FOLIO 1

BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ORDINARIA 23/2018
DEL 21 DE JUNIO DE 2018

En la Ciudad de México, a las doce horas con treinta minutos del veintiuno de junio de dos mil dieciocho, en el edificio ubicado en avenida Cinco de Mayo, número seis, colonia Centro, delegación Cuauhtémoc, se reunieron Claudia Álvarez Toca, Directora de la Unidad de Transparencia, Erik Mauricio Sánchez Medina, Gerente Jurídico Consultivo, suplente del Director Jurídico, y José Ramón Rodríguez Mancilla, Gerente de Organización de la Información, suplente del Director de Coordinación de la Información, todos integrantes del Comité de Transparencia de este Instituto Central, así como Rodolfo Salvador Luna de la Torre, 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, párrafos primero y segundo, 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. ----------

Claudia Álvarez Toca, Presidenta de dicho órgano colegiado, en términos del artículo 4o. del Reglamento Interior del Banco de México, y Quinta, párrafo primero, inciso a), 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 existía 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, párrafo primero, inciso d), y Sexta, párrafo primero, inciso b), 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 presentes 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 51, párrafo segundo, y 83 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 43, párrafo segundo, 44, fracción IX, de la Ley General de Transparencia y Acceso a la Información Pública; 4o. y 31, fracciones III y XX, del Reglamento Interior del Banco de México, y Quinta, párrafo primero, inciso e), de las Reglas de Operación del Comité de Transparencia del Banco

de México, por unanimidad, aprobó 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 AMPLIACIÓN DEL PLAZO DE RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO CTC-BM-23585. ----------

El Secretario dio lectura al oficio de catorce de junio del año en curso, suscrito por el titular de la Dirección de Operaciones Nacionales del Banco de México, que se agrega a la presente acta como **ANEXO "C"**, por medio del cual dicha unidad administrativa solicitó a este Comité de Transparencia confirmar la ampliación del plazo ordinario de respuesta para la solicitud de acceso a la información citada, por los motivos expuestos en el oficio referido.----------

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, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 132, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 9, 64, 65 fracción II, y 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Vigésimo octavo de los "*Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública*", vigentes, confirma la ampliación del plazo de respuesta, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "D"**. ----------

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE MEDICIÓN ECONÓMICA, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO CTC-BM-23821. ----------

El Secretario dio lectura al oficio de doce de junio del dos mil dieciocho, suscrito por el titular de la Dirección de Medición Económica del Banco de México, mismo que se agrega a la presente acta como **ANEXO "E"**, por virtud del cual dicha unidad administrativa ha determinado clasificar la información que se señala en dicho oficio, conforme a la fundamentación y motivación expresadas en el referido oficio, y solicitó a este órgano colegiado confirmar tal clasificación.----------

Después de un amplio intercambio de opiniones, se determinó 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; 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, resolvió confirmar la clasificación de la información realizada por la unidad administrativa citada, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "F"**. ----------

TERCERO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA GERENCIA DE GESTIÓN FIDUCIARIA, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000030018. ----------

El Secretario dio lectura al oficio con referencia O10.GGF.010/2018, suscrito por el titular de la Gerencia de Gestión Fiduciaria del Banco de México, mismo que se agrega a la presente acta como **ANEXO "G"**, por virtud del cual dicha unidad administrativa ha determinado clasificar la información

que se señala en dicho oficio, conforme a la fundamentación y motivación expresadas en el referido oficio, y solicitó a este órgano colegiado confirmar tal clasificación. ----------

Después de un amplio intercambio de opiniones, se determinó 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; 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, resolvió confirmar la clasificación de la información realizada por la unidad administrativa citada, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "H"**.----------

CUARTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA DIRECCIÓN DE REGULACIÓN Y SUPERVISIÓN Y DE LA GERENCIA DE POLÍTICA Y VIGILANCIA DE LOS SISTEMAS DE PAGOS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000026518. ----------

El Secretario dio lectura al oficio de quince de junio de dos mil dieciocho, suscrito por los titulares de la Dirección de Regulación y Supervisión, unidad administrativa adscrita a la Dirección General de Asuntos del Sistema Financiero, y de la Gerencia de Política y Vigilancia de los Sistemas de Pagos, unidad administrativa adscrita a la Dirección de Sistemas de Pagos del Banco de México, mismo que se agrega a la presente acta como **ANEXO "I"**, por virtud del cual dichas unidades administrativas han determinado clasificar la información que se señala en dicho oficio, conforme a la fundamentación y motivación señaladas en la prueba de daño contenida en cuerpo del oficio en comento, y solicitaron a este órgano colegiado confirmar tal clasificación. ----------

Después de un amplio intercambio de opiniones, se determinó 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; 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, resolvió confirmar la clasificación de la información realizada por las unidades administrativas citadas, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "J"**. ----------

QUINTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA DIRECCIÓN DE REGULACIÓN Y SUPERVISIÓN Y DE LA GERENCIA DE POLÍTICA Y VIGILANCIA DE LOS SISTEMAS DE PAGOS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000026618. ----------

El Secretario dio lectura al oficio de quince de junio de dos mil dieciocho, suscrito por los titulares de la Dirección de Regulación y Supervisión, unidad administrativa adscrita a la Dirección General de Asuntos del Sistema Financiero, y de la Gerencia de Política y Vigilancia de los Sistemas de Pagos, unidad administrativa adscrita a la Dirección de Sistemas de Pagos del Banco de México, mismo que se agrega a la presente acta como **ANEXO "K"**, por virtud del cual dichas unidades administrativas han determinado clasificar la información que se señala en dicho oficio, conforme a la fundamentación y motivación señaladas en la prueba de daño contenida en cuerpo del oficio en comento, y solicitaron a este órgano colegiado confirmar tal clasificación. ----------

