, en contravención a una de sus finalidades previstas en el artículo 2o. de su Ley, que es precisamente promover el sano desarrollo del sistema financiero. El divulgar las grabaciones del personal que celebra las operaciones que realiza este Instituto central como como agente financiero del Gobierno Federal, impedirá el cumplimiento de dicha finalidad, pues afecta la debida competencia entre las instituciones financieras y debilita la confianza en algunas de ellas. Este argumento es incluso válido para el programa de coberturas petroleras que, si bien se realiza en mercados financieros internacionales de primer orden, debido a la interconexión y dependencia que existe entre las economías, la afectación a cualquiera de las entidades financieras que integran los mercados financieros se traduce en una afectación al mercado nacional y a las entidades financieras que están establecidas en nuestro país.

El debilitamiento de la confianza en algunas instituciones incrementa su costo de financiamiento que, a su vez, encarece el crédito a hogares y empresas, con implicaciones adversas sobre el desarrollo y dinamismo de la actividad económica. Esto último a través de mayores comisiones y tasas de interés en créditos al consumo, hipotecarios, refaccionarios, de habilitación y avío, entre otros.

En caso de ponerse en riesgo la realización de cualquiera de las operaciones de agente financiero del Gobierno Federal, esto tendrá implicaciones directas sobre las finanzas públicas del país y la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero mexicano al ponerse en duda la capacidad de pago del Gobierno Federal. En efecto, un incremento en el costo de financiamiento del Gobierno Federal por una menor participación de las instituciones financieras en las operaciones que Banco de México realiza en su nombre en los mercados nacionales, o el no contar con un programa de cobertura petrolera podría poner en riesgo las finanzas públicas.

Una debilidad en las finanzas públicas genera incertidumbre respecto de la capacidad crediticia del Gobierno Federal, ejemplo de ello es el cambio en la perspectiva de la calificación crediticia de la deuda del Estado Mexicano, de estable a negativa, por parte de la calificadora Fitch Ratings el pasado 31 de octubre. En el comunicado que acompañó la decisión, la calificadora argumentó que "...Aunque Fitch espera que la próxima administración continúe apoyando los aspectos fundamentales del marco de política macroeconómica –disciplina presupuestaria y autonomía del Banco de México (Banxico)–, persisten los riesgos relacionados con la postura fiscal del gobierno entrante". La revisión en la perspectiva de riesgo crediticio del país desencadenó una serie de revisiones a la perspectiva de riesgo crediticio de los emisores nacionales, entre ellos, algunas instituciones financieras mexicanas. En el comunicado de fecha 6 de noviembre de 2018, la calificadora señaló: "...Fitch Ratings has conducted a portfolio review of selected Mexican Financial Institutions (FIs) following the revision of Mexico's sovereign rating Outlook to Negative from Stable on Oct. 31, 2018 (Fitch Ratings realizó una revisión de la cartera de instituciones financieras mexicanas (IF) seleccionadas luego de la revisión de la calificación de la calificación soberana de México a Negativo desde Estable el 31 de octubre de 2018)".

3) **Identificable**, toda vez que revelar la información contenida en las grabaciones del personal del Banco de México que celebra las operaciones como agente financiero del Gobierno Federal, puede derivar en conclusiones erróneas sobre el riesgo de los intermediarios financieros, en particular en el caso de las instituciones que participan en las operaciones llevadas a cabo en los mercados nacionales, y generarles pérdidas potenciales a los mismos y, en un caso extremo, una corrida bancaria en su contra. Cuando una institución sufre una corrida bancaria se produce una oleada especulativa, que bien puede definirse como un sentimiento de desconfianza generalizada y especulación poco fundamentada sobre la solidez de las instituciones de crédito por parte de los depositantes de todo el sistema financiero. Este hecho incrementa en forma considerable la probabilidad de contagio a clientes de otras instituciones y de un retiro masivo de los depositantes de las instituciones que no quieren perder sus ahorros, poniendo en riesgo la estabilidad financiera y la economía nacional en su conjunto. Adicionalmente, si como resultado de una corrida bancaria una institución de crédito se declara en bancarrota, es muy probable que ese participante no pueda cumplir con sus obligaciones en los sistemas de pagos, provocando con ello que otros participantes también incumplan, generando lo que se conoce como riesgo sistémico. Si además la institución de crédito en bancarrota es sistémicamente importante, el contagio podría esparcirse rápidamente a todo el sistema financiero, incrementando los riesgos para el sano desarrollo del mismo y para la estabilidad financiera, con el consecuente daño grave a la economía nacional.

En relación con la revisión a la baja de las calificaciones a algunos bancos mexicanos que ocurren normalmente cuando existen dudas respecto a la solidez de las finanzas públicas

del país, es importante resaltar que un deterioro en la calificación de dichas entidades puede restringir su acceso a financiamiento e incrementar el costo del mismo, dificultando el cumplimiento de sus obligaciones con los potenciales riesgos que esto implica para los sistemas de pagos y la estabilidad financiera del país. Más aún, siendo los bancos mexicanos de los principales tenedores de deuda emitida por el Gobierno de México, la baja calificación de dichos títulos afecta la liquidez de las instituciones financieras tenedoras, colocándose en una situación de riesgo que, dependiendo de la institución financiera afectada, podría representar un riesgo al sistema financiero en su conjunto. Adicionalmente, una percepción de mayor riesgo en las finanzas públicas podría generar desconfianza y la salida de los títulos emitidos por el Gobierno Mexicano de varios índices de referencia de inversión y por ende una redistribución de las carteras de inversión de participantes extranjeros, que también son de los principales tenedores de estos valores, generando una venta importante de títulos y un incremento en el costo de financiamiento del Gobierno Federal.

En el caso particular de las coberturas petroleras, debe señalarse que en el caso de no poder cubrir íntegramente los ingresos petroleros del Gobierno, un ajuste a la baja en los precios internacionales del petróleo implicaría una disminución en los ingresos del Gobierno Federal, lo que a su vez requeriría un mayor endeudamiento para cubrir dicha disminución. Lo anterior representaría un cambio en la política fiscal del Gobierno Federal (proceso de consolidación fiscal), lo que podría afectar la percepción de riesgo de la deuda del Gobierno con su consecuente aumento en el costo de financiamiento del mismo.

Finalmente, el dar a conocer detalles de las llamadas y grabaciones del personal encargado del **soporte del funcionamiento de los Sistemas de Pagos** representa un riesgo de perjuicio significativo al interés público en virtud de que dicho riesgo es:

1) **Real**, en razón de revelar o divulgar la información relacionada con los registros y grabaciones de llamadas realizadas y recibidas que soportan el funcionamiento de los Sistemas de Pagos, facilita a una persona o grupo de personas con intenciones delincuenciales distinguir las comunicaciones de los Servidores Públicos que están relacionadas con aspectos de seguridad informática, especificaciones técnicas en materia de seguridad, procesos de continuidad operativa y de contingencia; así mismo permitiría identificar los tiempos de respuesta de los Participantes ante presuntas vulneraciones, protocolos de comunicación y, en general, información relacionada con la infraestructura de los sistemas de pago administrados por este Instituto Central, lo cual posibilita la realización de acciones hostiles en contra de las tecnologías de la información de este Banco Central, así como de las infraestructuras que éste administra, opera y supervisa, lo cual, podría menoscabar la efectividad de las infraestructuras a tal grado, que su destrucción o inhabilitación afectaría seriamente la efectividad de las medidas implementadas en los sistemas financiero y económico, del país, arriesgando el

funcionamiento de esos sistemas y, en consecuencia, de la economía nacional en su conjunto.

Asimismo, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se fundamentan en descubrir y aprovechar vulnerabilidades de dichos sistemas, así como brechas de seguridad en los procesos y protocolos de operación, 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, la infraestructura informática y sus procesos operativos.

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. [6]

En el caso en concreto, los registros y grabaciones de llamadas realizadas y recibidas que soportan el funcionamiento de los Sistemas de Pagos contiene información relacionada con especificaciones técnicas en materia de seguridad, procesos de continuidad operativa, información sobre los componentes de los sistemas informáticos así como especificaciones de equipos de cómputo y telecomunicaciones, especificaciones en materia de seguridad informática, protocolos de actuación para la operación de los sistemas de pagos así como las condiciones de operación de los mismos, entre otros, por lo que su divulgación proporcionaría elementos de información que facilitarían a los cibercriminales aprovechar los puntos débiles de las infraestructuras de los mercados financieros, entre ellas, los sistemas de pagos, 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 infraestructuras.

2) **Demostrable**, ya que es un hecho notorio que los sistemas de pagos de Bancos Centrales han sufrido ataques cibernéticos a través de los participantes de estas infraestructuras de

[6] 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.

forma constante y organizada. Dichos ataques tienen por objeto el robo de recursos económicos a través del empleo de vulnerabilidades en las instituciones, aplicativos e infraestructura tecnológica de los sistemas.

Adicionalmente, está documentado que durante los últimos años se ha observado un incremento sostenido de ataques informáticos en el sector financiero a nivel mundial, incluyendo Bancos Centrales y diversas instituciones financieras. Las investigaciones realizadas señalan que estos ataques han sido orquestados por organizaciones criminales internacionales con herramientas y técnicas sofisticadas que, además de dañar la reputación de las instituciones afectadas, han generado cuantiosas pérdidas económicas.[7]

En relación con lo anterior, es importante señalar que México ocupa el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica[8] y que tan sólo en México, el costo causado por el cibercrimen ascendió a $5,500 millones de dólares y afectó alrededor de 22.4 millones de personas; mientras que a nivel mundial, el costo ascendió a $125,900 millones de dólares y afectó a 689.4 millones de personas.[9] Por lo anterior, este Instituto Central[10] y autoridades como la Secretaría de Hacienda y Crédito Público[11] se han pronunciado sobre la importancia de fortalecer la ciberseguridad para la estabilidad del sistema financiero.

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

i) El ataque de tipo "Watering hole" en Polonia, que permitió utilizar un servidor de la Autoridad de Supervisión Financiera para distribuir código malicioso a más de 20 bancos

---

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

8 Arreola Javier. "Ciberseguridad (casi) a prueba del enemigo 'invisible'". Forbes México. http://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/ consultado el 13 de noviembre de 2018.

9 Informe Norton sobre Ciberseguridad 2016 - Comparaciones Globales https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf consultado el 13 de noviembre de 2018.

10 En septiembre de 2016, el Banco de México publicó el documento "Política y funciones del Banco de México respecto a las infraestructuras de los mercados financieros" en el cual dedica una sección especial al tema de seguridad informática. Este documento se encuentra disponible en la siguiente dirección electrónica: http://www.banxico.org.mx/sistemas-de-pago/informacion-general/politica-del-banco-de-mexico-respecto-de-las-infra/%7B2EAC65D2-21F4-AB2D-D250-06926EE796F8%7D.pdf, consultado el 13 de noviembre de 2018.

11 Secretaría de Hacienda y Crédito Público. "Fortalecer la ciberseguridad, relevante para el desarrollo de México." 29 de octubre de 2017. https://www.gob.mx/shcp/prensa/informe-semanal-del-vocero-132251?idiom=es consultado el 13 de noviembre de 2018.

polacos[12] , el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada;[13]

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; [14]

iii) El ataque mediante el código malicioso "Petya", enfocado en borrar archivos y discos duros completos, que paralizó las actividades de aerolíneas, bancos y bufetes de abogados en Europa; [15]

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; [16]

v) 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; [17]

vi) Los cibertataques reportados por la empresa de ciberseguridad S21sec realizados por el grupo cibercriminal llamado 'Cobalt', el cual consistió en un ataque realizado a los cajero

---

[12] 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 13 de noviembre de 2018.

[13] 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 13 de noviembre de 2018.

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

[15] Marín, Eduardo. "Descubren Que Petya, El Ataque Que Paralizó Empresas De Toda Europa, No Secuestraba Archivos Sino Que Los Borraba." Gizmodo En Español, Es.gizmodo.com, 28 de junio de 2017, http://es.gizmodo.com/descubren-que-petya-el-ataque-que-paralizo-empresas-de-1796492938 consultado el 13 de noviembre de 2018.

[16] 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 13 de noviembre de 2018.

[17] Nussman, Chris. "DHS Bulletin on Denial of Service (TDoS) Attacks on PSAPs." NENA The 911 Association, 17 de marzo de 2013, www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm, consultado el 13 de noviembre de 2018.

automáticos basado en red, es decir que no se requiere acceso físico al cajero para perpetrarlos, sino que la infección se lleva a cabo desde la propia red interna del banco; [18]

vii) El ciberataque basado en la modalidad de denegación de servicio distribuido (DDoS) en Holanda, en el cual diez millones de holandeses se quedaron sin firma digital por el bloqueo del portal como consecuencia de una avalancha de solicitudes; [19]

viii) Los ciberataques a los que fue víctima Delta Air Lines, entre el 26 de septiembre al 12 de octubre de 2017, los cuales fueron informados a través de un comunicado que la compañía [24]7.ai, proveedora de servicios informáticos de ésta y otras compañías, suceso que causó que los datos bancarios de algunos de los usuarios de la aerolínea se hayan visto comprometidos durante ese periodo. [20]

ix) Los ataques cibernéticos que han sufrido otros Bancos Centrales a través de la infraestructura de sistemas de pagos conocida como SWIFT, la cual ha sido utilizada para realizar robos de capital, uno de estos casos es el del Banco Central de Bangladesh, que sufrió un robo de 81 millones de dólares. [21] 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. [22] 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. [23]

x) El ataque ocurrido a las instituciones financieras participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI®), el cual consistió en la alteración de sus aplicativos para conectarse a esta Infraestructura de Mercado Financiera (IMF), mediante código malicioso, el cual distribuyó dinero desde las cuentas concentradoras de los participantes

---

[18] S21Sec. "COBALT: EL CIBERCRIMEN ORGANIZADO GOLPEA LOS CAJEROS AUTOMÁTICOS EUROPEOS." S21Sec, 23 de noviembre de 2016, www.s21sec.com/es/blog/2016/11/cobalt-cibercrimen-organizado-que-ataca-a-los-cajeros-automaticos-europeos consultado el 13 de noviembre de 2018.

[19] Recalde, Luis. EL CIBERESPACIO: EL NUEVO TEATRO DE GUERRA GLOBAL. Revista De Ciencias De Seguridad y Defensa, http://geo1.espe.edu.ec/wp-content/uploads/2016/07/art15.pdf consultado el 13 de noviembre de 2018.

[20] Delta Airlines. "INFORMATION ON [24]7.AI CYBER INCIDENT." Information on [24]7.Ai Cyber Incident, 7 de abril de 2018, www.delta.com/content/www/en_US/response.html consultado el 13 de noviembre de 2018.

[21] Michael Riley, Alan Katz. "Swift Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh". Bloomberg. 26 de Mayo de 2016. https://www.bloomberg.com/news/articles/2016-05-26/swift-hack-probe-expands-to-up-to-dozen-banks-beyond-bangladesh consultado el 13 de noviembre de 2018.

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

[23] Antony Peyton. "Symantec reveals more hack attempts on Swift network". Banking Technology. 11 de octubre de 2016. https://www.bankingtech.com/2016/10/symantec-reveals-more-hack-attempts-on-swift-network/ consultado el 13 de noviembre de 2018.

a cuentas de usuarios específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero.[24] 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.[25]

Inclusive, uno de los modus operandi de los ciberataques es precisamente a través de la obtención de información pública, información fácilmente accesible o información inaccesible, lo cual puede ocurrir mediante solicitudes de acceso a la información, o bien, a través de las organizaciones que operan o tienen acceso a los sistemas, en complicidad o no, con el único objeto de conocer las vulnerabilidades en las instituciones, empresas, sistemas, protocolos y procedimientos de operación e infraestructura de tecnologías de la información.[26]

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.[27]

Por lo anterior, los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar cualquier tipo de información asociada a los sistemas o los procesos en los que intervienen así como las especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuyo rol no esté autorizado[28], entre otros, en el entendido de que dicha información, al

---

[24] Banco de México. "Información sobre los ataques a los Participantes del SPEI". http://www.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/%7B2B9BB8C6-D66B-38C4-CC90-F72A7BC335C9%7D.pdf, consultado el 13 de noviembre de 2018.

[25] Acorde con los "Puntos importantes sobre la situación actual del SPEI" publicados en la página de internet del Banco de México. http://www.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/%7B022CD9D7-11A9-68E6-D1A5-965F57A23F60%7D.pdf, consultados el 13 de noviembre de 2018

[26] El Economista, *El sistema financiero mexicano fue víctima de una campaña de ciberataques*, 15 de mayo de 2018. https://www.eleconomista.com.mx/sectorfinanciero/El-sistema-financiero-mexicano-fue-victima-de-una-campana-de-ciberataques-20180515-0097.html consultado el 13 de noviembre de 2018.

[27] 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 13 de noviembre de 2018.

[28] 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

estar en posesión de personas no autorizadas, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central de la Nación, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

3) **Identificable**, ya que a la fecha de realización de la presente prueba de daño, es un hecho notorio que los sistemas de pagos están siendo objeto de ciberataques a gran escala, como quedó demostrado en la sección anterior. Si bien dichos ataques no han logrado irrumpir en los sistemas del Banco de México, resulta claramente identificable que el objeto final de dichos ataques son los sistemas de pagos que maneja el Banco de México, cuya seguridad depende de la reserva de la información materia de la presente prueba de daño.

En ese sentido, un ataque informático derivado de proporcionar la información materia de la presente prueba de daño, podría resultar en la afectación de las órdenes de transferencia en las cuentas bancarias de los distintos participantes y de los usuarios del sistema en comento. A su vez, estas afectaciones en las órdenes de transferencia podrían derivar en una pérdida de patrimonio no sólo para las instituciones financieras del país y demás participantes de los sistemas de pagos, sino en perjuicio de la población usuaria de los pagos electrónicos interbancarios, es decir millones de personas físicas y morales, incluyendo aquellos empleados del sector público o privado que reciben su pago de salario vía transferencia electrónica que realizan sus patrones.

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

---

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 13 de noviembre de 2018.

Por lo anterior, un ataque perpetrado directamente al SPEI o a sus participantes, ocasionado por dar a conocer información, representa un perjuicio significativo para el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias, pues de acuerdo con la información del Banco de México, de agosto de 2017 a agosto de 2018, se realizaron aproximadamente 603 millones de pagos electrónicos interbancarios por un monto de 293 billones de pesos; lo anterior equivale a más de 63 mil operaciones por un monto de aproximadamente 31 mil millones de pesos por hora, únicamente para lo que respecta al SPEI. [29]

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

El riesgo de perjuicio que supondría la divulgación de la información, supera el interés público general de que se difunda, pues dar a conocer las grabaciones de las llamadas del personal del Banco de México que instrumenta las operaciones con propósitos de regulación monetaria, regulación cambiaria, de inversión y administración de las reservas internacionales, de agente financiero del Gobierno Federal y de soporte de los Sistemas de Pagos, no abona un beneficio a la transparencia comparable con el perjuicio de debilitar la efectividad de las medidas de política en materia monetaria, o de una oleada especulativa que afecte a las instituciones, muchas de ellas de importancia sistémica, o de debilitar la efectividad de las medidas adoptadas en relación con las políticas en materia cambiaria, las acciones encaminadas a mantener la estabilidad del poder adquisitivo de la moneda nacional, evitar distorsiones en la estabilidad de los mercados, garantizar la estabilidad del sistema financiero, de los sistemas de pagos y de la economía nacional en su conjunto, de no incrementar el costo de las operaciones financieras que realiza el Banco en sus operaciones de inversión y administración de la Reserva Internacional, de no incrementar el costo de las operaciones del Banco, en su carácter de agente financiero del Gobierno Federal, en particular de la Secretaría de Hacienda y Crédito Público como sujeto obligado del sector público federal y de proteger al sistema financiero y en consecuencia a sus usuarios, respecto de otorgar publicidad a diversa información contenida en las grabaciones de las llamadas realizadas por el personal que instrumenta las operaciones antes mencionadas. En atención a lo anterior, la reserva en la

---

29 Banco de México. Sistemas de pago de alto valor, Sistemas de liquidación en tiempo real (CF252) – Sistema de Pagos Electrónico Interbancarios. http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es

publicidad de la información, resulta la forma menos restrictiva disponible para evitar un perjuicio mayor.