BANCO DE MÉXICO

Después de un amplio intercambio de opiniones, se determinó 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; 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, resolvió confirmar la clasificación de la información realizada por las unidades administrativas citadas, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "L"**. ----------
SEXTO. SOLICITUD DE CONFIRMACIÓN DE LA 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 6110000029418. ----------
El Secretario dio lectura al con referencia D01/C366/2018, suscrito por el titular de la Dirección de Sistemas de Pagos del Banco de México, mismo que se agrega a la presente acta como **ANEXO "M"**, por virtud del cual dicha unidad administrativa ha determinado clasificar la información que se señala en dicho oficio, conforme a la fundamentación y motivación señaladas en la prueba de daño contenida en cuerpo del oficio en comento, y solicitó a este órgano colegiado confirmar tal clasificación. ----------
Después de un amplio intercambio de opiniones, se determinó 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; 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, resolvió confirmar la clasificación de la información realizada por la unidad administrativa citada, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "N"**. ----------
SÉPTIMO. SOLICITUD DE CONFIRMACIÓN DE LA 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 6110000029618. ----------
El Secretario dio lectura al oficio con referencia D01/C363/2018, mismo que se agrega a la presente acta como **ANEXO "Ñ"**, a través del cual, el titular de la Dirección de Sistemas de Pagos del Banco de México, hizo del conocimiento de este Comité de Transparencia que subsisten las causas que dieron origen a la clasificación de los documentos señalados en dicho oficio, en términos de la motivación y fundamentación señaladas en la respectiva prueba de daño que en su momento pusieron a disposición de este órgano colegiado. Y, a través de dicho oficio, señalaron que dichos documentos son materia de la solicitud referida, y solicitaron a este Comité de Transparencia confirmar la clasificación de la información. Asimismo, mediante ese mismo oficio, hizo del conocimiento de este órgano colegiado que ha determinado clasificar el documento señalado en el segundo cuadro de dicho escrito, conforme a la fundamentación y motivación señaladas en la prueba de daño que acompañaron al oficio en comento, y solicitó a este Comité de Transparencia confirmar tal clasificación. ----------
Después de un amplio intercambio de opiniones, se determinó lo siguiente: ----------

BANCO DE MÉXICO

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; 64 y 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción II, del Reglamento Interior del Banco de México y Quinta de las Reglas de Operación del Comité de Transparencia, resolvió confirmar la clasificación de la información para dar respuesta a la solicitud de acceso a la información referida en este apartado, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "O"**.----------

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

CLAUDIA ÁLVAREZ TOCA
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

RODOLFO SALVADOR LUNA DE LA TORRE
Secretario

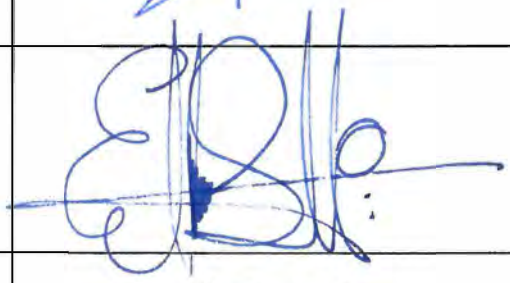
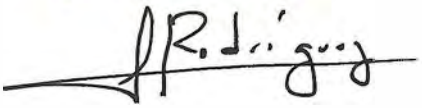
BANCO DE MÉXICO

LISTA DE ASISTENCIA

SESIÓN ORDINARIA 23/2018

21 DE JUNIO DE 2018

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA Directora de la Unidad de Transparencia Integrante	
ERIK MAURICIO SÁNCHEZ MEDINA Gerente Jurídico Consultivo Integrante Suplente	
JOSÉ RAMÓN RODRÍGUEZ MANCILLA Gerente de Organización de la Información Integrante suplente	
RODOLFO SALVADOR LUNA DE LA TORRE Secretario del Comité de Transparencia	

BANCO DE MÉXICO

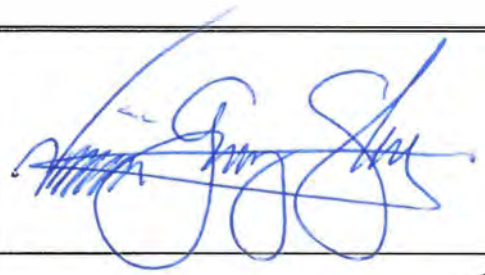
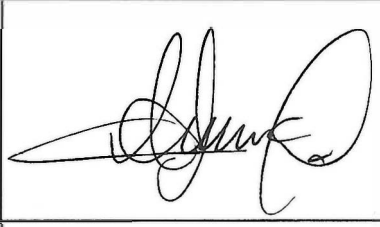
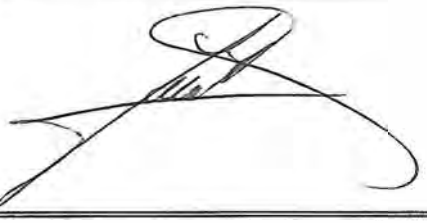
INVITADOS PERMANENTES

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

INVITADOS

ALAN CRUZ PICHARDO Subgerente de Apoyo Jurídico a la Transparencia	
CARLOS EDUARDO CICERO LEBRIJA Gerente de Gestión de Transparencia	
MARÍA DEL CARMEN REY CABARCOS Gerente de Riesgos No Financieros	

RODRIGO MÉNDEZ PRECIADO Gerente de Enlace Institucional y Relaciones Públicas	
MARGARITA LISSETE PONCE GUARNEROS Subgerente de Identificación y Evaluación de Riesgos Operativos	
OTHÓN MARTINO MORENO GONZÁLEZ Gerente de Política y Vigilancia de los Sistemas de Pagos	
LILIANA GARCÍA OCHOA Líder de Especialidad de la Gerencia de Estudios de Sistemas de Pagos	
XIMENA AIDEE DOMÍNGUEZ HERNÁNDEZ Investigador de la Gerencia de Estudios de Sistemas de Pagos	
CLAUDIA TAPIA RANGEL Especialista Investigador	
MARTÍN CAMPOS FERNÁNDEZ Analista de Información	

VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión	
MARÍA ISABEL PÉREZ ROMERO Gerente de Autorizaciones, Regulación y Sanciones	
ALDO DYLAN HEFFNER RODRÍGUEZ Director de Medición Económica	
GERARDO ANTONIO AVILEZ ALONSO Gerente de Sistemas de Información Económica	
ANDRÉS FLORES GRANADOS Subgerente Técnico de la DGIE	
LUIS RODRIGO SALDAÑA ARELLANO Gerente de Gestión Fiduciaria	
LUIS ALBERTO SALGADO RODRÍGUEZ Subgerente Legal Fiduciario	

CARLA BARRI ROSENDO Jefa de la Oficina Legal Fiduciaria	
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	
Iebeth Leyva	

ANEXO "B"

BANCO DE MÉXICO

Comité de Transparencia

ORDEN DEL DÍA
Sesión Ordinaria 23/2018
21 de junio de 2018

PRIMERO. SOLICITUD DE CONFIRMACIÓN DE AMPLIACIÓN DEL PLAZO DE RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO CTC-BM-23585.

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE MEDICIÓN ECONÓMICA, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO CTC-BM-23821.

TERCERO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA GERENCIA DE GESTIÓN FIDUCIARIA, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000030018.

CUARTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA DIRECCIÓN DE REGULACIÓN Y SUPERVISIÓN Y DE LA GERENCIA DE POLÍTICA Y VIGILANCIA DE LOS SISTEMAS DE PAGOS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000026518.

QUINTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA DIRECCIÓN DE REGULACIÓN Y SUPERVISIÓN Y DE LA GERENCIA DE POLÍTICA Y VIGILANCIA DE LOS SISTEMAS DE PAGOS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000026618.

SEXTO. SOLICITUD DE CONFIRMACIÓN DE LA 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 6110000029418.

SÉPTIMO. SOLICITUD DE CONFIRMACIÓN DE LA 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 6110000029618.

ANEXO "C"

BANCO DE MÉXICO

Ciudad de México, a 14 de junio de 2018.

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

Me refiero a la solicitud de acceso a la información identificada con el número de folio **CTC-BM-23585**, que nos hizo llegar la Unidad de Transparencia el 24 de mayo de 2018, a través del sistema electrónico de atención a solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual menciona lo siguiente:

> *"En relación a la solicitud CTC-BM-22672:En la primera petición: La oferta más alta y más baja en cada subasta de bonos de 2006 a 2017, potencialmente con identificadores para cada postor... solo obtuvimos datos de MBONOS, ¿nos podrían proporcionar esta información pero para todo tipo de Bonos y no solo MBONOS?Gracias"*

Sobre el particular, se somete a aprobación de ese órgano colegiado la ampliación del plazo de respuesta a la solicitud indicada en el párrafo anterior, ya que dada la naturaleza, vastedad y complejidad de la misma se está llevando a cabo la obtención, verificación y análisis de la información. Por lo que en aras de atender la solicitud en la forma más completa posible, esta Dirección debe estar en posibilidad de continuar realizando una búsqueda exhaustiva, razonable y detallada. Lo anterior, con la finalidad de que la información que se entregue al solicitante sea accesible, confiable, verificable, veraz y oportuna, y que, de igual forma, se atienda debidamente el requerimiento de acceso a la información del particular.

La solicitud mencionada se presenta con fundamento en los artículos 44, fracción II, y 132, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, y 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; 4, párrafo primero, 8, párrafo primero, y 19 Bis, fracciones II, III, V y X, del Reglamento Interior del Banco de México; Primero, párrafo primero, y Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como en el lineamiento Vigésimo Octavo de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", publicados en el Diario Oficial de la Federación el 12 de febrero de 2016.

A t e n t a m e n t e,

MTRO. JUAN RAFAEL GARCÍA PADILLA
Director de Operaciones Nacionales

BANCO DE MÉXICO
RECIBIDO
14 JUN 2018
Comité de Transparencia
Por: 31530 Hora: 16:45

Recibí un oficio constante en una página.

ANEXO "D"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DE PLAZO
Folio: CTC-BM-23585

VISTOS, para resolver sobre la ampliación del plazo de respuesta relativa a la solicitud de acceso a la información al rubro indicada; y

RESULTANDO

PRIMERO. Que el veinticuatro de mayo de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **CTC-BM-23585**, la cual se transcribe a continuación:

> *" En relación a la solicitud CTC-BM-22672:*
>
> *En la primera petición: La oferta más alta y más baja en cada subasta de bonos de 2006 a 2017, potencialmente con identificadores para cada postor... solo obtuvimos datos de MBONOS, ¿nos podrían proporcionar esta información pero para todo tipo de Bonos y no solo MBONOS?*
>
> *Gracias"*

SEGUNDO. Que la Unidad de Transparencia del Banco de México remitió para su atención a la entonces Dirección General de Operaciones de Banca Central del Banco de México, el mismo veinticuatro de mayo del presente año, la solicitud de acceso a la información referida en el resultando anterior, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Con fecha treinta de mayo de dos mil dieciocho, se publicaron en el Diario Oficial de la Federación, las Reformas al Reglamento Interior y al acuerdo de adscripción de las Unidades Administrativas del Banco de México, a través del cual se modificó la denominación de la "Dirección General de Operaciones de Banca Central" por el de "Dirección General de Operaciones y Sistemas de Pagos".

CUARTO. Con relación a los resultandos Segundo y Tercero, el titular de la Dirección de Operaciones Nacionales, unidad administrativa adscrita a la ahora Dirección General de Operaciones y Sistemas de Pagos del Banco de México, mediante oficio de catorce de junio dos mil dieciocho, sometió a la consideración del Comité de Transparencia la determinación de ampliación del plazo de respuesta

a la referida solicitud de acceso a la información. Al respecto, en dicho documento manifestaron de manera medular lo siguiente:

> *"…se somete a aprobación de ese órgano colegiado la ampliación del plazo de respuesta a la solicitud indicada en el párrafo anterior, ya que dada la naturaleza, vastedad y complejidad de la misma se está llevando a cabo la obtención, verificación y análisis de la información. Por lo que en aras de atender la solicitud en la forma más completa posible, esta Dirección debe estar en posibilidad de continuar realizando una búsqueda exhaustiva, razonable y detallada. Lo anterior, con la finalidad de que la información que se entregue al solicitante sea accesible, confiable, verificable, veraz y oportuna, y que, de igual forma, se atienda debidamente el requerimiento de acceso a la información del particular."*

CONSIDERANDO

PRIMERO. De conformidad con lo previsto en los artículos 44, fracción II, 131 y 132, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, y 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Vigésimo octavo de los "*Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública*", este Comité de Transparencia cuenta con facultades 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 unidades administrativas del Banco.

SEGUNDO. Mediante el oficio referido en el resultando Cuarto, la Dirección de Operaciones Nacionales, expuso las razones para ampliar el plazo de respuesta a la solicitud de acceso a la información citada al rubro, particularmente, debido a que dada la naturaleza, vastedad y complejidad de la misma se está llevando a cabo la obtención, verificación y análisis de la información requerida con diversas unidades administrativas de este Instituto Central, por lo que en aras de atender la solicitud en la forma más completa posible, dicha Dirección debe estar en posibilidad de continuar realizando una búsqueda exhaustiva, razonable y detallada. Lo anterior, con la finalidad de que la información que se entregue al solicitante sea accesible, confiable, verificable, veraz y oportuna

TERCERO. Que de conformidad con los artículos 131 de la Ley General de Transparencia y Acceso a la Información Pública y 133 de la Ley Federal de Transparencia y Acceso a la Información Pública, es necesario que las áreas competentes de los sujetos obligados realicen una búsqueda exhaustiva y razonable de la información solicitada, con la finalidad de garantizar el efectivo derecho de acceso a la información. En consecuencia, es necesario que cuente con un plazo adecuado, acorde a las circunstancias particulares, como pueden ser la complejidad técnica, material o jurídica, así como las cargas de trabajo.