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que se debe prevalecer el interés público de proteger la efectividad de las medidas de política en materia monetaria, de no afectar la efectividad de uno de los mecanismos de política cambiaria establecidos por la Comisión de Cambios; de no incrementar el costo de las operaciones cambiarias realizadas por el Banco central a nombre propio y a nombre del Gobierno Federal, en su carácter de agente financiero, en particular de la Secretaría de Hacienda y Crédito Público como sujeto obligado del sector público federal; y de proteger los sistemas de pagos y en consecuencia al sistema financiero y sus usuarios de la perpetración de ataques cibernéticos dirigidos específicamente a los sistemas de pagos administrados por el Banco de México y a la infraestructura relacionada con estos, los cuales tengan como resultado la creación de mecanismos que faciliten el acceso indebido, la substracción de información - como datos personales referente a sus usuarios y las operaciones que realizan -, la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción en éstos; respecto de otorgar publicidad de las grabaciones del personal que celebra las operaciones con propósitos de regulación monetaria, cambiaria, de inversión y administración de la reserva internacional, de agente financiero del Gobierno Federal y de las que dan soporte a los sistemas de pagos. En atención a lo anterior, la reserva en la publicidad de la información, resulta la forma menos restrictiva disponible para evitar un perjuicio mayor.

La reserva de la información deberá mantenerse, al menos por cinco años, pues dar a conocer detalles de las grabaciones que realiza el personal encargado de instrumentas las operaciones monetarias, cambiarias y de agente financiero en los mercados nacionales, como por ejemplo el nombre de las instituciones con las que se realizan, podría generar señales erróneas al público sobre la solidez o debilidad de las instituciones que participan en las mencionadas operaciones, lo cual pondría a estas instituciones, en desventaja frente a sus competidores y las podría afectar en la confianza que el público inversionista tiene en ellas al ser el universo de participantes reducido y con pocas variaciones a lo largo del tiempo. La reserva de la información al menos por cinco años aplica también para las grabaciones que realiza el personal como agente financiero que se realizan en mercados internacionales toda vez que la realización dichas operaciones es un evento que se realiza cada año y, por las características del mercado en que se llevan a cabo (especializado y reducido en cuanto al número de contrapartes), las probabilidades de efectuar operaciones con la misma contraparte en años consecutivos son altas, lo que implicará que las instituciones ajenas a las operaciones en cuestión podrán dar seguimiento a las operaciones de las instituciones que son o han sido contrapartes del Banco de México en este tipo de operaciones y con base en dicha información determinar si participan o no en el programa, abriendo la posibilidad, como se mencionó con anterioridad, que puedan utilizar la información con fines especulativos para comprar anticipadamente el mismo tipo de instrumentos, incrementando el costo de las operaciones

financieras que nos ocupan. De la misma forma, las llamadas y grabaciones de las mismas del personal que soporta las operaciones de los sistemas de pagos deben reservarse por el plazo de cinco años toda vez que, como se ha manifestado esta acción atiende a la protección de las medidas de seguridad informática, con la finalidad de evitar proporcionar información que facilite intrusiones que puedan vulnerar los protocolos de operación e inhabilitar los sistemas de tecnologías de la información y comunicaciones, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques informáticos, no solo de las vulnerabilidades identificadas sino de aquellas que no se encuentran reconocidas provocando afectaciones a las Infraestructuras de los Mercados Financieros que opera y administra este Instituto Central, entre ellas los sistemas de pagos, menoscabaría la efectividad de las medidas implementadas en relación con las políticas en materia del sistema financiero del país, y ponga en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, así como comprometería las acciones encaminadas a propiciar el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos. Por lo antes expuesto, la divulgación de las grabaciones del personal y en su caso, el listado de llamadas que instrumenta las operaciones cambiarias, monetarias, de administración de la reserva internacional, de agente financiero del Gobierno Federal y de soporte de los sistemas de pagos, comprometería 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, se comprometerían las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero o el buen funcionamiento de los sistemas de pagos; se otorgaría una ventaja indebida, generando distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pagos, y se generaría un incumplimiento de las obligaciones de los participantes en un sistema de pagos, afectando seriamente al sistema financiero.

Por lo antes expuesto, con fundamento en los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 103, segundo párrafo, 104, 105, 106, fracciones I y III, 107, 108, último párrafo, 109, 113, fracción IV, y 114 de la Ley General de Transparencia y Acceso a la Información Pública; 97, 98, fracciones I y III, 100, 102, 103, 110, fracción IV, y 111de la Ley Federal de Transparencia y Acceso a la Información Pública; 1, 2, 3, fracciones I, II, III, y IV, de la Ley del Banco de México, 4, párrafo primero, 8, párrafos primero y tercero, 10, párrafo primero, 12, 19, 19 Bis, y 20, del Reglamento Interior del Banco de México, Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, así como Primero, Cuarto, Quinto, Sexto, párrafo segundo, Séptimo, fracción III, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I, II, III y IV, Trigésimo tercero, Trigésimo cuarto, párrafos primero y segundo, Quincuagésimo cuarto y Quincuagésimo quinto, párrafo primero, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, la información referente a la grabación de las llamadas que realizó el personal de la Dirección General de Operaciones y Sistemas

de Pagos del 8 de octubre al 16 de octubre de 2018, es de clasificarse como reservada, pues su divulgación pondrían en riesgo las funciones del Banco de México, el funcionamiento del sistema financiero y de la economía nacional en su conjunto, se dañaría el buen funcionamiento de los sistemas de pagos, se crearían distorsiones en los sistemas de pagos, se comprometerían las acciones encaminadas a propiciar el buen funcionamiento de los sistemas de pagos y se generaría el incumplimiento de obligaciones de un participante en los sistemas de pagos.

Referencia 1

Britain's bank run

The Bank that failed

The governor of the Bank of England is the biggest casualty of a financial fiasco—but far from the only one

Print edition | Leaders
Sep 20th 2007

Bloomberg/Landov

BRITAIN prides itself on its expertise in finance. The City is the brightest jewel in the economy's crown. Banks and financiers have based themselves in London because of the depth and sophistication of its markets and the sure touch with which they have been regulated.

Referencia 2

Wall Street humiliated by nationalisation of banks

By Stephen Foley in New York | Wednesday 15 October 2008 00:00 | 0 comments

Reuters

The US government is set to become the largest shareholder in its national banks, pumping in $250bn (£143bn) to prop up its financial system and marking one of the most startling moments in a credit crisis that has broughtquasi-nationalisation to the home of free-market capitalism.

President George Bush appeared in the White House Rose Garden yesterday morning to declare that his government was immediately taking stakes in nine of the biggest banks in America, and would extend its hand to hundreds and possibly thousands more.

Referencia 3

La Jornada

México SA

Carlos Fernández-Vega

■ Abono para la especulación II

■ Cachorros zarandeados

A mediados de 1989, Carlos Salinas de Gortari puso en circulación los Bonos de la Tesorería de la Federación, Tesobonos, a diferencia, decía, del "público ahorrador en general". Se trataba de valores gubernamentales, cotizados en dólares y pagaderos en pesos, con interés generalmente más el diferencial del tipo de cambio entre la fecha de compra y la de amortización. Como en el caso de los Petrobonos y los Cetes, estos nuevos títulos duraron en pocos meses.

El resultado de los Tesobonos no rompió expectativa alguna, hasta que a mediados de noviembre de 1994 –unas semanas antes de la entrenzadas devaluación por los "errores de diciembre"– se convirtieron en piezas de colección. Más allá de su aquello, algún amigo informó a los principales especuladores financieros y bursátiles lo que estaba a punto de suceder: el fin de la ficción primer mundista machacadamente difundida por el salinato y el derrumbe económico-financiero del país.

Dos semanas antes del desplome de la moneda nacional (21 de diciembre de 1994), cinco casas de bolsa pertenecientes a igual número de grupos financieros (constituidos tras la reprivatización bancaria), incrementaron en casi 400 por ciento la adquisición de Tesobonos. Al igual que en el caso de los CAP's antes de la venta de los bancos, en esta ocasión las más movidas fueron Acciones y Valores, del Grupo Financiero Banamex-Accival (Roberto Hernández y Alfredo Harp Helú); Inverméxico, del Grupo Financiero de igual nombre (Carlos Gómez y Gómez, uno de los destinatarios del correo electrónico referido en el México SA del 17 de abril); Operadora de Bolsa, del Grupo Financiero Obsa-Serfin (Adrián Sada); Probursa, del Grupo Financiero Marcanel-Probursa (José Madariaga Lomelín, en ese entonces presidente de los banqueros), y Mexival, del Grupo Financiero Mexival-Bancpaís (Angel Isidoro Rodríguez, el Divino).

La crisis estalló en la cara de millones de desamparados mexicanos, pero los especuladores financieros y bursátiles, no sin la contribución de sus amigos en el gobierno, ya habían tomado sus precauciones: con el grueso de los Tesobonos en sus alforjas, presionaron y obtuvieron de la administración Zedillo sus ases: valores les fueran pagados en dólares y no en pesos, como lo estableció el decreto presidencial (junio de 1995) para su emisión y circulación. Así, parte de la deuda interna –contratada en pesos para ser pagada en pesos, a un tipo de cambio de 3.4 pesos por dólar– simple y sencillamente se disparó (a un tipo de cambio de 7.63 pesos por billete verde en febrero de 1996) para favorecer a ese grupúsculo de especuladores, más los extranjeros, con muy buenos amigos en las más altas esferas del poder.

En menos de 14 meses, el gobierno zedillista amortizó, en dólares, el saldo total de Tesobonos en circulación: alrededor de 30 mil millones de billetes verdes (que legalmente debieron pagarse en pesos, al igual que los intereses por ellos generados y el diferencial en el tipo de cambio); y buena parte de ellos ingresaron a las alforjas del selecto grupo de especuladores bursátiles y financieros. Según información proporcionada por el propio ex inquilino de Los Pinos, estos valores representaron 43 por ciento del "costo de la crisis en 1995", es decir, 30 mil de los 70 mil millones por él reconocidos.

De acuerdo con información de la Secretaría de Hacienda, al cierre de 1993 los Tesobonos representaban entre 5 y 6 por ciento de la deuda interna total del gobierno federal; al finalizar 1994, más de 50 por ciento. Para justificar el beneficio a los especuladores, la dependencia aseguró que "lo único que se hizo fue cambiar deuda interna por deuda externa" (Tesobonos en pesos por Tesobonos en dólares), pero lo hizo sin autorización del Congreso.

A pesar de ello, los "Tesobonos representaron el entramado de lo que ya se conocía: el "rescate" bancario, por medio del Fobaproa y sus 120 mil millones de dólares (también sin autorización del Congreso), que los mexicanos no terminan de pagar. Entre los beneficiarios, reiteradamente aparecen los nombres de los especuladores financieros y bursátiles que gozaron de los subastos cambiarios del Fobaproa, de la "devolución" de empresas a bancanas expulsadas a las instituciones estatizadas, de los bonos de indemnización bancaria, de los certificados de aportación patrimonial de la reprivatización de los bancos, de los Tesobonos y de la impunidad que al garante en turno de Los Pinos les brindó, les brinda.

A lo anterior agréguese los impuestos "diferidos" (cazados pero nunca entregados), los vencimientos crédito fiscales que no amortizan, las exenciones y regímenes tributarios especiales y tantas otras gracias que, por falta de espacio, escapan de esta breve reseña de cómo las finanzas nacionales han sido puestas al servicio de un mínimo rapaz y sin llenadera.

Viene al festín del pastoleo, los llamados "bancos petroleros ciudadanos" serían el más fresco entremés ca lo que el garante en turno pretende ponerles en charola de plata. Las maniobras vienen enseguida.

Por cierto: los especuladores bursátiles organizados (Bolsa Mexicana de Valores y las casas de bolsa) juran que "el sector financiero del país no recibió de parte del gobierno de la República ninguna información material sobre el contenido de la reforma energética" antes de que el inquilino de Los Pinos "la presentara a la nación", es decir: el pasado 8 de abril.

Bien: no iners a decir que sí, pero sólo para abonar a una declaración de Guillermo Prieto Treviño, presidente de la BMV, el 2 de abril de 2008 (seis días antes de que el inquilino de Los Pinos entregara su iniciativa al Congreso): "El mercado de capitales está listo para apoyar títulos de Pemex. La reforma energética es un objetivo en la bolsa y el sector financiero" (La Jornada, Antonio Castellanos, 2 de abril de 2008). Y los especuladores ya tienen las alforjas.

Las rebanadas del pastel

Si de especuladores y tráfico de influencias se trata, allí están los cachorros de Martita Sahagún, a quienes el SAT les propinó una buena zarandeada al ordenar a la PGR entregar copia de la indagatoria ministerial en su contra.

BANCO DE MÉXICO

Referencia 4

Información política confidencial

El blog de análisis político más citado y acertado de México

— "Las dos grises del PRI" / Luciano Sáenz — Peter Calvert visitó a su fan Felipe Calderón —

La crisis mexicana ahora sí parece crisis / Arturo Herrera

Publicado el agosto 25, 2009 en Las Aguilas

Si hay algo que sabemos los mexicanos es comer con picante, fallar penaltis y ligar las devaluaciones a las crisis económicas. Y no es para menos. La mayor parte de las crisis económicas en la historia moderna mexicana -por lo menos las más graves- han sido inauguradas con devaluaciones del peso.

En 1976, el peso pasó de 12,5 unidades por dólar, nivel en el que se había mantenido desde 1954, a 22 pesos por dólar en unas cuantas semanas. Situaciones similares ocurrieron en febrero de 1982 y en diciembre de 1994, cuando nuevamente al peso le bastaron unas cuantas semanas para perder la mitad de su valor.

En algunos de estos eventos se presume que algunos inversionistas mexicanos, usando información privilegiada, cambiaron pesos a dólares y los sacaron del país obteniendo jugosas ganancias.

Así pues, en el imaginario popular -y en el de gran número de políticos y analistas- las crisis van acompañadas de devaluaciones y tienen culpables muy precisos: el gobierno que no sabe manejar la política económica y *los sacadólares* que se enriquecen especulando contra el peso.

Por eso ésta ha sido una crisis singular para los mexicanos. De hecho el primer problema con el peso no se dio sino hasta el verano pasado, un año después de iniciada la crisis mundial, y fue un problema de ¡sobrevaluación! Sí, la moneda llegó a estar a 10 pesos por dólar y el problema de las autoridades financieras no era analizar cómo parar una devaluación (algo con lo que los funcionarios financieros mexicanos han venido lidiando durante décadas) ¡sino cómo evitar que el precio se siguiera apreciando!

Por ello, el 25 de julio la comisión de cambios, (formada de manera paritaria por funcionarios el Ministerio de Hacienda y el Banco de México, aunque con voto de calidad de la primera) anunció que el Banco de México dejaría de subastar dólares, es decir, explícitamente disminuiría la oferta de dólares para inducir una depreciación del tipo de cambio, una situación inédita.

Nuestro rating

- 2.25: 405 lectores (la mayoría de closet) no pueden estar equivocados

La Columna en tu e-mail

Recibe las actualizaciones de La Columna por Correo-e

Protagonistas y protagonismos

5 de julio AJ H1N1 Amalia García Andrés Manuel López Obrador Carlos Ahumada Carlos Salinas de Gortari Carmen Aristegui cepa H1N1 Chilmalhua Clara Brugada Cámara de Diputados derecho de réplica DF Eduardo Bours Encuestas Enrique Peña Nieto Estado de México Felipe Calderón Fernando Elizondo Fidel Herrera Fútbol Germán Martínez guardería ABC Hermosillo Hidalgo IFE influenza influenza estacional

BANCO DE MÉXICO

Referencia 5

DIARIO OFICIAL DE LA FEDERACIÓN

www.dof.gob.mx

Ejemplar de hoy | Trámites | Servicios | Leyes y Reglamentos | Preguntas Frecuentes

SI EL DOCUMENTO SE PRESENTA INCOMPLETO EN EL MARGEN DERECHO, ES QUE CONTIENE TABLAS QUE REBASAN EL ANCHO PREDETERMINADO. SI ES EL CASO, HAGA CLICK AQUÍ PARA VISUALIZARLO CORRECTAMENTE

DOF: 02/03/2012

CIRCULAR 5/2012, dirigida a las Instituciones de Crédito, Casas de Bolsa, Sociedades de Inversión, Sociedades de Inversión Especializadas de Fondos para el Retiro y a la Financiera Rural, relativa a las Subastas para la Colocación de Valores Gubernamentales y de Valores del IPAB.

Al margen un logotipo, que dice: Banco de México.

CIRCULAR 5/2012

A LAS INSTITUCIONES DE CRÉDITO, CASAS DE BOLSA, SOCIEDADES DE INVERSIÓN, SOCIEDADES DE INVERSIÓN ESPECIALIZADAS DE FONDOS PARA EL RETIRO Y A LA FINANCIERA RURAL:

ASUNTO: SUBASTAS PARA LA COLOCACIÓN DE VALORES GUBERNAMENTALES Y DE VALORES DEL IPAB

El Banco de México, en su carácter de agente financiero del Gobierno Federal de los Estados Unidos Mexicanos y del Instituto para la Protección al Ahorro Bancario (IPAB), con el propósito de continuar promoviendo el sano desarrollo del sistema financiero considera conveniente uniformar y compilar en un solo ordenamiento la regulación relativa a las subastas para la colocación de valores gubernamentales y de valores del IPAB, aplicable a las instituciones de crédito y a la Financiera Rural, así como a las casas de bolsa, sociedades de inversión y sociedades de inversión especializadas de fondos para el retiro, contenida actualmente, entre otras disposiciones, en el Anexo 6 de la Circular 2019/95, dirigida a las instituciones de banca múltiple; en el Anexo 3 de la Circular 1/2006, dirigida a las instituciones de banca de desarrollo y a la Financiera Rural; en los Apéndices 1 y 2 del Anexo 3 de la Circular 115/2002, dirigida a las casas de bolsa, y en la Circular 2/2002, dirigida a las sociedades de inversión y sociedades de inversión especializadas de fondos para el retiro.

Adicionalmente, para facilitar la consulta de la Circular se incluyen títulos para cada uno de los artículos con la intención de que sirvan como guía para la pronta identificación de su contenido, no obstante que tales títulos no forman parte de los artículos.

Por lo anterior, con fundamento en los artículos 28 de la Constitución Política de los Estados Unidos Mexicanos, párrafos sexto y séptimo; 3o. fracción III, 7o. fracción I, 8o., 10, 14 y 24 de la Ley del Banco de México; 9o. de la Ley Orgánica de Nacional Financiera; 6o. de la Ley Orgánica de Sociedad Hipotecaria Federal; 9o. de la Ley Orgánica del Banco del Ahorro Nacional y Servicios Financieros, 9o. de la Ley Orgánica del Banco Nacional de Comercio Exterior; 10 de la Ley Orgánica del Banco Nacional de Obras y Servicios Públicos; 5o. de la Ley Orgánica del Banco Nacional del Ejército, Fuerza Aérea y Armada; 18 y 19 de la Ley Orgánica de la Financiera Rural; 2o. de la Ley de Ingresos de la Federación para el Ejercicio Fiscal de 2012; 22 de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros; 4o. párrafo primero, 8o. párrafos cuarto y séptimo; 10 párrafo primero, 12 párrafo primero en relación con el 19 fracciones II y VII, y 14 Bis párrafo primero en relación con el 17 fracción I del Reglamento Interior del Banco de México, que le otorgan la atribución de expedir disposiciones a través de la Dirección General de Operaciones de Banca Central y de la Dirección General Jurídica, respectivamente, así como en el artículo Segundo fracciones VII y XI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, ha resuelto expedir las siguientes

REGLAS DE LAS SUBASTAS PARA LA COLOCACIÓN DE VALORES GUBERNAMENTALES Y DE VALORES DEL IPAB

CAPÍTULO I

DISPOSICIONES PRELIMINARES

Definiciones

Artículo 1o.- Para fines de brevedad, en singular o plural, en estas Reglas se entenderá por:

Banco:	al Banco de México, actuando en su carácter de agente financiero.
BONDES:	a los Bonos de Desarrollo del Gobierno Federal de los Estados Unidos Mexicanos, denominados en moneda nacional y en UDIS, tanto a tasa de interés fija como a tasa de interés variable.
CETES:	a los Certificados de la Tesorería de la Federación emitidos por el Gobierno Federal de los Estados Unidos Mexicanos.
Días Hábiles Bancarios:	a los días en que las entidades financieras no estén obligadas a cerrar sus puertas ni a suspender operaciones, en términos de las disposiciones de carácter general que, para tal efecto, emite la Comisión Nacional Bancaria y de Valores.
IPAB:	al Instituto para la Protección al Ahorro Bancario.
SIAC-BANXICO:	al Sistema de Atención a Cuentahabientes de Banco de México.
UDIS:	a las unidades de cuenta, cuyo valor en moneda nacional publica el

CONSULTA

Mar 2012

Do	Lu	Ma	Mi	Ju	Vi	Sá
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Crear Usuario
Búsqueda Avanzada
Novedades
Top Notas
Normas Oficiales
Suscripción
Quejas y Sugerencias
Obtener Copia del DOF
Publicaciones Relevantes
Verificar Copia del DOF
Enlaces Relevantes
Contáctenos
Filtro RSS
Historia del Diario Oficial
Estadísticas
Vacantes en Gobierno
Ex-trabajadores Migratorios

Traducir esta página

Inglés

La traducción es automática y puede contener errores o inconsistencias

INDICADORES

Tipo de Cambio y Tasas al 15/11/2018

DOLAR	UDIS
20.3979	6.149584
TIIE 28 DIAS	TIIE 91 DIAS
8.1223%	8.3228%
TIIE 182 DIAS	
8.4689%	

Ver más

BANCO DE MÉXICO

Referencia 6

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

Order Code RL32331

CRS Report for Congress
Received through the CRS Web

The Economic Impact of Cyber-Attacks

April 1, 2004

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

Forbes
(/)

Javier Arreola (https://www.forbes.com.mx/author/javier-arreola/)
mayo 20, 2016 @ 2:00 pm

Ciberseguridad (casi) a prueba del enemigo 'invisible'

Ni las compañías más grandes del mundo ni los gobiernos han podido evitar los ataques cibernéticos, y aun así es posible que tengas una ciberseguridad casi al 100% si sigues las recomendaciones de los expertos.