Por lo anterior, atendiendo a las razones expuestas por el área mencionada, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 132, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 9, 64, 65, fracción II, y 135, párrafo segundo, de la Ley Federal

de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Vigésimo octavo de los "*Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública*", vigentes, este Comité de Transparencia:

RESUELVE

ÚNICO. Se confirma la ampliación del plazo de respuesta, por **diez días hábiles adicionales** al plazo original, respecto de la solicitud de acceso a la información citada al rubro, en términos de lo expuesto en los considerandos Segundo y 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 veintiuno de junio de dos mil dieciocho. ----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

BANCO DE MÉXICO

ANEXO "E"

Ciudad de México, 12 de junio 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 **CTC-BM-23821,** que nos fue turnada por la Unidad de Transparencia el 1 de junio del año en curso, a través del sistema electrónico de atención a solicitudes, en el marco de la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables en la materia, la cual se transcribe a continuación:

> *"HolaMuchas gracias por su respuesta a la solicitud CTC-BM-23191.*
> *Habria forma de conocer detalles adicionales sobre como se componen las series del Cuadro CE167? Especificamente a los envios de Estados Unidos a Mexico me gustaria saber lo siguiente:*
> *a)Deslgoce State (USA) a Estado (MX)*
> *b) Que fuentes utilizan para integrar los flujos de Envios de Remesas de Estados Unidos a Mexico, que remesadores, bancos, organismos les reportan y de ser posible los montos*
> *Esto ultimo para poder calcular Market Shares de los jugadores en el mercado de las remesas de Estados Unidos a Mexico.Gracias."*

BANCO DE MÉXICO
RECIBIDO
12 JUN 2018
Comité de Transparencia
Por: CO442 Hora: 4:45 p.m
Recibí oficio constante en 3 páginas

Al respecto, la información consistente en: ***"(...) b) Que fuentes utilizan para integrar los flujos de Envios de Remesas de Estados Unidos a Mexico, que remesadores, bancos, organismos les reportan y de ser posible los montos (...)",*** tiene carácter confidencial en virtud de las siguientes consideraciones:

INFORMACIÓN CONFIDENCIAL, PROTEGIDA POR SECRETO ESTADÍSTICO

En términos del artículo 62, fracción I, de la Ley del Banco de México, el Instituto Central podrá, en coordinación con las demás autoridades competentes, elaborar, compilar y publicar estadísticas económicas y financieras, así como operar sistemas de información basados en ellas y recabar los datos necesarios para esos efectos. Esto incluye la información de remesas. Al respecto, dicha información debe sujetarse a lo dispuesto por la Ley del Sistema Nacional de Información Estadística y Geográfica.

Por cuanto hace a dicha información, los artículos 37 y 38 de la Ley del Sistema Nacional de Información Estadística y Geográfica disponen que **los datos que proporcionen para fines estadísticos los Informantes del Sistema** (que de acuerdo con el artículo 2, fracción VII, de ese mismo ordenamiento son las personas físicas y morales, a quienes les sean solicitados datos estadísticos y geográficos en términos de la Ley en comento) **a las Unidades** (que en términos del artículo 2, fracción XV, inciso d, son las áreas administrativas que cuenten con atribuciones para desarrollar Actividades Estadísticas y Geográficas o que cuenten con registros administrativos que permitan obtener información de Interés Nacional de organismos constitucionales autónomos, entre los cuales queda incluido el Banco de México) serán estrictamente confidenciales y que bajo ninguna circunstancia podrán ser utilizados para otro fin que no sea el estadístico, y que aquellos que provengan de registros administrativos serán manejados observando los principios de confidencialidad y reserva, por lo que no podrán divulgarse en ningún caso en forma nominativa o individualizada, ni harán prueba ante autoridad judicial o administrativa, incluyendo la fiscal, en juicio o fuera de él.

Asimismo, el artículo 47, párrafos primero y segundo, de la Ley del Sistema Nacional de Información Estadística y Geográfica, establece que los datos que proporcionen los Informantes del Sistema, serán confidenciales en términos de la misma Ley, y que la información no queda sujeta a la otrora Ley Federal de Transparencia y Acceso a la Información Pública.

En adición a lo anterior, el artículo 42 de la multicitada Ley del Sistema Nacional de Información Estadística y Geográfica, dispone que los Informantes del Sistema podrán denunciar ante las autoridades administrativas y judiciales, todo hecho o circunstancia del que se derive que se hubieren desconocido los principios de confidencialidad y reserva a que se refiere dicha Ley. Por otro lado, el artículo 104, fracción I de esa misma Ley, establece como infracción imputable a los servidores públicos de las Unidades la revelación de datos confidenciales.

En términos de los artículos 116, párrafo cuarto, de la Ley General de Transparencia y Acceso a la Información Pública, y 113, fracción III, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Cuadragésimo primero de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", la información consistente *en: **"(...) b) Que fuentes utilizan para integrar los flujos de Envios de Remesas de Estados Unidos a Mexico, que remesadores, bancos, organismos les reportan y de ser posible los montos (...)"*** se considera información confidencial, por haber sido presentada en tal carácter por los Informantes del Sistema, en términos de la Ley del Sistema Nacional de Información Estadística y Geográfica.

ANÁLISIS DE LAS EXCEPCIONES PARA PERMITIR EL ACCESO A LA INFORMACIÓN CONFIDENCIAL

Adicionalmente, hacemos de su conocimiento que, de conformidad con 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 que este Instituto Central se encuentre facultado para permitir el acceso a la información confidencial antes señalada, en razón de que:

a. El Banco de México no cuenta con el consentimiento expreso y por escrito de los particulares titulares de la información que usted solicita, 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.

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, puesto que no forma parte de aquella que el Banco de México tiene la obligación de publicar en términos del artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública. Lo anterior, 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 tiene la calidad de sujeto obligado o sujeto de derecho internacional, 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.

Asimismo, les comunicamos que, 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", el personal que, por la naturaleza de sus atribuciones, tiene acceso a la información clasificada es: el personal adscrito a la Oficina de Servicios No Factoriales; el titular de la Subgerencia de Análisis del Sector Externo; la titular de la Gerencia de Análisis y Medición del Sector Real; el titular de la Dirección de Medición Económica; y el titular de la Dirección General de Investigación Económica.

Por lo expuesto, en términos de los artículos 44, fracción II, y 137, inciso a) de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, y 140, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como en el Vigésimo quinto de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", solicitamos a ese Comité de Transparencia confirmar la clasificación como confidencial de la información relativa a ***"(...) b) Que fuentes utilizan para integrar los flujos de Envios de Remesas de Estados Unidos a Mexico, que remesadores, bancos, organismos les reportan y de ser posible los montos (...)"*** realizada por esta unidad administrativa del Banco de México.