Donald Rumsfeld, ex secretario de Defensa de Estados Unidos, quiso decir –en una famosa conferencia de prensa– que hay riesgos altos y riesgos bajos, y que hay riesgos que se ven y otros que no se ven. (Graham, 2014) Pero al combinar estos conceptos encontramos un cuadrante muy útil para tratar los temas de seguridad.

Por ejemplo, las personas saben que dejar abierta la puerta de su casa es un riesgo alto y visible. También podemos encontrar riesgos bajos que aún alcanzamos a ver, como la posibilidad de cruzar la calle cuando el semáforo está en rojo y que un vehículo "se lo pase" y te atropelle. Y hay riesgos bajos que no alcanzamos a ver, como que te roben la cartera en un lugar público y que al llegar a tu casa la busques y concluyas que la perdiste.

Sin embargo, los riesgos altos que no alcanzamos a ver son el tema de este artículo. Por ejemplo, la posibilidad de que alguien entre a tu casa, extraiga algo que tengas guardado, y salga de ella sin que te des cuenta. En temas cibernéticos, esto es más común de lo que parece: hackers entran a tu correo, cibercriminales que

MÁS COBERTURA

Equipo de López Obrador presenta la segunda parte de Pejenomics (https://www.forbes.com.mx/equi de-lopez-obrador-presenta-la-segunda-parte-de-pejenomics/)

ONU condena uso excesivo de la fuerza de Israel contra palestinos (https://www.forbes.com.mx/onu-condena-uso-excesivo-de-la-fuerza-de-israel-contra-palestinos/)

SCJN otorga amparo a Ríos Piter para consumo recreativo de mariguana (https://www.forbes.com.mx/scjn-otorga-amparo-a-rios-piter-para-consumo-recreativo-de-mariguana/)

REFERENCIA 9

Informe Norton sobre Ciberseguridad 2016

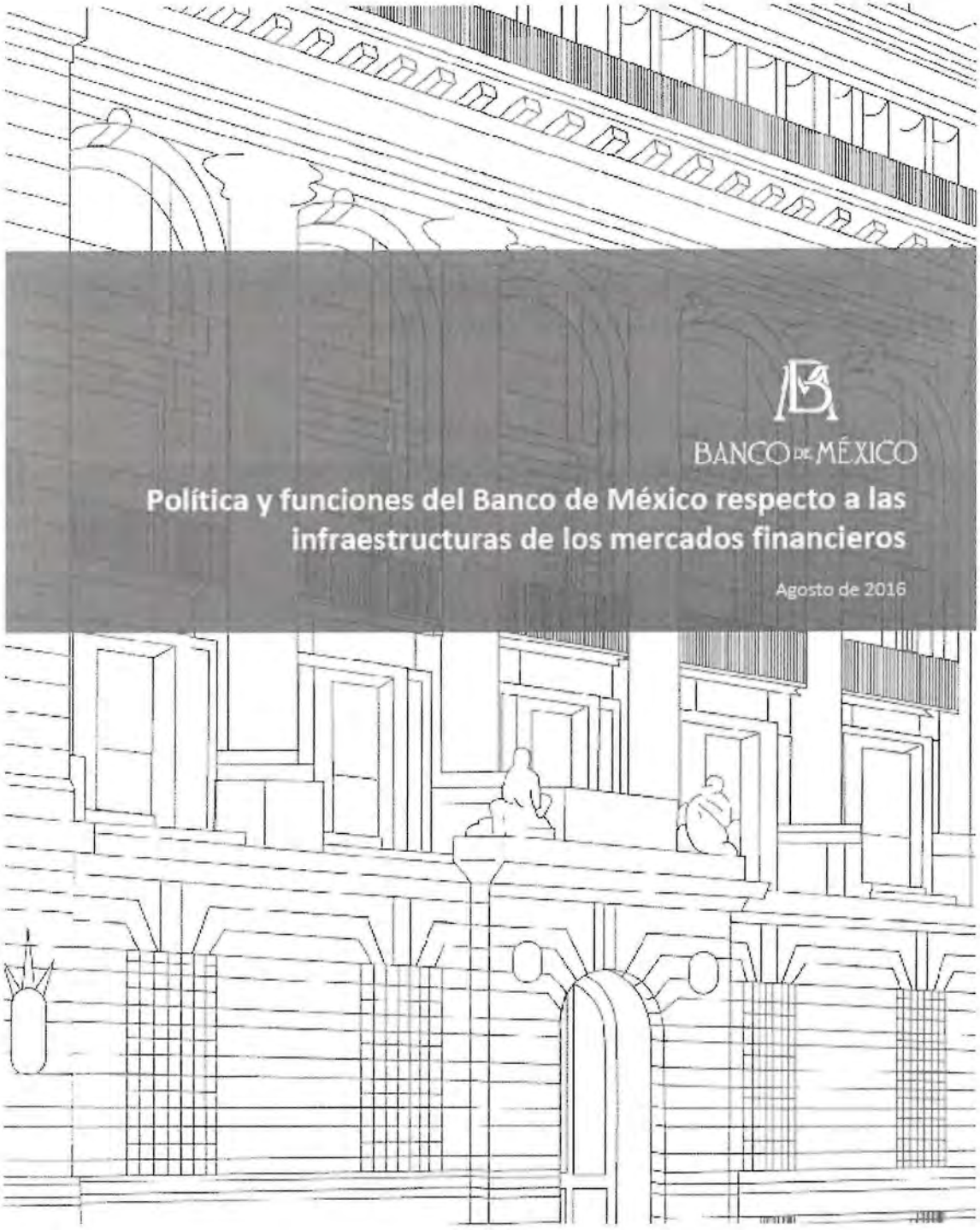
Comparaciones Globales

PRINCIPALES CONCLUSIONES	MÉXICO	GLOBAL (21 países)
Total de consumidores afectados por el cibercrimen en el último año	**22.4 millones (45%)**	689.4 millones (31%)
Total de costos financieros causados por el cibercrimen en el último año	**$5,500 millones (USD)**	$125,900 millones (USD)
Total de tiempo perdido por el cibercrimen en el último año	**28.8 horas**	19.7 horas
Los crímenes cibernéticos más comunes que han experimentado los consumidores	**Robo de dispositivo móvil: 33% Robo de contraseña:26% Correo electrónico hackeado: 20%**	Robo de contraseña: 18% Correo electrónico hackeado: 16% Robo de dispositivo móvil: 15%
Porcentaje de usuarios que no pueden identificar un correo electrónico "phishing" o suponen que es legítimo	**30%**	41%
Porcentaje de usuarios que han experimentado una consecuencia negativa después de responder a un correo electrónico "phishing"	**68%**	80%
Porcentaje de personas que se consideran capaces de determinar si usan una red de Wi-Fi segura	**61%**	48%
Dispositivo doméstico con mayor probabilidad de ser protegido por los encuestados	**Sistema de seguridad en casa: 79%**	Sistema de seguridad en casa: 76%
Porcentaje que piensa que los dispositivos domésticos conectados ofrecen a los hackers nuevas formas de robar datos	**71%**	72%
Porcentaje de personas que piensan que los dispositivos domésticos conectados están diseñados considerando la seguridad	**64%**	62%
Porcentaje con al menos un dispositivo no protegido	**39%**	35%
Porcentaje que confía en su capacidad para mantener segura la información personal en línea	**43%**	40%
Porcentaje que cree que es más difícil mantenerse a salvo y seguro en línea en los últimos 5 años	**65%**	63%
Porcentaje de padres que creen que sus hijos son más propensos a ser intimidados en línea que en un patio de recreo	**48%**	48%
Porcentaje que cree que los niños están expuestos a más peligros en línea ahora que hace 5 años	**86%**	78%

Norton

BANCO DE MÉXICO

REFERENCIA 10



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

(http://

Informe Semanal del Vocero

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

Informe Semanal del Vocero

Autor
Secretaría de Hacienda y Crédito Público

Fecha de publicación
29 de octubre de 2017

Categoría
Comunicado

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

BANCO DE MÉXICO

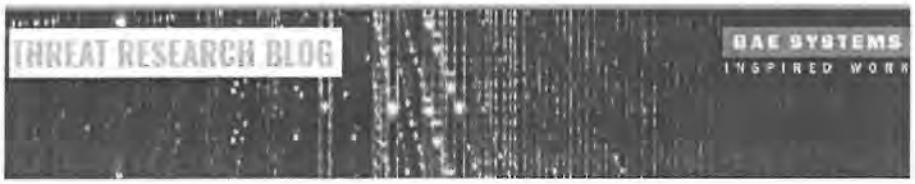
REFERENCIA 13

Más golrans@gmail.com Escritorio Cerrar sesión

BAE SYSTEMS THREAT RESEARCH BLOG

Resources Contact us

Home Products Solutions News & Events Partners About Us Careers



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.

POPULAR POSTS


TWO BYTES TO $951M


MAHACRYPTOR RANSOMWORM


CYBER HEIST ATTRIBUTION

CONTACT

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

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

Article World Neurosurgery · June 2017

CITATION
1

READS
142

1 author:

Eastern Maine Medical Center

164 PUBLICATIONS 604 CITATIONS

SEE PROFILE

REFERENCIA 15

Descubren que Petya, el ataque que paralizó empresas de toda Europa, no secuestraba archivos sino que los borraba

Eduardo Marín
6/28/17 3:17pm •

13.9K 2 2

Imagen: Björn Olsson, bajo licencia Creative Commons.

Un nuevo ataque de ransomware, conocido como Petya, hizo que se paralizaran las actividades en un gran número de oficinas de compañías importantes en Europa, incluyendo aerolíneas, bancos y bufetes de abogados. Sin embargo, un nuevo análisis asegura que este ataque era mucho peor de lo que imaginamos.

BANCO DE MÉXICO

REFERENCIA 16

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 Mexico y América Latina.

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

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

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

Teléfono de Comunicación Social: 15551024

Descarga el comunicado (http://www.bancomext.com/wp-content/uploads/2018/01/2_COMUNICADO_DE_PRENSA_BANCOMEXT_18011[illegible].pdf)

BANCO DE MÉXICO

REFERENCIA 17

MENU

NENA News, Press, & Stories...: Home Page

Email to a Friend (/members/send.asp?in=119592)

DHS Bulletin on Denial of Service (TDoS) Attacks on PSAPs

Sunday, March 17, 2013 (0 Comments)
Posted by: Chris Nussman

The Department of Homeland Security (DHS) NCCIC - National Coordinating Center for Communications - the DHS Office of Emergency Communications, DHS - Office of Infrastructure Protection, Federal Communications Commission, the National Cyber and Forensics Training Alliance, the FBI-National Cyber Investigative Joint Task Force working in coordination with the National Emergency Number Association (NENA), the Association of Public Safety Communications Officials (APCO) International, Louisiana Fusion Center, Mansfield Police Department and telecommunications service providers to identify and mitigate the effects of a criminal Telephony Denial of Service (TDoS) against public safety communications, hospitals and ambulance services. This is for immediate dissemination to public safety answering points (PSAPs) and emergency communications centers and personnel.

Background: Information received from multiple jurisdictions indicates the possibility of attacks targeting the telephone systems of public sector entities. Dozens of such attacks have targeted the administrative PSAP lines (not the 911 emergency line). The perpetrators of the attack have launched high volume of calls against the target network, tying up the system from receiving legitimate calls. This type of attack is referred to as a TDoS or Telephony Denial of Service attack. These attacks are ongoing. Many similar attacks have occurred targeting various businesses and public entities, including the financial sector and other public emergency operations interests, including air ambulance, ambulance and hospital communications.

COBALT: EL CIBERCRIMEN ORGANIZADO GOLPEA LOS CAJEROS AUTOMÁTICOS EUROPEOS

By S21sec Posted 2016/11/23 In Ciberseguridad

El malware en cajeros automáticos (ATMs) es un asunto de gran actualidad y que genera una gran preocupación en el sector bancario. El número de ataques está creciendo muy rápidamente y **está afectando a toda clase de países y regiones.**

En julio de 2016, los cibercriminales consiguieron extraer un total de **2 millones de dólares** de 34 cajeros automáticos del banco taiwanés First Bank. En agosto de 2016, consiguieron atacar el banco estatal tailandés Government Savings Bank, permitiendo así a los cibercriminales hacerse con un botín de **350.000 dólares** en metálico y forzando al banco a desactivar **3300 cajeros** automáticos, o lo que es lo mismo, cerca de la mitad de su red. Tal y como ya anticipamos en un post anterior, era altamente probable que estos ataques se extendiesen a otros países y regiones, y ahora le ha tocado el **turno a Europa**.

Revista de Ciencias de Seguridad y Defensa (Vol. 1, No. 2, 2016)

EL CIBERESPACIO: EL NUEVO TEATRO DE GUERRA GLOBAL

Luis Recalde H.,
Universidad de las Fuerzas Armadas - ESPE

Resumen

Finalizada o controlada la tradicional guerra convencional, el mundo tiene un nuevo teatro de operaciones llamado ciberespacio. De allí se han desprendido diversos ataques que traspasaron las fronteras virtuales; así, la tecnología de vanguardia ha formulado el nuevo campo de batalla global, desarrollado por los nuevos sistemas cibernéticos.

Palabras clave: ciberespacio, fronteras virtuales, espacio tridimensional, ciberguerras

Introducción

El teatro de guerra es una zona del globo terráqueo relativamente extensa, compuesta por los espacios terrestres, marítimos y aéreos que están - o estarían - potencialmente implicados en operaciones de guerra. Bajo esta perspectiva, estaríamos hablando de una determinada zona geográfica "tangible" de la tierra compuesta por los dominios tridimensionales de las operaciones militares convencionales, y que puede estar involucrada en una acción bélica determinada.

Hace algunos siglos, cuando se comenzaron a estudiar las guerras, generalmente se analizaban las formas de enfrentamientos básicos, por ejemplo la falange griega o la romana, éstas se enfocaban en el empleo táctico de las fuerzas en un determinado teatro de operaciones, hasta que Jomini (1838) pensó que, siguiendo una serie de leyes, un contingente militar podría estar en condiciones de vencer más fácilmente. Estas leyes se referían no solo al enfrentamiento y al combate en sí (es decir, la táctica de la que todos se habían ocupado hasta ese entonces), sino también a la maniobra de aproximación y retirada y a la logística de sostenimiento de las operaciones. A la combinación sincronizada en el terreno de estos aspectos previos al hecho táctico se lo conoce hoy como el "arte operacional" (Vergara, 2003).

Mientras Clausewitz (1831), concebía que la guerra era demasiado compleja, impredecible y un arte muy especial, porque se ejercía sobre elementos que reaccionan en función de su empleo y conducción. Pero lo más importante es que quería probar la naturaleza fundamental de la guerra y su lugar en el espectro de la actividad humana, por lo que la guerra fue orientada a una sistematización en el pensamiento de la conducción militar que, para una mejor interpretación, la guerra podía definirse en tres niveles:

- El que fijaba las causas por las que se debía ir a la guerra, al que llamaron nivel estratégico
- El que entendía los movimientos (maniobras) y la logística de las tropas en el terreno, al que llamaron nivel operacional
- El de los enfrentamientos en sí, al que llamaron nivel táctico (Vergara, 2003).

Por lo tanto en la guerra tradicionalmente visualizada, las fuerzas militares beligerantes emplean sus medios en un espacio tridimensional definido (aire, mar y tierra), y que es uno de los elementos decisivos para la consecución de un objetivo preestablecido en el nivel estratégico militar.

DELTA

MY TRIPS BOOK A TRIP FLIGHT STATUS CHECK IN SIGN IN JOIN

INFORMATION ON [24]7.AI CYBER INCIDENT

OVERVIEW

Last updated on April 7, 2018, 9:00 ET

Last week, on March 28, Delta was notified by [24]7.ai, a company that provides online chat services for Delta and many other companies, that [24]7.ai had been involved in a cyber incident. It is our understanding that the incident occurred at [24]7.ai from Sept. 26 to Oct. 12, 2017 and that during this time certain customer payment information for [24]7.ai clients, including Delta, may have been accessed – no other customer personal information, such as passport, government ID, security or SkyMiles information was impacted. **Delta customers who believe they could be impacted, should visit** https://delta.alvaotd.com **to enroll in the free protection services being offered.**

Upon being notified of [24]7.ai's incident last week, Delta immediately began working with [24]7.ai to understand any potential impact the incident had on Delta customers, delta.com, or any Delta computer system. We also engaged federal law enforcement and forensic teams, and have confirmed that the incident was resolved by [24]7.ai last October. At this point, even though only a small subset of our customers would have been exposed, we cannot say definitively whether any of our customers' information was actually accessed or subsequently compromised.

We appreciate and understand that this information is concerning to our customers. The security and confidentiality of our customers' information is of critical importance to us and a responsibility we take extremely seriously. We will be updating http://www.delta.com/response regularly to address customer questions and concerns. We will also be directly contacting customers who may have been impacted by the [24]7.ai cyber incident. In the event any of our customers' payment cards were used fraudulently as a result of the [24]7.ai cyber incident, we will ensure our customers are not responsible for that activity.

+ Click to enlarge

FREQUENTLY ASKED QUESTIONS

1. **How did [24]7.ai's cyber incident occur?**
   - [24]7.ai is a company that provides online chat services for many companies, including Delta.
   - We understand malware present in [24]7.ai's software between Sept. 26 and Oct. 12, 2017, made unauthorized access possible for the following fields of information when manually completing a payment card purchase on any page of the delta.com desktop platform during the same timeframe: name, address, payment card number, CW number, and expiration date.
   - *No other customer personal information, such as passport, government ID, security or SkyMiles information was impacted.*
2. **What customers were impacted?**
   - At this point, we understand that the malware was present for a short period of time and potentially exposed several hundred thousand customers.
   - While we believe we have identified with some precision the transactions that could have been impacted, we cannot say definitively whether any of our customers' information was actually accessed or subsequently compromised.
   - There was no impact to the fly.Delta app, mobile.delta.com or any other Delta computer system. Payment card information for those customers who used Delta Wallet to complete transactions was not compromised. The malware could only collect the information shown on the screen, so credit card information automatically populated by Delta Wallet functionality would have remained masked and not useable.
   - Customers did not have to interact with the online chat tool to be impacted.
3. **What is Delta doing to make this right for customers?**
   - Delta launched www.delta.com/response, a dedicated website, on April 5 at noon ET, which we will be updating regularly to address customer questions and concerns.
   - Delta will be working diligently to directly contact customers, including by first-class postal mail, who may have been impacted by the [24]7.ai cyber incident.