Atentamente

Mtro. Aldo Dylan Heffner Rodríguez
Director de Medición Económica

ANEXO "F"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
Folio: CTC-BM-23821

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

RESULTANDO

PRIMERO. El primero de junio de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **CTC-BM-23821,** que en su parte conducente refiere:

> *"Hola*
>
> *Muchas gracias por su respuesta a la solicitud CTC-BM-23191.*
>
> *Habria forma de conocer detalles adicionales sobre como se componen las series del Cuadro CE167? Especificamente a los envios de Estados Unidos a Mexico me gustaria saber lo siguiente:*
>
> *a) Deslgoce State (USA) a Estado (MX)*
> *b) Que fuentes utilizan para integrar los flujos de Envios de Remesas de Estados Unidos a Mexico, que remesadores, bancos, organismos les reportan y de ser posible los montos. Esto ultimo para poder calcular Market Shares de los jugadores en el mercado de las remesas de Estados Unidos a Mexico.*
>
> ..."

SEGUNDO. El primero de junio de dos mil dieciocho, la Unidad de Transparencia de este Instituto Central remitió a la Dirección General de Investigación Económica del Banco de México, para su atención, la referida solicitud, a través del sistema electrónico de gestión interna de solicitudes de información previsto para esos efectos.

TERCERO. El titular de la Dirección de Medición Económica, unidad administrativa adscrita a la Dirección General de Investigación Económica, mediante oficio de doce de junio del presente año, informó a este órgano colegiado que ha determinado clasificar como confidencial la información que precisa en el referido oficio, en términos de la fundamentación y motivación expresadas en el mismo.

CONSIDERANDOS

PRIMERO. 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, este Comité de Transparencia cuenta con facultades 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 unidades administrativas del Banco.

SEGUNDO. En seguida se analiza la clasificación realizada por la unidad administrativa referida, conforme a lo siguiente:

Este órgano colegiado advierte que es procedente la clasificación de la información referida como confidencial conforme a la fundamentación y motivación expresada en el oficio correspondiente.

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 expresada en el oficio señalado en la sección de resultandos de esta 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 como confidencial de la información** en términos del considerando Segundo de la presente resolución.

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

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

ANEXO "G"

BANCO DE MÉXICO

REF.: O10.GGF.010/2018
12 de junio de 2018

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

Me refiero a la solicitud de acceso a la información identificada con el número de folio **6110000030018,** la cual se transcribe a continuación:

> *"Por medio del presente solicito me se enviado, en formato digital el contrato de Fideicomiso relativo a los Museos Diego Rivera y Frida Kahlo, de igual forma solicito me informen lo siguiente (1) ¿Si dentro del patrimonio del Fideicomiso se incluyó la obra literaria El Diario de Frida Kahlo?; (2) ¿Si el Banco de México, en su calidad de fiduciario está facultado para otorgar licencias de uso a terceros sobre El Diario de Frida Kahlo?; (3) ¿Si el Banco de México está facultado para autorizar a terceros la adaptación de la obra literaria El Diario de Frida Kahlo en una obra audiovisual?; (4) ¿Si el Banco de México está facultado para autorizar a terceros producir una obra audiovisual basada en El Diario de Frida Kahlo y que dicha obra se pueda explotar o divulgar por cualquier medio o formato?; (5) ¿Si las licencias de uso que otorga el Banco de México están sujetas a Lineamientos o requisitos y cuáles son esos requisitos?; (6) Si para producir una obra audiovisual basada en El Diario de Frida Kahlo, además de la autorización del Banco de México, es necesario obtener el consentimiento de otro tercero (incluyendo herederos) para llevar a cabo una obra audiovisual basado en dicho diario, o sólo basta la licencia que otorgue el Banco de México?; y; (7)¿Cuáles serían los derechos y obligaciones derivados de la Licencia para ambas partes?"*

Sobre el particular me permito hacer de su conocimiento que la Unidad Administrativa a cargo del suscrito, ha clasificado como **confidencial** la información relativa a "*...solicito me se enviado, en formato digital el contrato de Fideicomiso relativo a los Museos Diego Rivera y Frida Kahlo...",* con fundamento en las siguientes disposiciones:

FUNDAMENTOS

1. De conformidad con el artículo 116, tercer párrafo, de la Ley General de Transparencia y Acceso a la Información Pública, 113, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como en el Trigésimo Octavo de los

"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" (en adelante "Lineamientos"), se considera información confidencial, los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos.

2. El Cuadragésimo Segundo de los mencionados Lineamientos, establece que para clasificar la información por secreto fiduciario o bancario, deberán acreditarse los siguientes elementos:

I. Que intervenga una institución de crédito realizando alguna de las operaciones referidas en la Ley de Instituciones de Crédito;

II. Que se refiera a datos o información que se obtenga o genere con motivo de la celebración de dichas operaciones;

III. Que sea requerida por una persona diversa al depositante, deudor, titular, beneficiario, fideicomitente, fideicomisario, comitente o mandante, a los representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio, y

IV. Que refiera a información cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos.

CONSIDERACIONES

1. El Fideicomiso Museos Diego Rivera y Frida Kahlo fue constituido por Diego Rivera en 1955, en el cual designó al Banco de México (en ese entonces S.A.) como Fiduciario, con el objeto de mantener abierto al público en general los Museos que hoy se conocen como Diego Rivera "Anahuacalli" y Frida Kahlo "Casa Azul".

El cumplimiento de los fines del citado fideicomiso se logra con la generación de recursos propios de su patrimonio, sin que el Banco de México por su propio derecho, aporte recursos a dicho patrimonio. En ese sentido, la naturaleza de los recursos que integran su patrimonio no es de naturaleza pública, como tampoco lo es la del propio Fideicomiso.

Sin perjuicio de que el fideicomiso de que se trata no se encuentra dentro de los previstos por el artículo 7 de la Ley del Banco de México, a la fecha este Instituto Central

continúa con el carácter de fiduciario en el mismo, con fundamento en el artículo Décimo Transitorio de su Ley.