Technology

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

By Michael Riley and Alan Katz
26 de mayo de 2016 8:36 GMT-5
Updated on 26 de mayo de 2016 15:21 GMT-5

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

Swift Hack Investigation Expands to Southeast Asia

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

Recuadro 7
RIESGO CIBERNÉTICO: RELEVANCIA Y ENFOQUES PARA SU REGULACIÓN Y SUPERVISIÓN

Felipe Clavijo Ramírez
Daniel Osorio
Eduardo Yanquen*

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

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

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

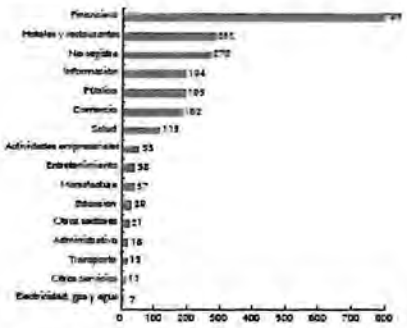
La forma más común como se ha materializado el riesgo cibernético en años recientes ha sido mediante lo que se conoce como ataques cibernéticos. En esencia, estos son acciones ilegales realizadas por *hackers*, con el objetivo principal de obtener cierto beneficio, al generar daños en los sistemas tecnológicos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

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

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

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

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



Fuente: Verizon (2016).

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

News

Symantec reveals more hack attempts on Swift network

Written by Antony Peyton (https://www.bankingtech.com/author/antonypeyton/) 11 Oct 2016

Symantec has found evidence that the Odinaff group has mounted attacks on Swift users, using malware to hide customers' own records of Swift messages relating to fraudulent transactions.

The tools used are designed to monitor customers' local message logs for keywords relating to certain transactions. They will then move these logs out of customers' local Swift software environment. Symantec says it has no indication that Swift network was itself compromised.

(https://www.bankingtech.com/file
1.png)
Odinaff attacks by region (IMAGE: Symantec) Click to enlarge

Symantec says these Odinaff attacks are an example of another group believed to be involved in this kind of activity, following the Bangladesh central bank heist (https://www.bankingtech.com/455732/typo-spells-confusion-in-101m-cyber-bank-heist/) linked to the Lazarus group.

There are no apparent links between Odinaff's attacks and the attacks on banks' Swift environments attributed to Lazarus and the Swift-related malware used by the Odinaff group bears no resemblance to Trojan.Banswift, the malware used in the Lazarus-linked attacks.

But Symantec notes that the attacks involving Odinaff share some links to the Carbanak group, whose activities became public in late 2014. Carbanak also specialises in high-value attacks against financial institutions and has been implicated in a string of attacks against banks in addition to point of sale (PoS) intrusions.

This is bad news for Swift but its fight back against these attacks has been extensive and ongoing. It has spoken strongly (https://www.bankingtech.com/595372/swift-issues-plea-to-collaborate-in-fight-against-cybercrime/) on the subject and recently unveiled SwiftSmart (https://www.bankingtech.com/602332/swift-smart-modules-seek-stronger-security/) modules to help its customers operate their Swift environment "securely and in-line with best practice". This move is also a "critical part" of its Customer Security Programme

BANCO DE MÉXICO

REFERENCIA 24

BANCO DE MÉXICO

REFERENCIA 25

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.**

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

+2
2 Votes

Social Engineering Fundamentals, Part I: Hacker Tactics

By: Ω

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/125624)

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 28

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.

BANCO DE MÉXICO

REFERENCIA 29

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real.

Fecha de consulta: 26/09/2018 12:59:39

Título	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios SPEI®, Número de operaciones	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios SPEI®, Importe (millones de pesos)
Periodo disponible	Ene 1992 - Ago 2018	Ene 1992 - Ago 2018
Periodicidad	Mensual	Mensual
Cifra	Volumen	Flujos
Unidad	Operaciones	Millones de Pesos
Base		
Aviso		
Tipo de información	Niveles	Niveles
Fecha	SF46188	SF46189
Ene 2017	35,016,703	23,877,271
Feb 2017	34,817,472	21,505,024
Mar 2017	40,016,546	26,180,217
Abr 2017	35,954,794	20,494,020
May 2017	37,831,714	21,984,690
Jun 2017	43,806,037	23,093,365
Jul 2017	35,242,331	21,576,446
Ago 2017	42,207,091	22,005,722
Sep 2017	42,473,998	21,881,177
Oct 2017	40,172,877	22,509,386
Nov 2017	43,888,894	21,719,416
Dic 2017	48,576,208	23,658,129
Ene 2018	43,696,159	24,177,775
Feb 2018	43,392,790	20,965,410
Mar 2018	46,956,342	23,580,617
Abr 2018	49,608,372	23,993,595
May 2018	46,106,472	22,005,913
Jun 2018	53,607,479	23,215,548
Jul 2018	46,293,171	21,428,148
Ago 2018	56,288,104	22,102,662

BANCO DE MÉXICO

Ciudad de México, a 16 de noviembre de 2018.

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

Nos referimos a la solicitud de acceso a la información identificada con el número de folio **6110000057718,** que nos turnó la Unidad de Transparencia el diecisiete de octubre del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

> *"Necesito de todos los servidores públicos los registros de las llamas recibidas y realizadas del mes de septiembre a la fecha, y en caso de grabarlas las de las última semana a la fecha de la presentación de esta solicitud, desde luego de linea oficial asignada."*

Al respecto, nos permitimos informarles que, en términos de lo dispuesto por los artículos 100 y 106, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública; así como 97 y 98, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, esta unidad administrativa ha determinado clasificar la información relativa a la totalidad de **las grabaciones de las llamadas realizadas o recibidas a través de las Extensiones Telefónicas Seleccionadas, del personal de la Oficina de Comercialización Numismática adscrita a la Dirección de Administración de Emisión,** en términos de los siguientes fundamentos y motivos:

INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL

Conforme a la disposición Sexta de la Norma Administrativa Interna "Administración del sistema de seguimiento de extensiones telefónicas" (NAI), las Extensiones Telefónicas Seleccionadas (ETS) serán aquellas extensiones que se ubiquen en las instalaciones del Banco, destinadas a hacer y recibir llamadas para:

a. La negociación, concertación, celebración, conciliación, trámite, formalización o ejecución de actos u operaciones, cuyo registro y conservación sean necesarios para acreditar y, en su caso revisar, los términos y condiciones en que fueron realizadas.

b. Reportar emergencias o hechos que deban ser atendidos con urgencia, relacionados con temas de protección civil y seguridad interna en las instalaciones del "Banco".

Por su parte, la disposición Quinta, de la NAI en comento, señala que la grabación de las llamadas realizadas o recibidas a través de las ETS, así como la consulta de dichas

grabaciones, son parte de las operaciones del Sistema de Seguimiento de Extensiones Telefónicas (SSET).
Asimismo, la disposición Décima de la NAI referida señala que las actividades de supervisión de la correcta operación de la infraestructura del SSET, se realizarán **sin consultar las grabaciones de las llamadas.**

La Décima cuarta disposición de la citada NAI, señala que la consulta de las grabaciones podrá realizarse tanto por los titulares de la Dirección General de Emisión, de la Dirección General de Operaciones y Sistemas de Pagos y la Coordinación Administrativa del Fondo Mexicano del Petróleo para la Estabilización y el Desarrollo, así como por los trabajadores especificados en la solicitud de la consulta. En relación con lo anterior, la disposición Décima quinta de la citada NAI, establece que serán los titulares de las unidades administrativas señaladas, los responsables del uso adecuado de la información obtenida a través de las grabaciones de las llamadas; y que la Dirección General de Tecnologías de la Información (DGTI) será responsable del debido resguardo de dicha información.

En adición a lo anterior, la disposición Décimo sexta de la NAI en comento, señala que las unidades administrativas referidas en el párrafo precedente, deberán salvaguardar el derecho a la **intimidad o privacidad** de las personas que intervengan en las conversaciones grabadas.

De conformidad con lo dispuesto en los artículos 116, párrafo primero, de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública: y el Trigésimo octavo, fracción I, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, es confidencial la información que contenga datos personales concernientes a una persona identificada o identificable.

En este sentido se hace notar la **confidencialidad** de las grabaciones de las llamadas realizadas y recibidas por los trabajadores de la Oficina de Comercialización Numismática adscrita a la Dirección de Administración de Emisión, a través de las ETS, en virtud de que los datos personales que pudieran contener dichas llamadas, tienen información de la cual pueden ser titulares los interlocutores con quienes interactúan los servidores públicos de la unidad administrativa antes señalada.

En efecto, las llamadas que reciben o efectúan los servidores públicos de las unidades administrativas en cuestión, a través de las extensiones destinadas para los fines descritos en el inciso **a.**, disposición Sexta de la NAI, pueden contener datos personales, mismos que no pueden ser disociados de las grabaciones de llamadas telefónicas en los formatos en que se encuentran.

Lo anterior, máxime que la autodeterminación informativa de los titulares de la información contenida en las llamadas telefónicas grabadas en virtud de la NAI, no se pierde en función de la naturaleza y características del equipo telefónico del que recibieron las llamadas en su momento, ni porque en las mismas intervengan servidores públicos.

En ese sentido, se observa una imposibilidad para los sujetos obligados de identificar y disociar el contenido en concreto de las llamadas telefónicas en cuestión que tenga el carácter de públicos y cuál debe ser protegido.

En adición a lo anterior, considerando que la fecha de ingreso de la misma fue el dieciséis de octubre del presente año, y que las grabaciones de las llamadas requeridas, corresponden al periodo de 8 al 16 de octubre del presente año. En tal sentido, resulta evidente que existe una incapacidad material y técnica para la revisión de cada una de las llamadas para determinar su naturaleza, así como para la elaboración de versiones públicas en virtud del formato en que se encuentra la información solicitada.

Atento a lo expuesto, fundado y motivado, estas unidades administrativas determinan clasificar como **confidencial** la información relativa a la totalidad de **las grabaciones de las llamadas realizadas o recibidas a través de las Extensiones Telefónicas Seleccionadas, del personal de la Oficina de Comercialización Numismática adscrita a la Dirección de Administración de Emisión.**

2. INFORMACIÓN CLASIFICADA COMO RESERVADA

Se debe señalar que la Dirección de Administración de Emisión, tiene entre sus atribuciones la de comercializar monedas en metales finos, por lo que en virtud del ejercicio de ésta atribución se graban las extensiones del personal de la Oficina de Comercialización Numismática.

En ese sentido, y en virtud de la imposibilidad de identificar y disociar el contenido en concreto de las llamadas telefónicas en cuestión que tenga el carácter de público y cuál debe ser protegido, a efecto de determinar la naturaleza de dichas llamadas, esta unidad administrativa determina clasificar como **reservada** la información relativa a la totalidad de **las grabaciones de las llamadas realizadas o recibidas a través de las Extensiones Telefónicas Seleccionadas, del personal de la Oficina de Comercialización Numismática adscrita a la Dirección de Administración de Emisión,** en términos de la fundamentación y motivación expuestos en la prueba de daño que se adjunta al presente oficio.

Por lo expuesto, en términos de los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de

BANCO DE MÉXICO

Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México, solicitamos a ese órgano colegiado confirmar la clasificación referida.

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informo que el personal que por la naturaleza de sus atribuciones tiene acceso al documento clasificado es el Director General de Emisión, y el personal con nivel de Gerente o superior, al que le otorgue privilegios de acceso para consulta de las grabaciones.

Quedamos a sus órdenes, para cualquier aclaración o comentario adicional.

Atentamente,

MTRO. CARLOS GUTIÉRREZ CAPPELLO
Gerente de Gestión de la Dirección General de Emisión
En suplencia por ausencia de la Directora de Administración de Emisión, en términos del artículo 66, del Reglamento Interior del Banco de México.

BANCO DE MÉXICO
RECIBIDO
[illegible] 2018
Comité de Transparencia
Por: [illegible] Hora: 11:00

Recibo este oficio en cuatro páginas y una prueba de daño.

PRUEBA DE DAÑO

Totalidad de las grabaciones de las llamadas realizadas o recibidas a través de las Extensiones Telefónicas Seleccionadas, del personal de la **Oficina de Comercialización Numismática adscrita a la** ***Dirección de Administración de Emisión***

En términos de lo dispuesto en los artículos 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos, 113, fracciones V y VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracciones V y VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como el Vigésimo tercero 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, es de clasificarse como información reservada aquella cuya publicación, entre otras cosas:

- Pueda poner en riesgo la vida, seguridad o salud de personas físicas.
- Obstruya la prevención de los delitos.

Por lo que la información relativa a la ***"Totalidad de las grabaciones de las llamadas realizadas o recibidas a través de las Extensiones Telefónicas Seleccionadas, del personal de la Oficina de Comercialización Numismática adscrita a la Dirección de Administración de Emisión"***, es clasificada como reservada, ya que la divulgación de la citada información representa un riesgo de perjuicio significativo al interés público, toda vez que dicho riesgo es:

1) Real, pues revelar o divulgar información materia de la presente proporcionaría datos que pueden ser utilizados para la planeación y ejecución de actividades ilícitas, como robos, atentados y/o secuestros, lo que pondría en riesgo a los empleados del Banco de México, encargados de su custodia, resguardo y distribución, a sus instalaciones y a las contrapartes autorizados para la comercialización y distribución de dichos productos numismáticos en metales finos.

Lo anterior, en virtud de que a través de las llamadas realizadas o recibidas en las Extensiones Telefónicas Seleccionadas, y asignadas a los trabajadores de la Oficina de Comercialización Numismática adscrita a la Dirección de Administración de Emisión, relativas a la negociación respecto de la comercialización de piezas numismáticas acuñadas en metales finos, se establecen **cantidades, fechas y lugares** de los pagos y entrega que se pudieran generar en dichas negociaciones, mismos que al estar relacionados con productos elaborados en metales preciosos, y en cantidades de piezas, ascienden a importes considerables.

En tal virtud, personas o grupos de personas con intenciones delictivas pudieran aprovechar la información proporcionada para realizar hechos constitutivos de delitos en contra de los servidores públicos del Banco de México, de las instalaciones en las que se resguardan las piezas numismáticas referidas, o de las contrapartes, entre otras con la finalidad de sustraer la piezas numismáticas en metales preciosos o el numerario con el que se efectuaría el pago, lo que pondría en riesgo la vida, seguridad o salud de personas físicas.

En consecuencia, resulta evidente que el otorgamiento de la información materia de la presente, actualiza las causales de reserva previstas en los artículos 113, fracciones V y VII, de la Ley General de Transparencia y Acceso a la Información Pública, y 110, fracciones V y VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

En este sentido, conforme a la experiencia en el contexto de seguridad y robo, un modo de operación común de los grupos dedicados a la comisión de delitos como el robo se facilita o logra, a través del conocimiento y

divulgación de información como la contenida en la ***"Totalidad de las grabaciones de las llamadas realizadas o recibidas a través de las Extensiones Telefónicas Seleccionadas, del personal de la Oficina de Comercialización Numismática adscrita a la Dirección de Administración de Emisión"***, entre otra, la relativa a la cantidad, fecha y lugar de pago, por lo que el hecho de divulgarla, es decir, hacerla del dominio público, implicaría un riesgo y una amenaza inminente a las instalaciones en las que se resguardan las piezas numismáticas en metales preciosos referidas, así como al personal que labora en el mismo, y a las contrapartes autorizadas para su comercialización, ya que dicha información puede ser utilizada por diversos grupos delincuenciales para planear ataques o robos a dichas instalaciones y personas, con lo que se pone en riesgo la vida, seguridad o salud de las mismas.

2) Demostrable, se han presentado acontecimientos violentos relacionados con el robo de piezas numismáticas en México y el mundo por lo que se trata de una amenaza constante y por tal motivo, es importante mencionar que el actuar de la delincuencia organizada, normalmente conlleva a la pérdida de vidas humanas, y en la actualidad, ésta mantiene una constante actividad delictiva tanto a nivel nacional como internacional.

Para evidenciar la realización de las actividades delictivas descritas, se enuncian los siguientes acontecimientos hechos del conocimiento del público a través de medios de circulación nacional e internacional:

1. En la Ciudad de México, a principios del año 2000, fue robada la escultura denominada "Corrunus" obra de Leonora Carrington y que formaba parte de la exposición "Libertad en bronce 2000" del Paseo de la Reforma.[1]

2. En Argentina, a principios de 2008 se dio el robo del Museo Numismático e Histórico del Banco Nación, los asaltantes sustrajeron piezas por un valor de 750 mil dólares.[2]

3. En Illinois, en 2009 durante la descarga de piezas para una exhibición numismática fue asaltado y agredido un distribuidor. El importe de lo robado fue de alrededor de $65,000 USD.[3]

4. En Octubre de 2014, un reloj suizo valuado en 500 mil dólares (7 millones de pesos) fue robado durante un evento realizado en el hotel St. Regis de la capital mexicana.[4]

5. En julio de 2015, en Cheyenne, Wyoming, se cometió un robo y asesinato doble en una tienda local de productos numismáticos.[5]

---

[1] Fuente: (enero 2000) "Roban escultura de Carrington ".Sitio web: http://www.jornada.unam.mx/2000/02/01/roban.html

[2] Fuente: (10 de mayo de 2008) "Cae la banda que robó las monedas del Nación ". Consultado el 11 de marzo de 2016. Periódico La Nación. Sitio web: http://www.lanacion.com.ar/1011376-cae-la-banda-que-robo-las-monedas-del-nacion

[3] Fuente: (04/05/2009) "Dealer Robbed While Unloading at Illinois Coin Show". Consultado el 16 de marzo de 2016. Sitio web: http://www.numismaticcrimes.org/?q=reports&page=8

[4] Fuente: (25/10/2014) "Roban reloj valuado en 7 millones de pesos durante exhibición en el DF". Sitio web: http://www.proceso.com.mx/395777/roban-reloj-valuado-en-7-millones-de-pesos-durante-exhibicion

[5] Fuente: (07/21/2015) "Cheyenne Coin Dealer Murdered". Consultado 1 de abril de 2016. Sitio web: http://www.numismaticcrimes.org/?q=node/513

6. En Florida, también en 2015, un distribuidor numismático fue asaltado y golpeado con serias lesiones camino a su tienda. El importe de lo robado fue de aproximadamente $40,000 USD en diversas piezas numismáticas que transportaba en su maletín.[6]

7. En la Ciudad de México, en 2016, se presentó el caso de un robo de 12 pinturas valuadas en $20,000 USD durante su traslado. Estas piezas formaban parte de una exposición.[7]

8. En marzo de 2017, la moneda de oro más grande del mundo, llamada "Big Maple Leaf", desapareció del lugar en el que estaba expuesta en el Museo Bode, en Berlín; el robo se llevó a cabo en la madrugada. La policía de Berlín cree que el o los responsables del robo rompieron una ventana en la parte trasera del museo. Tras revisar la zona, encontraron una escalera en las vías del tren. No está claro cómo hicieron los ladrones para evadir el sistema de alarmas o para cargar la moneda.[8]

9. En abril de 2018, roban el Museo Dobrée de Nantes. Varios individuos entraron al museo y robaron el relicario del corazón de Ana de Bretaña. Junto al relicario, los ladrones robaron también una importante colección de monedas y medallas medievales de oro. La lista es de 57 monedas y 10 medallas. [9]

10. En Vista, California en mayo de 2018, roban el "California Numismatic Funding". Algunos individuos ingresaron al edificio y tomaron una gran cantidad de monedas a granel en bolsas de lona, así como también lingotes de plata. [10]

11. En Nuevo León, México, en junio de 2018, roban en una casa alhajas y una colección de monedas. La afectada reportó que los delincuentes se llevaron un lote de joyas que estimó su valor en unos 400 mil pesos y una colección con al menos 250 monedas cuyo valor no fue revelado. [11]

12. En Cuauhtémoc, CDMX., en julio de 2018, aprovechan remodelación para robar Casa de Moneda de México. Debido a que la Casa de Moneda de México se encontraba en remodelación, fue asaltada por al menos cuatro hombres. Uno de ellos sorprendió al guardia de seguridad privada que custodiaba el inmueble ubicado en Paseo de la Reforma, informó el subsecretario de Operación Policial de la Zona Sur, Álvaro Sánchez Valdez. En este asalto participaron al menos cuatro personas, uno de los asaltantes sorprendió al vigilante preguntando por un empleado; después, lo amagó, dando oportunidad a que sus cómplices ingresaran y rompieran una vitrina donde se encontraban las monedas. Se desconoce el monto de lo robado, pero se tiene información de que en este inmueble había, tanto monedas antiguas, como otras elaboradas de oro y plata –como las llamadas onzas troy–, por lo que, de acuerdo con fuentes policiales consultadas, el botín pudo ser de al menos tres millones de pesos.[12]

[6] Fuente: (08/24/2015) "Aggravated Robbery (Dealer) Florida". Consultado el 16 de marzo de 2016. Sitio web: http://www.numismaticcrimes.org/?q=reports&page=4

[7] Fuente: (27/06/20106) "Roban a la ALDF pinturas valuadas en ¡20 mil dólares!". Sitio web: https://elbigdata.mx/2016/06/roban-a-la-aldf-pinturas-valuadas-en-20-mil-dolares/

[8] Fuente: (27/03/2017) "Cómo lograron robar en Berlín la moneda de oro más grande del mundo, de 100 kg de peso y valorada en US$4 millones". Sitio web: http://www.bbc.com/mundo/noticias-39412894

[9] Fuente: (18/04/2018) "ROBO EN EL MUSEO DOBRÉE DE NANTES: 57 MONEDAS Y 10 MEDALLAS DE ORO MEDIEVALES MAS EL CORAZÓN DE ORO DE ANA DE BRETAÑA". Sitio web: http://wearenumismatics.com/robo-monedas-corazon-ana-bretana-nantes/

[10] Fuente: (07/05/2018) "Coin Shop Burglary". Sitio web: https://coinweek.com/people-in-the-news/crime-and-fraud/numismatic-crime-information-center-update-for-may-7-2018/

[11] Fuente: (20/06/2018) "Roban en una casa 400 mil en joyas". Sitio web: https://www.pressreader.com/mexico/el-norte/20180620/282205126609196

Con relación a lo anterior, cabe destacar que se podrían enumerar más ejemplos relacionados con este ilícito, sin embargo, la finalidad de clasificar la información en cuestión radica en evitar poner en riesgo la vida y seguridad de personas físicas, dado el alto valor que llegan a adquirir algunas piezas numismáticas.

3) Identificable, ya que al tomar en consideración los casos antes expuestos, es notorio que existen grupos delictivos que cuentan con el desarrollo, sofisticación y capacidades operativas avanzadas para realizar este tipo de ataques, y el hecho de hacer pública la información que contienen las grabaciones de las llamadas realizadas o recibidas materia de la presente, pondría al alcance de estos grupos delictivos, las herramientas necesarias para la planeación y ejecución de los mismos, obteniendo fácilmente información exacta sobre aquellas piezas que resulten de mayor valor.

El riesgo de perjuicio que supondría la divulgación, supera el interés público general de que se difunda, pues dar a conocer la información clasificada, lejos de otorgar un beneficio a la sociedad, generaría riesgos en personas, cuestión que generaría inquietud en grupos delictivos, por consiguiente, no satisface un interés público, por el contrario, es información que pone en riesgo considerable la vida del personal que participa en la negociación relativa a la comercialización de las piezas referidas, así como, a los integrantes de la sociedad que podrían estar alrededor de un asalto o ataque.

Asimismo, el interés público se centra en que el Banco de México, como autoridad del Estado Mexicano, proteja los derechos humanos en acatamiento al artículo 1o. de la Constitución Federal, entre los cuales se encuentra, en primer lugar, el derecho a la vida, así como el derecho a la salud.

De igual manera, es también de interés público que el Banco Central cumpla con su mandato constitucional para satisfacer la demanda de la sociedad, por lo que revelar o divulgar la información clasificada no aporta un beneficio a la transparencia comparable con el perjuicio que representaría un atentado en contra de las personas referidas en la presente prueba de daño.

En efecto, revelar esta información otorgaría elementos que, facilitarían el conocimiento de las cantidades, fecha y lugar de pago, entre otra información, lo cual pondría en riesgo la vida de los servidores públicos del Banco de México o de las contrapartes.

[12] Fuente: (14/07/2018) "Aprovechan remodelación para robar Casa de Moneda de México". Sitio web: https://www.excelsior.com.mx/comunidad/aprovechan-remodelacion-para-robar-casa-de-moneda-de-mexico/1252673

En este sentido, el artículo 1o., tercer párrafo, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) señala que todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad.

Asimismo, el Pleno de la Suprema Corte de Justicia de la Nación (SCJN) ha sostenido que la CPEUM protege el derecho a la vida de todos los individuos, pues lo contempla como un derecho fundamental, sin el cual no cabe la existencia ni disfrute de los demás derechos. También ha señalado que la protección del derecho a la vida es un derecho inherente a la persona humana.

Es así que, en términos de la CPEUM y de la SCJN, el derecho a la vida no sólo es un derecho fundamental, sino que además es presupuesto necesario para el disfrute de los demás derechos. Por lo anterior, este derecho requiere de la máxima protección posible, lo que conlleva a que se adopten las medidas necesarias y efectivas para que no sea vulnerado.

Lo anterior ha sido reconocido por la LGTAIP, estableciendo en su artículo 113, fracción V, que es de reservarse la información que de divulgarse pondría en inminente riesgo la vida, seguridad o salud de las personas.

Asimismo, el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, al resolver el recurso RRA 0408/18, determinó que con la divulgación de información sobre medidas de seguridad implementadas para la protección de personas, como son su calidad, equipo y materiales utilizados, se aumenta el riesgo y la vulnerabilidad a la vida, seguridad o salud tanto de las personas a las que van dirigidas los mecanismos de protección, como a quienes proveen dicho servicio.

De igual manera, 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.

La reserva de la información relativa a la ***"Totalidad de las grabaciones de las llamadas realizadas o recibidas a través de las Extensiones Telefónicas Seleccionadas, del personal de la*** **Oficina de Comercialización Numismática adscrita a la** ***Dirección de Administración de Emisión"***, satisface un interés público, ya que llevando a cabo una ponderación entre el derecho de acceso a la información, la prevención de actividades ilícitas como robos, resulta más favorable a la población el proteger su vida.[13] En tal sentido, el bienestar social que se obtiene por no dar a

[13] **INTERPRETACIÓN CONFORME. SUS ALCANCES EN RELACIÓN CON EL PRINCIPIO DE INTERPRETACIÓN MÁS FAVORABLE A LA PERSONA.** El principio de interpretación conforme se fundamenta en el diverso de conservación legal, lo que supone que dicha interpretación está limitada por dos aspectos: uno subjetivo y otro objetivo; por un lado, aquél encuentra su límite en la voluntad del legislador, es decir, se relaciona con la funcionalidad y el alcance que el legislador imprimió a la norma y, por otro, el criterio objetivo es el resultado final o el propio texto de la norma en cuestión. En el caso de la voluntad objetiva del

conocer la información referida es más favorable a la sociedad en general, que el revelar información que pudiera poner en peligro su vida.

Por otro lado, la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que como se ha demostrado, el perjuicio que se causaría a personas, en caso de proporcionar la información en comento, sería mayor al beneficio personal de quien la obtenga. Asimismo, la reserva de la información materia de la presente resulta la forma menos restrictiva disponible para evitar un perjuicio mayor a la sociedad.

Es indispensable señalar que dar a conocer la información que nos ocupa compromete la vida, la seguridad y salud de personas físicas, riesgos de perjuicio claramente mayores a los que representaría el beneficio de divulgar la información al público en general. Por lo tanto, podemos concluir que revelar al público dicha información, no aporta un beneficio a la sociedad comparado con el perjuicio que podrían sufrir la salud, la seguridad y la vida de las personas involucradas.

Asimismo, debe prevalecer el interés público sobre el interés particular, toda vez que la protección al derecho a la vida, salud y seguridad de las personas aporta un mayor beneficio que el perjuicio que se obtendría de privilegiar el derecho humano al acceso a la información, máxime que el derecho a la vida, salud y seguridad de las personas constituyen una base y sustento para el ejercicio de otros derechos, como lo es el de acceso a la información, por lo que aquéllos deben prevalecer sobre éste e incluso cualquier otro derecho.

Lo anterior, como resultado de una prueba de interés público a través de la aplicación del principio de proporcionalidad , en razón de que es de explorado derecho que los derechos fundamentales a la vida y salud tienen un peso abstracto mayor que otros derechos, como el de acceso a la información, con indiferencia del peso

legislador, la interpretación conforme puede realizarse siempre y cuando el sentido normativo resultante de la ley no conlleve una distorsión, sino una atemperación o adecuación frente al texto original de la disposición normativa impugnada; asimismo, el principio de interpretación conforme se fundamenta en una presunción general de validez de las normas que tiene como propósito la conservación de las leyes; por ello, se trata de un método que opera antes de estimar inconstitucional o inconvencional un precepto legal. En ese sentido, sólo cuando exista una clara incompatibilidad o contradicción que se torne insalvable entre una norma ordinaria y la Constitución Política de los Estados Unidos Mexicanos o algún instrumento internacional, se realizará una declaración de inconstitucionalidad o, en su caso, de inconvencionalidad; por tanto, el operador jurídico, al utilizar el principio de interpretación conforme, deberá agotar todas las posibilidades de encontrar en la disposición normativa impugnada un significado que la haga compatible con la Constitución o con algún instrumento internacional. Al respecto, dicha técnica interpretativa está íntimamente vinculada con el principio de interpretación más favorable a la persona, el cual obliga a maximizar la interpretación conforme de todas las normas expedidas por el legislador al texto constitucional y a los instrumentos internacionales, en aquellos escenarios en los que permita la efectividad de los derechos humanos de las personas frente al vacío legislativo que previsiblemente pudiera ocasionar la declaración de inconstitucionalidad de la disposición de observancia general. Por tanto, mientras la interpretación conforme supone armonizar su contenido con el texto constitucional, el principio de interpretación más favorable a la persona lo potencia significativamente, al obligar al operador jurídico a optar por la disposición que más beneficie a la persona y en todo caso a la sociedad.

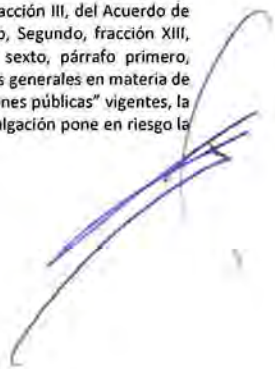
(Época: Décima Época; Registro: 2014204; Instancia: Pleno; Tipo de Tesis: Aislada; Fuente: Semanario Judicial de la Federación; Publicación: viernes 12 de mayo de 2017 10:17 h; Materia(s): (Constitucional); Tesis: P. II/2017 (10a.)

relativo que se aplique a la fórmula en cada caso, presentado en la ocasión que nos ocupa como el interés de un particular o de un sector determinado de la población de la información clasificada. En tal sentido, sin importar el peso relativo que se aplique en la fórmula, considerando los derechos que están en juego, el peso abstracto de los derechos a la vida y salud indudablemente tendría como resultado la prevalencia de estos sobre el derecho de acceso a la información. En consecuencia, la limitación es una medida necesaria, idónea y proporcional.

En conclusión, el hecho de reservar esta información resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, ya que proporcionarla incrementa el riesgo de pérdida de vidas humanas, riesgos de perjuicio claramente mayores a los que representaría el beneficio particular de divulgar la información objeto de la presente prueba de daño.

En razón de lo anterior, y vistas las consideraciones expuestas en el presente documento, se solicita la reserva de dicha información, por el plazo máximo de 5 años a partir de la fecha de reserva, pues las la información materia de la presente se utilizan constantemente, en virtud de la duración de las relaciones pactadas con las contrapartes autorizadas para la comercialización de piezas y productos numismáticos en metales preciosos, mismas que no siempre cuentan con una fecha de conclusión exacta, por lo que es muy probable que al término de dicho plazo, subsistan los motivos que dieron lugar a la presente reserva.

Por lo antes expuesto, con fundamento en lo dispuesto por los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, de la Constitución Política de los Estados Unidos Mexicanos; 1, 100, 103, 104, 105, 108, último párrafo, 113, fracciones V y VII, y 114, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 97, 102, 103, 105, último párrafo, 110 fracciones V y VII, y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública; 4, párrafo primero, 8, párrafos primero, segundo y tercero, 10, párrafo primero, 16 y 16 Bis 2, fracción IV, del Reglamento Interior del Banco de México; Primero, párrafo primero, y Segundo, fracción III, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Cuarto, Octavo, párrafos primero, segundo y tercero, Vigésimo tercero, Vigésimo sexto, párrafo primero, Trigésimo tercero, y Trigésimo cuarto, párrafos primero y segundo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, la información materia de la presente es clasificada como reservada, toda vez que su divulgación pone en riesgo la vida, seguridad y salud de personas físicas y que obstruye la prevención de delitos.



ANEXO "D"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000057718

VISTOS, para resolver sobre la clasificación de información relativa a la solicitud de acceso al rubro indicada; y

RESULTANDO

PRIMERO. Que el dieciséis de octubre de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000057718,** la cual se transcribe a continuación:

> *"Necesito de todos los servidores públicos los registros de las llamas recibidas y realizadas del mes de septiembre a la fecha, y en caso de grabarlas las de las última semana a la fecha de la presentación de esta solicitud, desde luego de linea oficial asignada."*

SEGUNDO. Que el mismo dieciséis de octubre, la solicitud de información mencionada en el resultando anterior, fue turnada para su atención a la Dirección de Sistemas, unidad administrativa adscrita al a Dirección General de Tecnologías de la Información; y a la Dirección General de Operaciones y Sistemas de Pagos. Y el diecisiete de octubre de dos mil dieciocho, fue turnada a la Dirección General de Emisión, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que los titulares de la Dirección de Operaciones Internacionales y de la Dirección de Operaciones Nacionales, ambas unidades administrativas adscritas a la Dirección General de Operaciones y Sistemas de Pagos, mediante oficio de treinta y uno de octubre de dos mil dieciocho, sometieron a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

CUARTO. Que este órgano colegiado, mediante resolución emitida en su sesión celebrada el nueve de noviembre de dos mil dieciocho, confirmó la ampliación del plazo ordinario de respuesta por diez días, para la atención de la solicitud al rubro citada. Dicha resolución, fue notificada al solicitante dentro del plazo ordinario.

QUINTO. Que el titular de la Dirección General de Tecnologías de la Información, mediante oficio con referencia DGTI-267/2018, hizo del conocimiento de este Comité de Transparencia su determinación de clasificar como confidencial la información que se indica en el mismo oficio, en términos de la motivación y fundamentación señaladas en el referido oficio, y solicitó a este órgano colegiado confirmar dicha clasificación, en sus términos.

SEXTO. Que el titular de la Dirección de Sistemas de Pagos, unidad administrativa adscrita a la Dirección General de Operaciones y Sistemas de Pagos, mediante oficio con referencia D01/C388/2018, hizo del conocimiento de este Comité de Transparencia su determinación de clasificar como reservada la información referida en el mismo oficio, en términos de la motivación

y fundamentación señaladas en la prueba de daño adjunta al referido oficio, y solicitó a este órgano colegiado confirmar dicha clasificación en sus términos.

SÉPTIMO. Que los titulares de la Dirección de Operaciones Internacionales, y de la Gerencia de Operaciones Nacionales, en suplencia por ausencia del Director de Operaciones Nacionales, unidades administrativas adscritas a la Dirección General de Operaciones y Sistemas de Pagos, mediante oficio de dieciséis de noviembre de dos mil dieciocho, hicieron del conocimiento de este Comité de Transparencia su determinación de clasificar como confidencial y como reservada la información referida en el mismo oficio, en términos de la motivación y fundamentación señaladas en el cuerpo del oficio en comento, y en la prueba de daño adjunta al mismo, y solicitaron a este órgano colegiado confirmar dicha clasificación en sus términos.

OCTAVO. Que el titular de la Gerencia de Gestión de la Dirección General de Emisión, en suplencia por ausencia de la Directora de Administración de Emisión, unidad administrativa adscrita a la Dirección General de Emisión, mediante oficio de dieciséis de noviembre de dos mil dieciocho, hizo del conocimiento de este Comité de Transparencia su determinación de clasificar como confidencial y como reservada la información referida en el mismo oficio, en términos de la motivación y fundamentación señaladas en el cuerpo del oficio en comento, y en la prueba de daño adjunta al mismo, y solicitó a este órgano colegiado confirmar dicha clasificación en sus términos.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas del Banco de México, de conformidad con lo previsto en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México.

SEGUNDO. Enseguida se analiza la clasificación referida en los oficios señalados en los resultandos Quinto, Sexto, Séptimo y Octavo de la presente determinación, conforme a lo siguiente:

1. Información confidencial. Este órgano colegiado advierte que es procedente la clasificación de la información referida como confidencial conforme a la fundamentación y motivación expresadas en los oficios correspondientes.

De igual manera, este Comité advierte que no se actualiza alguno de los supuestos de excepción previstos en Ley para que este Instituto Central se encuentre en posibilidad de permitir el acceso a la información señalada, en términos de los artículos 120 de la Ley General de Transparencia y Acceso a la Información Pública, y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública.

En consecuencia, **este Comité de Transparencia confirma la clasificación de la información referida como confidencial, conforme a la fundamentación y motivación expresadas en los oficios precisados en los resultandos Quinto, Séptimo y Octavo de la presente determinación.**

2. Información reservada. Este órgano colegiado advierte que es procedente la clasificación de la información referida como reservada, conforme a la fundamentación y motivación expresadas en los oficios señalados en los resultandos Quinto, Sexto, Séptimo y Octavo del presente determinación, así como en las correspondientes pruebas de daño, adjuntas a los mismos, las cuales, por economía procesal se tienen aquí por reproducidas como si a la letra se insertasen en obvio de repeticiones innecesarias.

En consecuencia, **este Comité de Transparencia confirma la clasificación de la información referida como reservada, conforme a la fundamentación y motivación expresadas en los oficios referidos y en las correspondientes pruebas de daño, adjuntas a dichos oficios.**

Por lo expuesto con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos, primero, segundo, tercero, y quinto, 65, fracción II, 102, párrafo primero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México; y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

PRIMERO. Se **confirma la clasificación de la información referida como confidencial,** conforme a la fundamentación y motivación expresadas en los oficios precisados en los resultandos Quinto, Séptimo y Octavo de la presente determinación, en términos del considerando Segundo de la presente.

SEGUNDO. Se **confirma la clasificación de la información referida como reservada,** conforme a la fundamentación y motivación expresadas en las correspondientes pruebas de daño, adjuntas a los oficios señalados en los resultandos Quinto, Sexto, Séptimo y Octavo de la presente resolución, en términos del considerando Segundo de la presente.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintitrés de noviembre de dos mil dieciocho.----------

COMITÉ DE TRANSPARENCIA

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

CARLOS EDUARDO CICERO LEBRIJA
Integrante Suplente

ANEXO "E"

BANCO DE MÉXICO

Ciudad de México, a 16 de noviembre de 2018
D01/C387/2018

COMITÉ DE TRANSPARENCIA
DEL BANCO DE MÉXICO
Presente

Nos referimos a la solicitud de acceso a la información, identificada con el número de folio **6110000057918,** que nos turnó la Unidad de Transparencia el dieciséis de octubre del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

> *"Buenos días. Se solicita*
>
> *1. Los estados de conexión y desconexión de la plataforma BANORTE-IXE en el periodo del día 18 al 28 de septiembre del año 2016.*
> *2. Los ciberataques o intentos de hackeo registrados por el SPEI de la plataforma BANORTE-IXE en septiembre del 2016.*
>
> *Gracias."*

Sobre el particular, me permito informarles que esta unidad administrativa, de conformidad con los artículos 100 y 106, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública; así como 97 y 98, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, ha determinado clasificar como reservado **el pronunciamiento respecto de confirmar o refutar los ataques a un participante específico del Sistema de Pagos Electrónicos Interbancarios (SPEI®),** de conformidad con la fundamentación y motivación señaladas en la prueba de daño que se adjunta al presente.

Por lo expuesto, en términos de los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 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.