Con base en lo anterior, esta unidad administrativa estima necesario clasificar como confidencial la información que nos ocupa, atendiendo a que la información solicitada constituye una operación materia del secreto fiduciario previsto en las disposiciones antes mencionadas, toda vez que en el caso concreto se actualizan todos y cada uno de los cuatro supuestos señalados en el apartado denominado Fundamentos, numeral 2 que antecede, en términos de lo que a continuación se indica:

i. En lo referente a la intervención de una institución de crédito realizando alguna de las operaciones referidas en la Ley de Instituciones de Crédito, la información que solicita el usuario se refiere al contrato de fideicomiso celebrado entre el señor Diego Rivera como fideicomitente y Banco de México como fiduciario, considerado como una operación de fideicomiso en términos de la fracción XV del artículo 46 de la Ley de Instituciones de Crédito, siendo el Banco de México una de las instituciones facultadas por la Ley para poder tener el carácter de Fiduciario, en términos de los artículos 7 y Décimo Transitorio de su Ley.

ii. Por su parte, en lo relativo a que se refiera a datos o información que se obtenga o genere con motivo de la celebración de dichas operaciones, es de destacar que la información que nos ocupa se refiere específicamente al contrato que rige al Fideicomiso Museos Diego Rivera y Frida Kahlo, que contiene entre otras disposiciones, aquéllas sobre la integración de su patrimonio, de su Comité Técnico, su constitución, atribuciones y funcionamiento, así como las características propias de la operación del fideicomiso en sí mismo. Motivo por el cual, la información solicitada se genera precisamente con motivo de la celebración de operaciones realizadas de conformidad con lo previsto en el artículo 46, fracción XV, de la Ley de Instituciones de Crédito.

iii. Adicionalmente, en lo relativo a que la información sea requerida por una persona diversa al depositante, deudor, titular, beneficiario, fideicomitente, fideicomisario, comitente o mandante, a los representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio, es de destacar que el solicitante no ha manifestado ubicarse en cualquiera de dichos supuestos, así como tampoco ha aportado elemento alguno que pudiera inferir la actualización de los mismos.

iv. Finalmente, respecto del requisito consistente en la que la solicitud se refiera a información cuya titularidad corresponda a particulares, sujetos de derecho internacional o sujetos obligados cuando no involucre el ejercicio de recursos públicos, en el caso

concreto la información corresponde a un patrimonio particular autónomo e independiente, con personalidad jurídica propia y distinta de la del Banco de México por propio derecho, sin que involucre en forma alguna el ejercicio de recursos públicos.

En consecuencia, con fundamento en los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, párrafo sexto, de la Constitución Política de los Estados Unidos Mexicanos; 116, tercer párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 4o, párrafo primero, 8o, 10, y 15 Bis, fracción IV, del Reglamento Interior del Banco de México; Primero, párrafo primero, y Segundo, fracción VII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como en el Trigésimo Octavo, y Cuadragésimo Segundo de los Lineamientos, la información relativa a "*...solicito me se enviado, en formato digital el contrato de Fideicomiso relativo a los Museos Diego Rivera y Frida Kahlo...*", contenida en la solicitud identificada con el número de folio **6110000030018**", **es clasificada como confidencial** por los motivos y fundamentos señalados en el presente escrito.

Finalmente, de conformidad con el Décimo de los Lineamientos, me permito hacer de su conocimiento que el personal que por la naturaleza de sus atribuciones tiene acceso a la información clasificada, es el adscrito a la Gerencia de Gestión Fiduciaria, a la Subgerencia Legal Fiduciaria, la Subgerencia de Control Presupuestal Fiduciario, así como a la Oficina Legal Fiduciaria.

Atentamente,

MTRO. LUIS RODRIGO SALDAÑA ARELLANO
Gerente de Gestión Fiduciaria

BANCO DE MÉXICO
RECIBIDO
14 JUN 2018
Comité de Transparencia
Por: Hora: 18:08

Se recibe oficio constante de cuatro páginas.

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000030018

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

RESULTANDO

PRIMERO. El primero de junio de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000030018,** que se transcribe a continuación:

> ***Descripción:*** *"Por medio del presente solicito me se enviado, en formato digital el contrato de Fideicomiso relativo a los Museos Diego Rivera y Frida Kahlo, de igual forma solicito me informen lo siguiente (1) ¿Si dentro del patrimonio del Fideicomiso se incluyó la obra literaria El Diario de Frida Kahlo?; (2) ¿Si el Banco de México, en su calidad de fiduciario está facultado para otorgar licencias de uso a terceros sobre El Diario de Frida Kahlo?; (3) ¿Si el Banco de México está facultado para autorizar a terceros la adaptación de la obra literaria El Diario de Frida Kahlo en una obra audiovisual?; (4) ¿Si el Banco de México está facultado para autorizar a terceros producir una obra audiovisual basada en El Diario de Frida Kahlo y que dicha obra se pueda explotar o divulgar por cualquier medio o formato?; (5) ¿Si las licencias de uso que otorga el Banco de México están sujetas a Lineamientos o requisitos y cuáles son esos requisitos?; (6) Si para producir una obra audiovisual basada en El Diario de Frida Kahlo, además de la autorización del Banco de México, es necesario obtener el consentimiento de otro tercero (incluyendo herederos) para llevar a cabo una obra audiovisual basado en dicho diario, o sólo basta la licencia que otorgue el Banco de México?; y; (7)¿Cuáles serían los derechos y obligaciones derivados de la Licencia para ambas partes?"*
>
> ***Datos adicionales:*** *"1 Banco de México, en su carácter de Fiduciario en el Fideicomiso relativo a los Museos Diego Rivera y Frida Kahlo.*
>
> *2 El Diario de Frida Kahlo.*
>
> *3.Otorgamiento de Licencias"*

SEGUNDO. El mismo primero de junio de dos mil dieciocho, la Unidad de Transparencia remitió, para su atención, la citada solicitud a la antes Gerencia Jurídica Fiduciaria, a través del sistema electrónico de gestión interna de solicitudes de información, previsto para esos efectos.

TERCERO. Con fecha treinta de mayo de dos mil dieciocho, se publicaron en el Diario Oficial de la Federación, las Reformas al Reglamento Interior y al acuerdo de adscripción de las Unidades Administrativas del Banco de México, a través del cual se modificó la denominación de la "Gerencia Jurídica Fiduciaria" por el de "Gerencia de Gestión Fiduciaria".

CUARTO. Con relación a los resultandos Segundo y Tercero, el titular de la Gerencia de Gestión Fiduciaria, mediante oficio REF.:O10.GGF.010/2018, informó a este Comité de Transparencia que dicha unidad administrativa: "... ha clasificado como confidencial la información relativa a " ... *solicito me se enviado, en formato digital el contrato de Fideicomiso relativo a los Museos Diego Rivera y Frida Kahlo* ... " Lo anterior, tal y como se fundamenta y motiva en el referido oficio, por lo que solicitó a este órgano colegiado confirmar dicha clasificación.

CONSIDERANDOS

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 unidades administrativas 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. En seguida se analiza la clasificación de la información realizada por la unidad administrativa señalada en el apartado de Resultandos de la presente determinación, conforme a lo siguiente:

Este órgano colegiado advierte que es procedente la clasificación de la información referida como confidencial conforme a la fundamentación y motivación expresada en el oficio correspondiente.