BANCO DE MÉXICO

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informo que el personal que por la naturaleza de sus atribuciones tiene acceso al referido documento clasificado es: Director, Gerentes, Subgerentes y demás personal adscrito a la Dirección de Sistemas de Pagos

Atentamente,

MANUEL MIGUEL ÁNGEL DÍAZ DÍAZ
Director de Sistemas de Pagos

BANCO DE MÉXICO
RECIBIDO
Comité de Transparencia
Por: BIBZJ Hora: 12:40
Recibo este oficio en dos páginas y una prueba de daño.

BANCO DE MÉXICO

PRUEBA DE DAÑO

Pronunciamiento respecto de la confirmación o refutación de los ataques a un Participante específico del Sistema de Pagos Electrónicos Interbancarios (SPEI®)

En términos de lo dispuesto por los artículos 6o., apartado A, párrafo sexto, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 113, fracción IV, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 110, fracción IV, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Vigésimo segundo, fracciones I, II y IV, 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" (Lineamientos), vigentes, se considera como información reservada, aquella cuya divulgación pueda:

- Menoscabar la efectividad de las medidas implementadas en relación con las políticas en materia del sistema financiero del país, y ponga en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país.
- Comprometer las acciones encaminadas a propiciar el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

- Generar el incumplimiento de las obligaciones de un participante en un sistema de pagos que dé lugar a que otros participantes incumplan, a su vez, con sus respectivas obligaciones y pueda afectar al sistema financiero.

En ese sentido, pronunciarse respecto de **confirmar o refutar los ataques a un participante específico del Sistema de Pagos Electrónicos Interbancarios (SPEI®)** afectaría el interés público ya que menoscabaría la efectividad de las medidas implementadas en relación con las políticas en materia del sistema financiero del país, y pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; comprometería las acciones encaminadas a proporcionar el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos; o bien, podría generar el incumplimiento de las obligaciones de un participante en el sistema de pagos que dé lugar a que otros participantes incumplan, a su vez, con sus respectivas obligaciones afectando al sistema financiero o generando irregularidades en los sistemas de pagos; toda vez que dicho riesgo es:

a) Real, pues confirmar o refutar los ataques a un participante específico del SPEI® facilita a una persona o grupo de personas con intenciones delincuenciales identificar, de manera directa o indirecta –deduciendo mediante múltiples solicitudes de información– las instituciones que han visto comprometida la seguridad informática de sus sistemas de información e infraestructuras informáticas y dado que las acciones para controlar o erradicar la materialización de este riesgo requieren de un curso de acción, es decir, que en algunos casos no se producen de manera

inmediata, posibilita y potencializa dentro de esta ventana de tiempo, el diseño de ataques focalizados así como la realización de acciones hostiles dirigidas a la institución financiera vulnerada, lo cual, debido a su interconexión con las Infraestructuras de Mercado Financiero (IMF) que administra y opera este Banco Central, podría menoscabar la efectividad de las mismas a tal grado, que afectaría seriamente la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, arriesgando el funcionamiento de esos sistemas y, en consecuencia, de la economía nacional en su conjunto.

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

Asimismo, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se fundamentan en **descubrir y aprovechar vulnerabilidades de dichos sistemas, empresas o instituciones,** basando cada descubrimiento en el análisis y estudio de la información existente relacionada, por ejemplo de las vulnerabilidades a las que ha sido objeto el sistema, la empresa o institución, las acciones realizadas para contener los efectos de la materialización del riesgo, 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 o instituciones correspondientes e infraestructura informática.

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

Inclusive, **confirmar o refutar los ataques a un participante particular del SPEI®,** facilita que mediante la explotación de las vulnerabilidades actuales, terceros logren acceder a información financiera o personal, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a dichas tecnologías.

Está documentado en la literatura especializada en la materia que los principales elementos de información que requiere conocer un cibercriminal son: **las vulnerabilidades a las que ha sido objeto el sistema o institución,** la arquitectura de los sistemas, sus especificaciones técnicas, horarios de operación, funcionalidad general, protocolos de comunicación, aspectos de seguridad

informática instrumentados, entre otros, para descubrir y aprovechar los puntos débiles que pudieran existir en estos elementos y atacar a los sistemas.[1]

Por lo anterior, **reservar el pronunciamiento respecto de confirmar o refutar los ataques a un participante específico del SPEI,** o de cualquier otra IMF que el Banco Central de la Nación emplea para dar soporte a los procesos de atención e implementación de las políticas en materia monetaria, cambiaria o del sistema financiero o el buen funcionamiento del sistema de pagos, permite reducir sustancialmente los ataques informáticos que pudieran resultar efectivos, considerando aquellos que pueden surgir por el simple hecho de emplear un medio universal de comunicación como lo es Internet y los propios exploradores Web.

b) Demostrable, ya que es un hecho notorio que los participantes del SPEI están siendo víctimas de ciberataques sin precedente, de forma constante y organizada. Dichos ataques tienen por objeto el robo de recursos económicos a través del empleo de vulnerabilidades en las instituciones, aplicativos e infraestructura tecnológica del sistema financiero mexicano.

Esta serie de ataques se encuentra en una fase avanzada por lo cual es totalmente demostrable que confirmar o refutar los ataques a un participante específico del SPEI® permitiría a los delincuentes o grupos delictivos llevar a cabo ciberataques focalizados que pudieran dañar de forma más severa las IMF, entre ellas, el SPEI® del cual depende el sistema financiero mexicano.

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

En relación con lo anterior, es importante señalar que México ocupa el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica[3] y que tan sólo en México, el costo causado por el *cibercrimen* ascendió a $5,500 millones de dólares y afectó alrededor de 22.4 millones de personas; mientras que a nivel mundial, el costo ascendió a $125,900 millones de dólares y afectó

---

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

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

[3] Arreola Javier. "Ciberseguridad (casi) a prueba del enemigo 'invisible'". Forbes México. https://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/ consultado el 13 de noviembre de 2018.

a 689.4 millones de personas.[4] Por lo anterior, este Instituto Central[5] y autoridades como la Secretaría de Hacienda y Crédito Público[6] se han pronunciado sobre la importancia de fortalecer la ciberseguridad para la estabilidad del sistema financiero.

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

i) El ataque de tipo *"Watering hole"* en Polonia, que permitió utilizar un servidor de la Autoridad de Supervisión Financiera para distribuir un código malicioso a más de 20 bancos polacos[7], el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada;[8]

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;[9]

---

[4] Informe Norton sobre Ciberseguridad 2016 – Comparaciones Globales http://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf consultado el 13 de noviembre de 2018

[5] En septiembre de 2016, el Banco de México publicó el documento "Política y funciones del Banco de México respecto a las infraestructuras de los mercados financieros" en el cual dedica una sección especial al tema de seguridad informática. Este documento se encuentra disponible en la siguiente dirección electrónica: http://www.banxico.org.mx/sistemas-de-pago/informacion-general/politica-del-banco-de-mexico-respecto-de-las-infra/%7B2EAC65D2-21F4-AB2D-D250-06926EE796F8%7D.pdf.

[6] Secretaría de Hacienda y Crédito Público "Fortalecer la ciberseguridad, relevante para el desarrollo de México." 29 de octubre de 2017. https://www.gob.mx/shcp/prensa/informe-semanal-del-vocero-132251?idiom=esconsultado el 13 de junio de 2018.

[7] 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 13 de noviembre de 2018.

[8] 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 13 de noviembre de 2018.

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

iii) El ataque mediante el código malicioso *"Petya"*, enfocado en borrar archivos y discos duros completos, que paralizó las actividades de aerolíneas, bancos y bufetes de abogados en Europa;[10]

iv) El ataque que se perpetuó a BANCOMEXT el 9 de enero de 2018 a través de una afectación en su plataforma de pagos internacionales provocada por un tercero. Dicho ataque es similar a intromisiones ocurridas en otras instituciones en México y América Latina;[11]

v) 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;[12]

vi) Los ciberataques reportados por la empresa de ciberseguridad S21sec realizados por el grupo cibercriminal llamado 'Cobalt', el cual consistió en un ataque realizado a los cajeros automáticos basado en red, es decir que no se requiere acceso físico al cajero para perpetrarlos, sino que la infección se lleva a cabo la propia red interna del canco;[13]

vii) El ciberataque basado en la modalidad de denegación de servicio distribuido (DDoS) en Holanda, en el cual diez millones de holandeses se quedaron sin firma digital por el bloqueo del portal como consecuencia de una avalancha de solicitudes;[14]

viii) Los ciberataques de los que fue víctima *Delta Air Lines,* entre el 26 de septiembre al 12 de octubre de 2017, los cuales fueron informados a través de un comunicado que la compañía *[24].ai,* proveedora de servicios informáticos de ésta y otras compañías,

---

[10] Marín, Eduardo. "Descubren Que Petya, El Ataque Que Paralizó Empresas De Toda Europa, No Secuestraba Archivos Sino Que Los Borraba." Gizmodo En Español, Es.gizmodo.com, 28 de junio de 2017, http://es.gizmodo.com/descubren-que-petya-el-ataque-que-paralizo-empresas-de-1796492938 consultado el 13 de noviembre de 2018.

[11] 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 13 de noviembre de 2018.

[12] Nussman, Chris. "DHS Bulletin on Denial of Service (TDoS) Attacks on PSAPs." NENA The 911 Association, 17 de marzo de 2013, www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm, consultado el 13 de noviembre de 2018.

[13] S21Sec. "COBALT: EL CIBERCRIMEN ORGANIZADO GOLPEA LOS CAJEROS AUTOMÁTICOS EUROPEOS." S21Sec, 23 de noviembre de 2016, www.s21sec.com/es/blog/2016/11/cobalt-cibercrimen-organizado-que-ataca-a-los-cajerosautomaticos-europeos consultado el 13 de junio de 2018.

[14] Recalde, Luis. EL CIBERESPACIO: EL NUEVO TEATRO DE GUERRA GLOBAL. Revista De Ciencias De Seguridad y Defensa, http://geo1.espe.edu.ec/wp-content/uploads/2016/07/art15.pdf consultado el 13 de noviembre de 2018.

suceso que causó que los datos bancarios de algunos de los usuarios de la aerolínea se hayan visto comprometidos durante ese periodo.[15]

ix) Los ataques cibernéticos que han sufrido otros Bancos Centrales a través de la infraestructura de sistemas de pagos conocida como SWIFT, la cual ha sido utilizada para realizar robos de capital, uno de estos casos es el del Banco Central de Bangladesh, que sufrió un robo de 81 millones de dólares.[16] 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.[17] 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.[18]

i) 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.[19] 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.[20]

Inclusive uno de los *modus operandi* de los ciberataques es precisamente a través de la obtención de información pública, información fácilmente accesible o información inaccesible, lo cual puede

---

[15] Delta Airlines. "INFORMATION ON [24)7.AI CYBER INCIDENT." Information on [24)7.Ai Cyber Incident, 7 de abril de 2018, www.delta.com/content/www/en_US/response.html consultado el 13 de noviembre de 2018.

[16] Michael Riley, Alan Katz. "Swift Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh". Bloomberg. 26 de Mayo de 2016. https://www.bloomberg.com/news/articles/2016-05-26/swift-hack-probe-expands-to-up-to-dozen-banks-beyond-bangladesh consultado el 13 de noviembre de 2018.

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

[18] Antony Peyton. "Symantec reveals more hack attempts on Swift network". Banking Technology. 11 de octubre de 2016. https://www.bankingtech.com/2016/10/symantec-reveals-more-hack-attempts-on-swift-network/ consultado el 13 de noviembre de 2018.

[19] Banco de México. "Información sobre los ataques a los Participantes del SPEI". http://www.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/%7B2B9BB8C6-D66B-38C4-CC90-F72A7BC335C9%7D.pdf, consultado el 13 de noviembre de 2018.

[20] Acorde con los "Puntos importantes sobre la situación actual del SPEI" publicados en la página de internet del Banco de México http://www.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/%7B022CD9D7-11A9-68E6-D1A5-965F57A23F60%7D.pdf, consultados el 13 de noviembre de 2018.

ocurrir mediante solicitudes de acceso a la información, o bien, a través de las organizaciones que operan o tienen acceso a los sistemas, en complicidad o no, con el único objeto de conocer las vulnerabilidades en las instituciones, empresas, sistemas e infraestructura de tecnologías de la información.[21]

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.[22]

Por lo anterior, **los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar cualquier información que potencialice la materialización de un riesgo de ciberseguridad,**[23] en el entendido de que dicha información, al estar en malas manos, 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.

c) Identificable, ya que a la fecha de realización de la presente prueba de daño, es un hecho notorio que las instituciones financieras están siendo objeto de ciberataques a gran escala, como quedó demostrado en la sección anterior. Si bien estos ataques no han logrado irrumpir o vulnerar las IMF que administra y opera el Banco de México, puede concluirse que existe la probabilidad de que el objeto de dichos ataques considere a estas infraestructuras, cuya seguridad depende de la reserva del pronunciamiento materia en comento.

En ese sentido, **un ataque informático derivado del pronunciamiento de este Instituto Central sobre confirmar o refutar los ataques a un participante particular del SPEI®, podrían resultar en la**

---

[21] El Economista, *El sistema financiera 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 13 de noviembre de 2018.

[22] Granger, S. (2001). Social engineering fundamentals, part 1: hacker tactics. Security Focus, 18 de diciembre de 2001. https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics consultado el 13 de noviembre de 2018.

[23] Ver por ejemplo las 10 medidas básicas de ciberseguridad de la Security Information Center, en particular la relacionada con "Implementar un programa de capacitación en seguridad cibernética para empleados" en donde recomiendan sensibilizar sobre los temas de ingeniería social que buscan obtener información mediante diversos canales de comunicación solicitando información sensible. https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_0.pdf consultado el 13 de noviembre de 2018.

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

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

Por lo anterior, un ataque informático perpetrado derivado del pronunciamiento en cuestión representa un perjuicio significativo para el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias, pues de acuerdo con la información del Banco de México, de agosto de 2017 a agosto de 2018, se realizaron aproximadamente 603 millones de pagos electrónicos interbancarios por un monto de 293 billones de pesos; lo anterior equivale a más de 63 mil operaciones por un monto de 31 mil millones de pesos por hora, únicamente para lo que respecta al SPEI®.[24]

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

Adicionalmente, **el riesgo de perjuicio que supondría dar a conocer el pronunciamiento de este Instituto Central sobre confirmar o refutar los ataques a un participante específico del SPEI®,**

---

24 Banco de México. Sistemas de pago de alto valor, Sistemas de liquidación en tiempo real (CF252) – Sistema de Pagos Electrónico Interbancarios. http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es

supera el interés público general de que se difunda, pues el interés público se centra en que se conserve la efectividad en las medidas implementadas en los sistemas financiero y económico, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto, la estabilidad en los mercados financieros y en los sistemas de pagos. Por lo que, dicho pronunciamiento, no satisface el interés público, por el contrario, revela información que pone en riesgo el buen funcionamiento de los sistemas de pagos y de la economía nacional en su conjunto. Asimismo, al realizar una interpretación sobre la alternativa que más satisface dicho interés, se puede concluir que debe prevalecer el derecho más favorable a las personas, esto es, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste.

En consecuencia, **dicho pronunciamiento, no aporta un beneficio mayor a la transparencia y rendición de cuentas que sea comparable con el perjuicio que implicaría el hecho de los efectos derivados de dicho pronunciamiento,** esto es, que permita planear y perpetrar ataques cibernéticos dirigidos específicamente a alguno de los participantes del SPEI® o alguna de las IMF administradas y operadas por el Banco de México, los cuales tengan como resultado el acceso indebido, la substracción de información -como datos personales referente a sus usuarios y las operaciones que realizan-, la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios proporcionados por los participantes o las IMF. 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, reservar el pronunciamiento materia del presente documento **evitará poner en riesgo el buen funcionamiento de los sistemas de pagos, del sistema financiero y de la economía nacional en su conjunto, lo cual sería claramente mayor al beneficio del interés que pudiera existir en proporcionar dicho pronunciamiento.**

Asimismo, **reservar el pronunciamiento en cuestión representa el medio menos restrictivo disponible para evitar el perjuicio,** en aras salvaguardar el buen funcionamiento de los sistemas de pagos, así como la estabilidad del sistema financiero, **puesto que el propio legislador determinó que el medio menos restrictivo es la clasificación de la información cuando actualice las causales 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., 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, 104, 105, 108, 109, 113, fracción IV, y 114 de la LGTAIP; 1, 97, 100, 102, 103, 105, 106, 110, fracción IV, y 111 de la LFTAIP, 2o. y 3o., de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero y tercero, 10, párrafo primero, 20, fracciones I, II, VI y VII, y 28 fracciones III y V del Reglamento Interior del Banco de México; Primero, párrafo primero, Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como, Primero, Cuarto, Sexto, párrafo segundo, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo,

fracciones I, II y IV, y Vigésimo sexto, párrafo segundo, de los Lineamientos, vigentes, se **clasifica la información materia de la presente, por el plazo de 5 años a partir de la fecha de clasificación,** toda vez que, como se ha manifestado esta acción atiende a la protección de las medidas de seguridad, con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de tecnologías de la información y comunicaciones, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques, no solo de las vulnerabilidades identificadas sino de aquellas que no se encuentran reconocidas provocando afectaciones a las IMF que opera y administra este Instituto Central, entre ellas los sistemas de pagos, menoscabaría la efectividad de las medidas implementadas en relación con las políticas en materia del sistema financiero del país, y ponga en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, así como comprometería las acciones encaminadas a propiciar el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos, y obstruya la persecución de delitos.

ANEXO "F"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000057918

VISTOS, para resolver sobre la clasificación de información relativa a la solicitud de acceso al rubro indicada; y

RESULTANDO

PRIMERO. Que el dieciséis de octubre de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000057918,** la cual se transcribe a continuación:

> *"Buenos días. Se solicita*
> *1. Los estados de conexión y desconexión de la plataforma BANORTE-IXE en el periodo del día 18 al 28 de septiembre del año 2016.*
> *2. Los ciberataques o intentos de hackeo registrados por el SPEI de la plataforma BANORTE-IXE en septiembre del 2016.*
> *Gracias."*

SEGUNDO. Que el mismo dieciséis de octubre, la solicitud de información mencionada en el resultando anterior, fue turnada para su atención a la Dirección de Sistemas de Pagos del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que el titular de la Dirección de Sistemas de Pagos del Banco de México, mediante oficio del ocho de noviembre del año en curso, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

CUARTO. Que este órgano colegiado, mediante resolución emitida en su sesión celebrada el nueve de noviembre del presente año, confirmó la ampliación del plazo ordinario de respuesta por diez días, para la atención de la solicitud al rubro citada. Dicha resolución, fue notificada al solicitante dentro del plazo ordinario.

QUINTO. Que el titular de la Dirección de Sistemas de Pagos del Banco de México, mediante oficio con referencia D01/C387/2018, hizo del conocimiento de este Comité de Transparencia su determinación de clasificar como reservada la información referida en dicho oficio, en términos de la motivación y fundamentación señaladas en la prueba de daño correspondiente, por lo que solicitó a este órgano colegiado confirmar dicha clasificación.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas del Banco de México, de conformidad con lo previsto en los artículos 44, fracción II, de la Ley General

de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México.

SEGUNDO. Enseguida se analiza la clasificación realizada por la unidad administrativa señalada en el resultando Quinto de la presente determinación, conforme a lo siguiente:

Este órgano colegiado estima que es procedente la clasificación de la información identificada como reservada, toda vez que se ubica en los supuestos de reserva, en términos de la fundamentación y motivación expresadas en la correspondiente prueba de daño, adjunta al oficio precisado en el resultando Quinto de la presente determinación, misma que se tiene por reproducida a la letra, en obvio de repeticiones innecesarias.

En consecuencia, **este Comité de Transparencia confirma la clasificación de la información referida como reservada, conforme a la fundamentación y motivación expresadas en la correspondiente prueba de daño, adjunta en el oficio precisado en el resultando Quinto de la presente determinación.**

Por lo expuesto con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos, primero, segundo, tercero, y quinto, 65, fracciones II y IX, 102, párrafo primero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracciones III y XX, del Reglamento Interior del Banco de México; y 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,** conforme a la fundamentación y motivación expresadas en la correspondiente prueba de daño.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintitrés de noviembre de dos mil dieciocho.----------

COMITÉ DE TRANSPARENCIA

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

CARLOS EDUARDO CICERO LEBRIJA
Integrante Suplente

ANEXO "G"

BANCO DE MÉXICO

Ciudad de México, a 15 de noviembre de 2018.

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
Presente.

Nos referimos a la solicitud de acceso a la información, identificada con el número de folio 6110000060218, que nos turnó la Unidad de Transparencia el veinticuatro de octubre del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

> *"Solicito una versión pública de los resultados y evidencias resultantes de los procesos de supervisión para el cumplimiento de los requerimientos de ciberseguridad durante 2017 que Banco de México realizó a los participantes que usan el Sistema de Pagos Electrónicos Interbancarios (SPEI) como parte de la regulación emitida y las obligaciones en materia de ciberseguridad que tiene establecidas el Banco de México para los participantes del SPEI."*

Sobre el particular, nos permitimos hacer de su conocimiento que con motivo de la atención de una solicitud de acceso diversa, los titulares de la Dirección de Regulación y Supervisión, y de la Gerencia de Política y Vigilancia de los Sistemas de Pagos, unidad administrativa adscrita a la Dirección de Sistemas de Pagos, mediante oficio de quince de junio de dos mil dieciocho, clasificaron como reservada la información relativa a ***"los resultados y evidencias resultantes de los procesos de supervisión para el cumplimiento de los requerimientos de ciberseguridad durante 2017 que Banco de México realizó a los participantes que usan el Sistema de Pagos Electrónicos Interbancarios (SPEI) como parte de la regulación emitida y las obligaciones en materia de ciberseguridad que tiene establecidas el Banco de México para los participantes del SPEI"***.

Dicha clasificación fue confirmada por el Comité de Transparencia mediante resolución emitida en su sesión Ordinaria 23/2018, de 21 de junio de 2018.

Al respecto, con motivo de una nueva reflexión realizada para la atención de la solicitud materia del presente, y tomando en consideración los recientes criterios emitidos por el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI) en la sustanciación de diversos recursos de revisión en materia de acceso a la información pública[1], estas unidades administrativas han determinado **modificar la clasificación** de la información realizada

[1] a) Resolución del Pleno del INAI en la sustanciación del recurso de revisión identificado con el número de expediente RRA 2537/18, interpuesto en contra de la respuesta emitida por la Secretaría de Relaciones Exteriores, relativa a la solicitud de acceso a la información con folio 0000500059218;

b) Resolución del Pleno del INAI en la sustanciación del recurso de revisión identificado con el número de expediente RRA 2747/18, interpuesto en contra de la respuesta emitida por el Servicio de Protección Federal, relativa a la solicitud de acceso a la información con folio 3600100001718; y

c) Resolución del Pleno del INAI en la sustanciación del recurso de revisión identificado con el número de expediente RRA 2794/18, interpuesto en contra de la respuesta emitida por el INAI, relativa a la solicitud de acceso a la información con folio 067800063318.

mediante el oficio de quince de junio de dos mil dieciocho, antes referido, en los términos que se indican más adelante en el presente oficio. Lo anterior, a fin de garantizar la seguridad jurídica y certidumbre del solicitante, al establecer con mayor precisión los supuestos normativos de clasificación que resultan aplicables al caso en concreto.

Al respecto, debe considerarse que de conformidad con los artículos 105, párrafo primero, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 103, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Cuarto, párrafo segundo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" (Lineamientos), vigentes, la aplicación de las excepciones al derecho de acceso a la información previstas en la Ley por los sujetos obligados, debe ser restrictiva y limitada, a fin de garantizar certidumbre al solicitante.

En ese sentido, a fin de ajustar la clasificación a los más recientes criterios emitidos por el INAI, no vulnerar la seguridad jurídica del solicitante y delimitar las causales de reserva estrictamente aplicables, en relación con diversa información relativa a ***"los resultados y evidencias resultantes de los procesos de supervisión para el cumplimiento de los requerimientos de ciberseguridad durante 2017 que Banco de México realizó a los participantes que usan el Sistema de Pagos Electrónicos Interbancarios (SPEI) como parte de la regulación emitida y las obligaciones en materia de ciberseguridad que tiene establecidas el Banco de México para los participantes del SPEI"***, estas unidades administrativas han determinado lo siguiente:

1. Respecto de "***<u>los resultados</u> (...) de los procesos de supervisión para el cumplimiento de los requerimientos de ciberseguridad durante 2017 que Banco de México realizó a los participantes que usan el Sistema de Pagos Electrónicos Interbancarios (SPEI) como parte de la regulación emitida y las obligaciones en materia de ciberseguridad que tiene establecidas el Banco de México para los participantes del SPEI"***, ambas unidades administrativas, mantienen la clasificación de información exclusivamente con base en la causal establecida en los artículos 113, fracción VI, de la LGTAIP; 110, fracción VI, de la LFTAIP; así como en el Vigésimo cuarto de los Lineamientos, vigentes.

2. Respecto de las ***"(...) <u>evidencias resultantes</u> de los procesos de supervisión para el cumplimiento de los requerimientos de ciberseguridad durante 2017 que Banco de México realizó a los participantes que usan el Sistema de Pagos Electrónicos Interbancarios (SPEI) como parte de la regulación emitida y las obligaciones en materia de ciberseguridad que tiene establecidas el Banco de México para los participantes del SPEI",*** ambas unidades administrativas, modifican la anterior clasificación de dicha información para ahora realizarla con base en las causales establecidas en los artículos 113, fracciones VI y VII, de la LGTAIP; 110, fracciones VI y VII, de la LFTAIP; así como en el Vigésimo cuarto y el Vigésimo sexto, párrafo primero, de los Lineamientos, vigentes.

3. La relación de las expresiones documentales que posee este sujeto obligado y que se considera atienden lo solicitado y que, por lo tanto, son los documentos que comprende la clasificación que se solicita son: **las actas parciales, actas de cierre y dictámenes generados con motivo del ejercicio de las facultades de supervisión**

del Banco de México a participantes del SPEI, durante el 2017 los cuales contienen las observaciones y, en su caso, resultados preliminares correspondientes emitidos o generados con motivo de la supervisión realizada a los intermediarios financieros participantes del SPEI. Lo anterior, toda vez que su difusión obstruiría las actividades de supervisión, verificación e inspección relativas al cumplimiento de las leyes, y disposiciones normativas.

Por lo expuesto, y con fundamento en lo dispuesto por los artículos 6, apartado A, párrafo sexto, y 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 100, 103, 104, 105, 108, último párrafo, 109, 113, fracciones VI y VII, y 114, de la LGTAIP; 1, 97, 100, 102, 103, 105, párrafo último, 106, 110, fracciones VI y VII, y 111 de la LFTAIP; 2 y 3 de la Ley del Banco de México; 4, párrafo primero, 8, párrafos primero, segundo y tercero, 10, párrafo primero, 20, fracciones I, XII y XVI, y 25 Bis 1, fracciones I, V y VI, del Reglamento Interior del Banco de México; Primero, párrafo primero, y Segundo, fracciones I y VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como el Primero, , Cuarto, Sexto, Séptimo, fracción I, Octavo párrafos primero, segundo y tercero, Décimo, Vigésimo cuarto, Vigésimo sexto, Trigésimo tercero, y Trigésimo cuarto, párrafos primero y segundo, de los Lineamientos, vigentes, nos permitimos informarles que estas unidades administrativas modifican la clasificación como reservada de la información realizada mediante el oficio de quince de junio de dos mil dieciocho, misma que fue confirmada por ese órgano colegiado en resolución emitida en su sesión ordinaria 23/2018, de veintiuno de junio del presente año, en términos de lo expresado en el presente oficio, y en la prueba de daño extraída del referido oficio de quince de junio del año en curso, en la que se realizaron los ajustes correspondientes y que adjuntamos al presente como un documento diverso.

En ese sentido, dicha información deberá permanecer clasificada en su totalidad como reservada por un plazo de cinco años, contados a partir de la fecha en que se confirmó dicha clasificación, por las causas señaladas a ese órgano colegiado en su momento, toda vez que no es procedente generar versiones públicas.

Lo anterior es acorde con lo sustentado por el INAI, al resolver el recurso de revisión RRA 0119/18, particularmente en las páginas 57, 58, 64 y 65 de la determinación correspondiente, en la cual determinó que si los datos que pueden dejarse visibles al elaborar una versión pública son de mínima relevancia, tales como la fecha de elaboración, al contener la totalidad del documento información reservada, no se colmaría su pretensión con la elaboración de versiones públicas. Dicho caso es relevante, puesto que el particular pretende acceder a los resultados y evidencias resultantes de los procesos de supervisión para el cumplimiento de los requerimientos de ciberseguridad durante 2017 que Banco de México realizó a los participantes que usan el Sistema de Pagos Electrónicos Interbancarios (SPEI) como parte de la regulación emitida y las obligaciones en materia de ciberseguridad que tiene establecidas el Banco de México para los participantes del SPEI, sin embargo, al testar esta información en versiones públicas, únicamente quedarían visibles datos irrelevantes como las fechas en que se emitieron y el número de páginas, por lo que no colmarían su pretensión dichas versiones.

BANCO DE MÉXICO

Por lo anterior, y en términos de los artículos 44 fracción II de la LGTAIP; 65, fracción II de la LFTAIP; así como 31, fracción III del Reglamento Interior del Banco de México, solicitamos a este H. Comité de Transparencia confirmar la clasificación realizada por estas unidades administrativas.

Atentamente,

Viviana Garza Salazar
Directora de Regulación y Supervisión

Manuel Miguel Ángel Díaz Díaz
Director de Sistemas de Pagos

BANCO DE MÉXICO
RECIBIDO
16 AGO 2018
Comité de Transparencia
Por: B12327 Hora: 12:46
Recibo este oficio en cuatro páginas y una prueba de daño.

BANCO DE MÉXICO

PRUEBA DE DAÑO

En términos de lo dispuesto por los artículos 6, párrafo cuarto, apartado A, fracciones I y VIII, párrafo sexto, y 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 113, fracciones VI y VII, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 110, fracción VI y VII, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Vigésimo cuarto y 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" (Lineamientos), vigentes, es de clasificarse como información reservada aquella que de divulgarse podría:

- Obstruir las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes.

- Obstruir la prevención de los delitos.

Por lo que la información relativa a ***"los resultados y evidencias resultantes de los procesos de supervisión para el cumplimiento de los requerimientos de ciberseguridad durante 2017 que Banco de México realizó a los participantes que usan el Sistema de Pagos Electrónicos Interbancarios (SPEI) como parte de la regulación emitida y las obligaciones en materia de ciberseguridad que tiene establecidas el Banco de México para los participantes del SPEI"***, es clasificada como reservada ya que su divulgación represente un riesgo de perjuicio significativo al interés público, toda vez que puede obstruir las actividades de supervisión, verificación e inspección relativas al cumplimiento de las leyes y disposiciones normativas, llevadas a cabo por este Instituto Central, en el ejercicio de sus facultades, y obstruiría la prevención de delitos informáticos[1] en contra del Banco de México cuya planeación y ejecución se facilitarían con la divulgación de la información referida, por lo que su divulgación representa un riesgo:

1. Real, ya que la información relacionada con el tema que nos ocupa se encuentra en un procedimiento de supervisión en curso, y en otros casos se está analizando la información obtenida de los intermediarios, de darse a conocer lo solicitado, se afectaría la oportunidad con la que el Banco de México, como autoridad supervisora, puede realizar determinadas acciones materiales de supervisión, pues los sujetos supervisados u otras entidades en situaciones similares, a los que podría hacerse extensiva la supervisión, podrían alterar o modificar los hechos, actos u omisiones a valorarse, así como el escenario, objeto o circunstancias materia de supervisión, y por ende podrían influir en el resultado de tales actividades, las cuales concluyen hasta que es emitida la sanción correspondiente, y esta es publicada y ejecutada.

En relación con lo anterior, debe destacarse que de conformidad con lo dispuesto en el artículo 28, párrafo séptimo, de la Constitución Federal, el Banco de México cuenta con las atribuciones de autoridad necesarias para proveer a la observancia de la regulación que emita. Para tal finalidad, de

[1] Cfr. Cassou Ruiz, Jorge Esteban, "Delitos informáticos en México", *Revista del Instituto de la Judicatura Federal,* México, núm. 28, julio-diciembre de 2008, pp. 220-225. https://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf Consultada el 12 de noviembre de 2018.

conformidad con los artículos 24, 35 Bis, 36 y 36 Bis, de la Ley del Banco de México, dicho Instituto Central podrá realizar la supervisión de los intermediarios y entidades financieras sujetos a la regulación que expida, mediante actos de inspección, vigilancia, y la sanción de los incumplimientos que se determinen.

Las diversas etapas del proceso de supervisión del cumplimiento de las disposiciones aplicables al sistema financiero, se encuentran establecidas en las Reglas de Supervisión, Programas de Autocorrección y del Procedimiento Sancionador (Reglas de Supervisión), y gráficamente se expresan en el manual del macroproceso Política de estabilidad financiera y seguimiento y evaluación del sistema financiero, proceso 2: Supervisión del cumplimiento de las disposiciones aplicables al sistema financiero.

La información que las instituciones financieras han proporcionado a este Instituto Central o que este ha recabado, como parte del procedimiento de supervisión del cumplimiento de las disposiciones que regulan su participación en el Sistema de Pagos Electrónicos Interbancarios (SPEI®), **así como las observaciones y resultados preliminares contenidos en las actas y/o dictámenes respectivos, están en proceso de revisión y análisis en distintas etapas del flujo operativo.**

El vínculo directo entre la información referida y los procedimientos de supervisión referidos, es evidente, pues su existencia está prevista en la normatividad aplicable, particularmente en las Reglas de Supervisión, y es el insumo fundamental de las siguientes etapas del proceso de supervisión, que concluirá con la emisión, en su caso, de las sanciones respectivas, su publicación y ejecución.

Toda vez que se encuentran revisiones en curso, y en otros casos se está analizando la información obtenida de los intermediarios, de darse a conocer la información materia de la presente, se afectaría la oportunidad con la que el Banco de México, como autoridad supervisora, puede realizar determinadas acciones materiales de supervisión, pues los sujetos supervisados u otras entidades en situaciones similares, a los que podría hacerse extensiva la supervisión, podrían alterar o modificar los hechos, actos u omisiones a valorarse, así como el escenario, objeto o circunstancias materia de supervisión, y por ende podrían influir en el resultado de tales actividades.

En consecuencia, se actualiza la causal de reserva prevista en los artículos 113, fracción VI, de la LGTAIP; 110, fracción VI, de la LFTAIP; así como en el Vigésimo cuarto de los Lineamientos, vigentes, ya que , como se ha expuesto, la información materia de la presente prueba de daño forma parte de un procedimiento de verificación del cumplimiento de diversas leyes y disposiciones normativas; asimismo, se encuentra directamente vinculada con las actividades realizadas por este Instituto Central como autoridad en el proceso de verificación referido, y su divulgación puede obstaculizar las actividades de inspección, supervisión o vigilancia que realiza este Banco Central en el procedimiento de verificación en comento.

Asimismo, difundir las observaciones o resultados (que además son todavía preliminares) obtenidos de las diferentes visitas de inspección sobre las vulnerabilidades de los intermediarios, tendría una

repercusión directa en sus procesos de ciberseguridad, por lo que su divulgación puede proporcionar a individuos o a grupos con intenciones hostiles, elementos de información que facilitarían aprovechar los puntos débiles 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 dichas infraestructuras. Por lo anterior, el SPEI® podría verse afectado al estar conectado con toda la banca mexicana, generando un riesgo sistémico importante.

En consecuencia, la divulgación de la información clasificada, representa un obstáculo para la prevención de conductas constitutivas de delitos, por lo que se actualiza la causal de reserva prevista en los artículos 113, fracción VII, de la LGTAIP; 110, fracción VII, de la LFTAIP; así como el Vigésimo sexto, párrafo primero, de los Lineamientos, vigentes.

2. Demostrable, toda vez que al difundir información de entidades financieras, resaltando aquella relacionada con los sistemas de pagos, que pueda generar confusión, percepciones erróneas o equívocas, incrementa el riesgo operacional y reputacional no solo de tales entidades, sino también de los sistemas de pagos y el sistema financiero en general, lo que puede conllevar la materialización de otro tipo de riesgos como los financieros y el legal repercutiendo en la determinación correspondiente.

Cabe destacar que el SPEI®, es el sistema de pagos sistémicamente más importante en México, es decir, puede transmitir impactos financieros de un participante a otro y en el peor de los casos podrían extenderse más allá del sistema y sus participantes, amenazando la estabilidad de los mercados de dinero y de otros mercados financieros nacionales e internacionales.

Adicionalmente, las instituciones financieras en México están siendo víctimas de ciberataques sin precedente, de forma constante y organizada, desde 2017. Dichos ataques tienen por objeto el robo de recursos económicos a través del empleo de vulnerabilidades en los aplicativos e infraestructura tecnológica del sistema financiero mexicano. A la fecha de elaboración de la presente prueba de daño, se estima un daño a este sistema de aproximadamente 300 millones de pesos. [2] 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,**[3] por lo cual es totalmente demostrable que el entregar información precisamente sobre las vulnerabilidades detectadas durante el procedimiento de supervisión de los sistemas de pagos permitiría a los delincuentes o grupos delictivos el llevar a cabo más ciberataques que pudieran dañar de forma más severa las infraestructuras de los mercados financieros, entre ellas, los sistemas de pagos de los cuales depende el sistema financiero mexicano.

---

[2] Información sobre los ataques a los participantes del SPEI en http://www.banxico.org.mx/spei/d/%7BFFC53F5A-CA04-3098-EBF6-B0F17E533183%7D.pdf. Consultada el 12 de noviembre de 2018.

[3] El Financiero, *El sistema financiero mexicano fue víctima de una campaña de ciberataques*, en https://www.eleconomista.com.mx/sectorfinanciero/El-sistema-financiero-mexicano-fue-victima-de-una-campana-de-ciberataques-20180515-0097.html. Consultada el 12 de noviembre de 2018.

3. **Identificable,** tomando en cuenta que la divulgación de la información que nos ocupa podría interrumpir o menoscabar la realización del procedimiento de verificación o sus resultados, la determinación de las medidas que, en su caso, se pudieran solicitar para ajustarse a lo dispuesto en la regulación o su implementación, así como los actos jurídicos que derivarían de los mismos. Lo anterior, toda vez que tales afectaciones pueden ocurrir en tanto no existan resoluciones firmes y definitivas.

Además, la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio. En efecto, toda vez que la información materia de la presente forma parte de diversos procedimientos de supervisión que se encuentran en trámite, dicha determinación es proporcional, considerando que la difusión de la información referida generaría un riesgo de daño o perjuicio significativo, particularmente el impedimento u obstaculización de actividades de supervisión, inspección y vigilancia, que se llevan a cabo para la verificación del cumplimiento de leyes y disposiciones normativas. Lo cual tiene mayor relevancia, en comparación con el interés que pudiera existir en conocer dicha información. Asimismo, con la divulgación de la información se generarían percepciones erróneas o equívocas que pudieran afectar injustificadamente a las entidades financieras, a sus clientes, inversionistas, empleados, a otras entidades con las que operan, principalmente otros participantes del SPEI® y sus usuarios, así como en general el sistema financiero mexicano, incluyendo a las autoridades financieras, situación que también evidencia la proporcionalidad de la clasificación que nos ocupa.

En este orden de ideas, la clasificación como reservada respecto de la información solicitada, resulta el medio menos restrictivo disponible para evitar los perjuicios señalados.

El riesgo de perjuicio que supondría la divulgación de la información solicitada, supera el interés público general de que se difunda, ya que el interés público se centra en que se conserve la efectividad en las medidas implementadas en los sistemas de pagos, que propician el buen funcionamiento de dichos sistemas y de la economía nacional en su conjunto, conservando la estabilidad en el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos, a través del cabal cumplimiento de los procesos de verificación, supervisión e inspección que realiza el Banco de México a los participantes del SPEI®, en ejercicio de las facultades que le otorgan para esos efectos las disposiciones normativas vigentes.

En consecuencia, dar a conocer la información materia de la presente prueba de daño, no aporta un beneficio a la transparencia que sea compatible con el perjuicio de que por su difusión se facilite un ataque para robar o modificar información, alterar el funcionamiento de los sistemas de pagos, o dejar inoperantes las tecnologías de la información utilizadas por los participantes del SPEI.