De igual manera, este Comité advierte que no se actualiza alguno de los supuestos de excepción previstos en la 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 expresada en el oficio señalado en la sección de Resultandos de esta 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 como confidencial de la información** realizada por la Gerencia de Gestión Fiduciaria del Banco de México, en términos del considerando Segundo de la presente resolución.

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

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

ANEXO "I"

BANCO DE MÉXICO

Ciudad de México, a 15 de junio 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 **6110000026518,** que ingresó el dieciséis de mayo 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 los RESULTADOS de evaluaciones o auditorías realizadas a BANAMEX respectos a su seguridad física, bases de datos y la seguridad implantada en sus transacciones, específicamente SPEI de 2017 y los últimos 4 meses. Saber si ha habido violaciones al sistema, ¿cuantas veces fue esto?, si no, los comentarios al respecto de parte de BANXICO. Los resultados se requieren a modo de estadística y a grosso modo."*
>
> ***Datos adicionales:***
>
> *"Evaluaciones o Auditorias a BANAMEX"*

Sobre el particular, 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 VIII, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 110, fracción VI y VIII, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); 1o., 2o., 35 Bis y 36 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; Segundo, fracciones I y VI del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Vigésimo cuarto y Vigésimo séptimo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas (Lineamientos), nos permitimos manifestarles que la información en posesión del Banco de México relativa a **los resultados de las evaluaciones o auditorías realizadas a Banamex respectos a su seguridad física, bases de datos y la seguridad implantada en sus transacciones, específicamente SPEI de 2017 y los últimos 4 meses. Saber si ha habido violaciones al sistema, ¿cuantas veces fue esto?, si no, los comentarios al respecto de parte de BANXICO** ha sido clasificada como **reservada**, al igual que la documentación correspondiente, por un periodo de **cinco años** a partir de la fecha en que dicha clasificación, en su caso, sea confirmada por ese órgano colegiado. Lo anterior, en virtud de que dicha información se encuentra directamente vinculada con un procedimiento en trámite que este Instituto Central se encuentra llevando a cabo como parte de sus actividades de verificación e inspección del cumplimiento de leyes y, a su vez, forma parte de un proceso deliberativo de los servidores públicos, respecto del cual aún no ha sido adoptada la decisión definitiva. En efecto, la información en cuestión ha sido recabada en ejercicio de sus facultades de inspección, supervisión o vigilancia y contiene opiniones, recomendaciones o puntos de vista relativos al procedimiento y proceso en comento, así como otra directamente relacionada con los mismos, por lo que su divulgación representa un riesgo:

1. **Real.** Lo anterior en virtud de que la información relacionada con el tema que nos ocupa está siendo analizada por el personal involucrado de las áreas competentes del Banco de México, por lo que su divulgación durante la existencia de un procedimiento de verificación del cumplimiento de leyes y de un proceso deliberativo puede conllevar percepciones erróneas o equívocas que pudieran afectar a la entidad financiera, la realización de actividades de inspección, supervisión y vigilancia, o la toma de decisiones en el proceso deliberativo por parte de este Instituto Central o de otras autoridades financieras que, en el ámbito de sus respectivas competencias, pueden llevar a cabo procedimientos o procesos similares relacionados con la información en comento.

Asimismo, de conformidad con los artículos vigésimo cuarto y vigésimo séptimo de los Lineamientos, se cumplen con los siguientes elementos:

a. **La existencia de un procedimiento de verificación del cumplimiento de las leyes en trámite y un proceso deliberativo en curso, precisando la fecha de inicio.** En efecto, en septiembre de 2017, este Instituto Central llevó a cabo una visita de supervisión a la institución de crédito referida en la solicitud con el fin de verificar el cumplimiento a las Disposiciones relativas Sistema de Pagos Electrónicos Interbancarios (SPEI), mismas que se detallan más adelante, respecto de la cual el proceso deliberativo se encuentra en curso.

b. **La vinculación directa con las actividades que realiza la autoridad en el procedimiento de verificación del cumplimiento de las leyes.** La información que la institución de banca múltiple en comento ha proporcionado a este Instituto Central, relacionada con la seguridad física, bases de datos y la seguridad implantada en sus transacciones, específicamente sobre el SPEI, es objeto de un minucioso análisis y revisión a fin de supervisar el cumplimiento de las disposiciones expedidas por el Banco en dicha materia aplicables a la entidad financiera.

c. **La difusión de la información impida u obstaculice las actividades de inspección, supervisión o vigilancia que realicen las autoridades en el procedimiento de verificación del cumplimiento de las leyes.** Esto se actualiza, toda vez que en caso de divulgación de la información, esta puede ser utilizada de forma incorrecta o errónea, modificada o alterada, impidiendo la evaluación de los procesos de la institución sujetos a las actividades de inspección, supervisión o vigilancia, por parte del Banco de México o de cualquier otra autoridad financiera con facultades similares en el ámbito de su competencia, ya sea, entre otros objetivos, para verificar el cumplimiento de disposiciones emitidas o el análisis de prácticas de mercado que afecten a los usuarios de los servicios financieros.

d. **La información consista en opiniones, recomendaciones o puntos de vista de los servidores públicos que participan en el proceso deliberativo**. En efecto, la información solicitada, contiene opiniones, recomendaciones y puntos de vista de los servidores públicos de diversas unidades administrativas del Banco de México, los cuales aún no son definitivos y están sujetos a cambios y modificaciones.

   En tal sentido, es importante mencionar que Banco de México debe analizar la información disponible para que su opinión esté debidamente fundada y motivada. Para realizar esta función, los servidores públicos de las unidades administrativas competentes deben examinar la información desde varios puntos de vista, opinando o recomendando sobre la conveniencia o inconveniencia de la toma de la decisión final. Dichas opiniones y recomendaciones son

contrastadas, argumentadas y discutidas entre los mismos servidores públicos, hasta que finalmente llegan a un consenso para adoptar la determinación final.

e. **La información se encuentre relacionada, de manera directa, con el proceso deliberativo.** La información que posee Banco de México relativa a la seguridad física, bases de datos y la seguridad implantada en las transacciones, específicamente sobre el Sistema de Pagos Electrónicos Interbancarios (SPEI), está directamente relacionada con la observancia de las "Reglas del Sistema de Pagos Electrónicos Interbancarios", dadas a conocer por medio de la Circular 17/2010, publicadas en el Diario Oficial de la Federación (DOF) el 15 de junio de 2010 y sus modificaciones, así como de la Circular 14/2017 publicada en el DOF el 4 de julio de 2017.

f. **Con su difusión se pueda llegar a interrumpir, menoscabar o inhibir el diseño, negociación, determinación o implementación de los asuntos sometidos a deliberación.** Cabe señalar que la información que se reserva consiste en insumos necesarios para el proceso deliberativo, puesto que es a través de tal información que podrá adoptarse una decisión definitiva respecto de la observancia de las disposiciones emitidas por este Banco Central.