Por lo anteriormente expuesto, con fundamento en lo establecido en los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 100, 103, 104, 105, 108, 109, 113, fracciones VI y VII, y 114 de la LGTAIP; 97, 100, 102, 103, 105, 106, 110, fracciones VI y VII, y 111 de la LFTAIP; 2o. y 3o. de la Ley del Banco de México; 4o., párrafo primero, 8o.., párrafos primero, segundo y tercero, 10, párrafo primero 20, fracciones I, XII y XVI, y 25 Bis 1, fracciones I, V y VI, del Reglamento Interior del Banco de México;

BANCO DE MÉXICO

Primero, párrafo primero, y Segundo, fracciones VI y X, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Cuarto, Sexto, párrafo segundo, Octavo, párrafos primero, segundo y tercero, Vigésimo cuarto y Vigésimo sexto, párrafo primero, de los Lineamientos, vigentes, la información en posesión del Banco de México, relativa a ***"los resultados y evidencias resultantes de los procesos de supervisión para el cumplimiento de los requerimientos de ciberseguridad durante 2017 que Banco de México realizó a los participantes que usan el Sistema de Pagos Electrónicos Interbancarios (SPEI) como parte de la regulación emitida y las obligaciones en materia de ciberseguridad que tiene establecidas el Banco de México para los participantes del SPEI"***, ha sido clasificada como reservada, al igual que la documentación correspondiente, por un periodo de cinco años a partir de la fecha en que se confirme la clasificación.

ANEXO "H"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000060218

VISTOS, para resolver sobre la clasificación de información relativa a la solicitud de acceso al rubro indicada; y

RESULTANDO

PRIMERO. Que el veinticuatro de octubre de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000060218**, la cual se transcribe a continuación:

> Descripción:
>
> *"Solicito una versión pública de los resultados y evidencias resultantes de los procesos de supervisión para el cumplimiento de los requerimientos de ciberseguridad durante 2017 que Banco de México realizó a los participantes que usan el Sistema de Pagos Electrónicos Interbancarios (SPEI) como parte de la regulación emitida y las obligaciones en materia de ciberseguridad que tiene establecidas el Banco de México para los participantes del SPEI."*
>
> Datos adicionales:
>
> *"El 16 de mayo el Gobernador del Banco de México Alejandro Díaz de León dio una conferencia respecto al ciberataque contra diversos bancos en una semana pasada. Aquí la transcripción de una parte del discurso del gobernador Díaz de León en la que habla de los procesos de supervisión a los que me refiero en la solicitud de información anterior. Los participantes de SPEI tienen obligaciones de ciberseguridad establecidas en la regulación que emitió Banxico desde julio de 2017, las principales medidas en materia de seguridad debían estar aplicadas a finales de 2017, cabe destacar que parte de la regulación emitida se refiere precisamente a los aplicativos que fueron vulnerados en algunos participantes. Banxico inició los procesos de supervisión para el cumplimiento de los requerimientos de ciberseguridad durante 2017 detectando un nivel de cumplimiento heterogéneo. A la fecha se tienen iniciados procesos de supervisión sobre el cumplimiento de requerimientos de ciberseguridad por parte de los participantes en diferentes sistemas de Banxico."*

SEGUNDO. Que el mismo veinticuatro de octubre, la solicitud de información mencionada, fue turnada para su atención a la Dirección de Sistemas de Pagos, así como a la Dirección General de Asuntos del Sistema Financiero, del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que la titular de la Dirección de Regulación y Supervisión, unidad administrativa adscrita a la Dirección General de Asuntos del Sistema Financiero, mediante oficio con referencia

KOI/23/2018, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

CUARTO. Que este órgano colegiado, mediante resolución emitida en su sesión celebrada el dieciséis de noviembre del presente año, confirmó la ampliación del plazo ordinario de respuesta por diez días, para la atención de la solicitud al rubro citada. Dicha resolución, fue notificada al solicitante dentro del plazo ordinario.

QUINTO. Que los titulares de la Dirección de Sistemas de Pagos y de la Dirección de Regulación y Supervisión del Banco de México, mediante oficio con fecha quince de noviembre del presente año, hicieron del conocimiento de este Comité de Transparencia su determinación de clasificar la información contenida en el documento que precisa en el mismo oficio, en términos de la motivación y fundamentación señaladas en la prueba de daño correspondiente, por lo que solicitó a este órgano colegiado confirmar dicha clasificación.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas del Banco de México, de conformidad con lo previsto en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México.

SEGUNDO. Enseguida se analiza la clasificación realizada por la unidad administrativa señalada en el resultando Quinto de la presente determinación, conforme a lo siguiente:

Este órgano colegiado estima que es procedente la clasificación de la información relativa a "***los resultados*** *(...) de los procesos de supervisión para el cumplimiento de los requerimientos de ciberseguridad durante 2017 que Banco de México realizó a los participantes que usan el Sistema de Pagos Electrónicos Interbancarios (SPEI) como parte de la regulación emitida y las obligaciones en materia de ciberseguridad que tiene establecidas el Banco de México para los participantes del SPEI*", tal y como se detalla en el oficio al que se refiere el resultando Quinto de la presente determinación, y la prueba de daño adjunta al mismo y que se tiene por reproducida a la letra, en obvio de repeticiones innecesarias, toda vez que dicha información se ubica **exclusivamente** en el supuesto de reserva señalado en los artículos 113, fracción VI, de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VI, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como el Vigésimo cuarto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes.

Asimismo, este Comité de Transparencia estima que es procedente la clasificación de la información relativa a " *(...)* ***evidencias resultantes*** *de los procesos de supervisión para el cumplimiento de los requerimientos de ciberseguridad durante 2017 que Banco de México realizó a los participantes que usan el Sistema de Pagos Electrónicos Interbancarios (SPEI) como parte de la regulación emitida y las obligaciones en materia de ciberseguridad que tiene establecidas el Banco de México para los participantes del SPEI*", tal y como se detalla en el oficio al que se refiere el resultando Quinto de la

presente determinación, y la prueba de daño adjunta al mismo y que se tiene por reproducida a la letra, en obvio de repeticiones innecesarias, toda vez que dicha información se ubica en los supuestos de reserva señalados en los artículos 113, fracciones VI y VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracciones VI y VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como el Vigésimo cuarto 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.

En consecuencia, **este Comité de Transparencia confirma la clasificación de la información referida como reservada, conforme a la fundamentación y motivación expresadas en el oficio precisado en el resultando Quinto de la presente determinación y en la prueba de daño adjunta al mismo.**

Por lo expuesto con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos, primero, segundo, tercero, y quinto, 65, fracciones II y IX, 102, párrafo primero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracciones III y XX, del Reglamento Interior del Banco de México; y 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,** conforme a la fundamentación y motivación expresadas en el oficio al que se refiere el resultando Quinto de la presente determinación, y la prueba de daño que acompaña al mismo, en términos del considerando Segundo de la presente.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintitrés de noviembre de dos mil dieciocho.----------

COMITÉ DE TRANSPARENCIA

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

CARLOS EDUARDO CICERO LEBRIJA
Integrante Suplente

ANEXO "I"

BANCO DE MÉXICO
RECIBIDO
14 NOV 2018
Comité de Transparencia
Por: JL5390 Hora: 12:00

BANCO DE MÉXICO

Se recibe oficio constante en dos páginas y una carátula.

Ciudad de México, a 14 de noviembre de 2018

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

Nos referimos a la solicitud de acceso a la información, identificada con el número de folio **6110000062118** que recibió la Unidad de Transparencia el treinta de octubre del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a:

> *"Buenas tardes, por este medio solicito el Documento de Seguridad estipulada por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados implementado en esa entidad pública referente al tratamiento de datos personales"*

Al respecto, nos permitimos informarles que estas unidades administrativas, de conformidad con los artículos 100, 106, fracción I, y 111, de la Ley General de Transparencia y Acceso a la Información Pública, 97, 98, fracción I, y 108, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, han determinado clasificar diversa información contenida en el documento que se indica más adelante, de conformidad con la fundamentación y motivación señaladas en la carátula y en la prueba de daño correspondientes.

Para facilitar su identificación, en el siguiente cuadro encontrarán el detalle del título del documento clasificado, el cual coincide con el que aparece en la carátula que debidamente firmada se acompaña al presente.

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXO
Documento de seguridad, Protección de Datos Personales, Junio 2018	**1**	**2**

Por lo expuesto, en términos de los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, inciso a), de los Lineamientos, atentamente solicitamos a ese Comité de Transparencia confirmar la clasificación de la información realizada por estas unidades administrativas, y aprobar la versión publica señalada en el cuadro precedente.

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones

públicas", informamos que el personal que por la naturaleza de sus atribuciones tiene acceso al referido documento clasificado es el adscrito a: Dirección de Sistemas (Director y Especialista en Tecnologías de la Información), Gerencia de Proyectos Informáticos Administrativos (Gerente), Subgerencia de Desarrollo de Sistemas Contable-Financieros (Subgerente), Subgerencia de Desarrollo de Sistemas de Capital Humano (Subgerente), Gerencia de Informática (Gerente y Especialistas en Tecnologías de la Información), Subgerencia de Desarrollo de Sistemas para Análisis de Información (Subgerente), Subgerencia de Desarrollo de Sistemas de Gestión Operativa (Subgerente), Gerencia de Seguridad de Tecnologías de la Información (Todo el personal), Dirección de Ciberseguridad (Director), Dirección de Coordinación de la Información (Todo el personal), la Unidad de Auditoría, el Gerente de Auditorías Operacionales y de Cumplimiento; el Gerente de Auditorías de Tecnología de Información y Especiales; la Subgerencia de Auditorías de Tecnología de Información; y los enlaces de transparencia, y todo el personal adscrito a la Unidad de Transparencia.

Atentamente,

ELIZABETH CASILLAS TREJO
Subgerente de Gestión de Obligaciones de Transparencia y Solicitudes de Información

SERGIO ZAMBRANO HERRERA
Subgerente de Análisis Jurídico y Promoción de Transparencia

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 100, 106, fracción I, 109 y 111 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97, 98, fracción I, 106, 108 y 118 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción I, Quincuagésimo sexto, Sexagésimo segundo, inciso a) y Sexagésimo tercero de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Lineamientos).

VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Subgerencia de Gestión de Obligaciones de Transparencia y Solicitudes de Información Subgerencia de Análisis Jurídico y Promoción de Transparencia
II. La identificación de los documentos del que se elaboran las versiones públicas.	Documento de seguridad, Protección de Datos Personales, Junio 2018
III. Firma del titular del área y de quien clasifica.	**ELIZABETH CASILLAS TREJO** Subgerencia de Gestión de Obligaciones de Transparencia y Solicitudes de Información **SERGIO ZAMBRANO HERRERA** Subgerente de Análisis Jurídico y Promoción de Transparencia
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia "Ordinaria", número 5a/2018, celebrada el 23 de octubre de 2018 Secretario del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, Secretario del Comité de Transparencia del Banco de México.

BANCO DE MÉXICO

A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación y, en los supuestos de información clasificada como reservada, el periodo de reserva:

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
1	Páginas identificadas con los numerales 4, 29, 30, 31 y 32	Información sobre los sistemas en los que se almacenan o tratan datos personales en el Banco de México y las acciones que se adoptarán como parte del plan de trabajo para la protección de dichos datos, descritos en el Documento de Seguridad	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

PRUEBA DE DAÑO

Información sobre los sistemas en los que se almacenan o tratan datos personales en el Banco de México y las acciones que se adoptarán como parte del plan de trabajo para la protección de dichos datos, descritos en el Documento de Seguridad

En términos de lo dispuesto en el artículo 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública y 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, es de clasificarse como información reservada aquella cuya publicación obstruya la prevención de los delitos, por lo que la **información sobre los sistemas en los que se almacenan o tratan datos personales en el Banco de México y las acciones que se adoptarán como parte del plan de trabajo para la protección de dichos datos, descritos en el Documento de Seguridad, es clasificada como reservada en virtud de lo siguiente:**

La divulgación de la citada información representa un riesgo de perjuicio significativo al interés público, en lo que respecta a la obstrucción en la prevención de los delitos, toda vez que dicho riesgo es:

1) Real, ya que revelar o divulgar información sobre los sistemas en los que se almacenan o tratan datos personales en el Banco de México y las acciones que se adoptarán como parte del plan de trabajo para la protección de dichos datos, descritos en el Documento de Seguridad, haría vulnerable la prevención de delitos como fraudes o robos de identidad, que podrían perpetrarse por personas o grupos delincuenciales.

2) Demostrable, ya que en los últimos años, el creciente avance de la tecnología ha propiciado cambios fundamentales en los procesos y modelos de negocio al interior de las organizaciones financieras. Estos avances, sin duda, han contribuido a introducir eficiencias operativas y ahorros de costos. Banco de México no es la excepción, al igual que otros bancos centrales, está cada vez mejor interconectado, y utiliza sistemas de tecnologías de información más complejos. Sin embargo, el uso de dichas tecnologías también conlleva mayores riesgos. Las vulneraciones de seguridad generan altos costos institucionales además de afectaciones en la esfera de otros derechos y libertades fundamentales de las personas.

En un entorno digital cada vez más interconectado, las brechas de seguridad en las Tecnologías de la Información y la Comunicación (TIC) pueden producir consecuencias no deseadas en la operación y, por ende, en la reputación del Banco de México y el sistema financiero del país. Las amenazas que pueden ocasionar la interrupción de la operación de las instituciones son cada día más evidentes y sofisticadas, independientemente de las acciones preventivas en materia de seguridad de la información y de las TIC, tanto la evidencia histórica como las recientes intrusiones cibernéticas a nivel internacional sugieren que prácticamente todas las industrias, y particularmente los servicios financieros, son susceptibles a posibles

eventos de pérdida o sustracción de información.

Con la finalidad de minimizar y evitar los riesgos de pérdida de datos personales, el Banco de México ha instrumentado de forma proactiva un programa de fortalecimiento de la seguridad de la información, el cual comprende un plan de trabajo con acciones concretas, que deben mantenerse reservadas, con la finalidad de que no pueda afectarse su efectividad y con ello, garantizar la continuidad de la operación de la institución.

Por otra parte, 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 (1) descubrir y aprovechar vulnerabilidades, basando cada descubrimiento en el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente de las aplicaciones, la arquitectura o servicios de tecnologías de información y de comunicaciones que se quieren vulnerar, y (2) tomar ventaja de cualquier información conocida para emplear técnicas de ingeniería social que les faciliten el acceso indebido a los sistemas, con el propósito de substraer información, alterarla, o causar un daño disruptivo.

Adicionalmente, debe destacarse que de vulnerarse alguno de los sistemas en los que se almacenan datos personales, se afectaría la reputación del Banco Central del Estado mexicano.

3) Identificable, ya que difundir información de datos personales contenidos en los archivos electrónicos, sistemas o aplicaciones del Banco de México descritos en el Documento de Seguridad del Instituto Central no aporta un beneficio a la transparencia que sea comparable con el perjuicio de que por su difusión se facilite un ataque para robar o modificar información, alterar el funcionamiento o dejar inoperantes a las tecnologías de la información y de comunicaciones que sustentan los procesos de archivo del Banco de México.

Cabe destacar que al hacer públicos los sistemas en los que se almacena o tratan datos personales, o bien información sobre las acciones que se implementarán para fortalecer la seguridad de dichos datos, ocasionaría un serio perjuicio a las actividades de prevención de los delitos que llevan a cabo las autoridades competentes, toda vez que facilitarían la vulneración de la integridad y confidencialidad de la información que éstos contienen.

El riesgo de perjuicio que supondría la divulgación, supera el interés público general de que se difunda, ya que no existe un beneficio social con la divulgación de los sistemas de almacenamiento y tratamiento de datos personales identificados en el Documento de Seguridad, o bien sobre las acciones que se tomarán como parte del plan de trabajo establecido. Por el contrario, difundir la citada

información podría poner en riesgo de vulneración los referidos sistemas y datos personales contenidos en los mismos.

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que debe prevalecer el interés público sobre el interés particular, en virtud de que al disminuir el riesgo de cualquier vulneración a los datos personales en posesión de este Banco Central, se contribuye a la prevención de los delitos.

El hecho de reservar esta información resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, ya que proporcionarla incrementaría el riesgo de obtener y utilizar de manera ilegal y sin autorización de su titular, datos personales para llevar a cabo conductas ilícitas como fraudes.

En razón de lo anterior, y vistas las consideraciones expuestas en el presente documento, la Unidad de Transparencia del Banco de México solicita la reserva de dicha información por un plazo de cinco años a partir de la fecha de la misma, ya que es indispensable proteger y evitar la divulgación de la información contenida en los archivos electrónicos, sistemas o aplicaciones del Banco de México descritos en el Documento de Seguridad del Instituto Central, con la intención de evitar conductas ilícitas.

Por lo expuesto, con fundamento en lo dispuesto por los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 100, 103, 104, 105, 106, fracción III, 108, último párrafo, 109, 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 98, fracción III, 100, 102, 106, 110, fracción VII, y 111, Ley Federal de Transparencia y Acceso a la Información Pública; 2o., y 4o. de la Ley del Banco de México; 4, párrafo primero, 8, párrafos primero y tercero, 10, párrafo primero, 31 Bis, fracciones, XXIV, XXVI y XXIX, del Reglamento Interior del Banco de México; Primero, párrafo primero, y Segundo, fracción XIII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Cuarto, Séptimo, fracción III, Octavo, párrafos primero, segundo y tercero, y 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”, la información contenida en los archivos electrónicos, sistemas o aplicaciones del Banco de México descritos en el Documento de Seguridad del Instituto Central, es reservada, toda vez que su divulgación dificultaría las labores, programas, políticas y lineamientos que la autoridad competente pueda tener en materia de prevención de los delitos.

ANEXO "J"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000062118

VISTOS, para resolver sobre la clasificación de información relativa a la solicitud de acceso al rubro indicada; y

RESULTANDO

PRIMERO. Que el treinta de octubre de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000062118,** la cual se transcribe a continuación:

> *"Buenas tardes, por este medio solicito el Documento de Seguridad estipulada por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados implementado en esa entidad pública referente al tratamiento de datos personales"*

SEGUNDO. Que el mismo treinta de octubre, la solicitud de información mencionada en el resultando anterior, fue turnada para su atención a la Unidad de Transparencia del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que los titulares de la Subgerencia de Gestión de Obligaciones de Transparencia y Solicitudes de Información y de la Subgerencia de Análisis Jurídico y Promoción de Transparencia, unidades adscritas a la Unidad de Transparencia del Banco de México, mediante oficio de catorce de noviembre del dos mil dieciocho, hicieron del conocimiento de este Comité de Transparencia su determinación de clasificar diversa información contenida en el documento que se indica en el mismo oficio, de conformidad con la fundamentación y motivación señaladas en la carátula y prueba de daño correspondientes, por lo que solicitó a este órgano colegiado confirmar dicha clasificación y aprobar la respectiva versión pública.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas del Banco de México, de conformidad con lo previsto en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México.

SEGUNDO. Enseguida se analiza la clasificación realizada por las unidades administrativas señaladas en el resultando Tercero de la presente determinación, conforme a lo siguiente:

Este órgano colegiado estima que es procedente la clasificación de la información identificada como reservada, toda vez que se ubica en los supuestos de reserva, en términos de la fundamentación y motivación expresadas en la correspondiente prueba de daño, adjunta al oficio precisado en el resultando Tercero de la presente determinación, misma que se tiene por reproducida a la letra, en obvio de repeticiones innecesarias.

En consecuencia, **este Comité de Transparencia confirma la clasificación de la información referida como reservada, conforme a la fundamentación y motivación expresadas en la correspondiente prueba de daño, adjunta en el oficio precisado en el resultando Tercero de la presente determinación.**

Por lo expuesto con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos, primero, segundo, tercero, y quinto, 65, fracciones II y IX, 102, párrafo primero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracciones III y XX, del Reglamento Interior del Banco de México; y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

PRIMERO. Se **confirma la clasificación de la información referida como reservada,** conforme a la fundamentación y motivación expresadas en la prueba de daño adjunta al oficio precisado en el resultando Tercero de la presente determinación.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintitrés de noviembre de dos mil dieciocho.----------

COMITÉ DE TRANSPARENCIA

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

CARLOS EDUARDO CICERO LEBRIJA
Integrante Suplente