Lo anterior, toda vez que revelar la información solicitada menoscabaría la determinación del asunto sometido a deliberación del Banco de México, ya que la divulgación de una decisión que no es la definitiva mandaría señales erróneas o equívocas sobre el cumplimiento del marco legal a la propia institución de crédito, a sus clientes, inversionistas, empleados, otras entidades con las que operan, principalmente, los demás participantes del SPEI y sus usuarios, así como en general respecto del sistema financiero mexicano, pudiendo poner en riesgo su estabilidad y funcionamiento, considerando que el SPEI, siendo el sistema de pagos más importante del país, es un elemento fundamental de la infraestructura financiera. También es importante mencionar que esperar a la decisión definitiva brinda seguridad jurídica a todas las partes. Esta finalidad podría no conseguirse de revelarse la información requerida por el particular con anterioridad a la toma de la opinión final del Banco de México.

Cabe señalar que si bien el solicitante únicamente requiere la información para sí mismo, el hecho de entregarla equivaldría a hacer pública la información, por lo que el Banco de México tendría que tomar medidas para que sus opiniones en el proceso deliberativo no se tomen como las definitivas, para que no se genere confusión entre las entidades del sistema financiero referidas, las autoridades en la materia y demás personas relacionadas con ellas.

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 un sistema de pagos sistémicamente importante 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.

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.

Efectivamente, en la inteligencia de que la clasificación de la información solicitada se lleva a cabo en términos de lo dispuesto por los artículos 113, fracciones VI y VIII, de la LGTAIP y 110, fracciones VI y VIII, de la LFTAIP, toda vez de que la información solicitada forma parte de un procedimiento de verificación del cumplimiento de las leyes que se encuentra en trámite y un proceso deliberativo respecto del cual aún no ha sido adoptada una decisión definitiva, dicha determinación es proporcional considerando que la difusión de la información solicitada generaría un riesgo de daño o perjuicio significativo, esto es, la interrupción o menoscabo de la determinación o su implementación, así como de las medidas y actos jurídicos que derivarían de la misma, lo cual sería claramente mayor a que se privilegiara el interés particular que pudiera existir en conocer dicha información.

En este orden de ideas, la clasificación como reservada respecto de la información solicitada, resulta el medio menos restrictivo disponible para evitar el perjuicio señalado anteriormente, así como la generación de percepciones erróneas o equívocas que pudieran afectar a la entidad financiera en particular, a sus clientes, inversionistas, empleados, otras entidades con las que operan, principalmente, los demás participantes del SPEI y sus usuarios, así como en general el sistema financiero mexicano, incluyendo a las autoridades financieras.

En atención a las consideraciones antes expuestas, concurren elementos que acreditan la existencia de un riesgo real, demostrable e identificable en el evento de que se divulgue la información solicitada. Asimismo, se considera que han quedado acreditadas también las circunstancias de modo, tiempo y lugar del daño o perjuicio significativo que se generaría al interés público con la divulgación de la información solicitada, las cuales pueden resumirse en los términos siguientes:

i. La información solicitada aún no es definitiva, pues forma parte de un procedimiento de verificación en trámite y un proceso deliberativo cuya decisión final aún no ha sido adoptada y, por lo tanto, su divulgación podría dar lugar a percepciones erróneas o equívocas.

ii. El riesgo de perjuicio por la publicidad de la información solicitada rebasa el interés público de que se dé a conocer su contenido, toda vez que se podría generar una percepción equivocada, por tratarse de un procedimiento de verificación en trámite y un proceso deliberativo inconcluso sujeto al análisis del Banco de México y sin menoscabar las facultades de otras autoridades financieras del país, en el ámbito de sus respectivas competencias, que podría afectar no solo a la institución de crédito en cuestión, sino también a otros participantes del SPEI y a sus respectivos usuarios.

Por lo anteriormente expuesto, con fundamento en lo establecido en 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; 100, 101, párrafo segundo, 103, 104, 105, 106, fracción I, 108, último párrafo, 109, 113, fracciones VI y VIII, y 114 de la LGTAIP; 97, párrafos primero, segundo y último, 98,

fracción I, 99, párrafo segundo, 100, 102, 103, 105, último párrafo, 106, 110, fracciones VI y VIII, y 111 de la LFTAIP; 1o., 2o. y 35 Bis y 36 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; Segundo, fracciones I y VI del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Vigésimo cuarto y Vigésimo séptimo, de los Lineamientos, la información en posesión del Banco de México, relativa a **los resultados de las evaluaciones o auditorías realizadas a Banamex respectos a su seguridad física, bases de datos y la seguridad implantada en sus transacciones, específicamente SPEI de 2017 y los últimos 4 meses. Saber si ha habido violaciones al sistema, ¿cuantas veces fue esto?, si no, los comentarios al respecto de parte de BANXICO**, ha sido clasificada como **reservada**, al igual que la documentación correspondiente, por un periodo de **cinco años** a partir de la fecha en que dicha clasificación, en su caso, sea confirmada por ese órgano colegiado.

A t e n t a m e n t e,

BANCO DE MÉXICO

VIVIANA GARZA SALAZAR
Directora de Regulación y Supervisión

OTHÓN MARTINO MORENO GONZÁLEZ
Gerente de Política y Vigilancia de los Sistemas de Pagos

BANCO DE MÉXICO
RECIBIDO
15 JUN 2018
Comité de Transparencia
Por: BIZ322 Hora: 15:56
Recibo este oficio en cinco páginas.

ANEXO "J"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000026518

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

RESULTANDO

PRIMERO. Que el dieciséis de mayo de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000026518,** la cual se transcribe a continuación:

> ***Descripción:*** *"Solicito los RESULTADOS de evaluaciones o auditorías realizadas a BANAMEX respectos a su seguridad física, bases de datos y la seguridad implantada en sus transacciones, específicamente SPEI de 2017 y los últimos 4 meses. Saber si ha habido violaciones al sistema, ¿cuantas veces fue esto?, si no, los comentarios al respecto de parte de BANXICO. Los resultados se requieren a modo de estadística y a grosso modo."*
>
> ***Datos adicionales:*** *"Evaluaciones o Auditorias a BANAMEX."*

SEGUNDO. Que la solicitud de información mencionada en el resultando anterior, fue turnada para su atención a la Dirección General de Asuntos del Sistema Financiero, y a la Dirección de Sistemas de Pagos, el mismo dieciséis de mayo del presente año, 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 con referencia D01/C351/2018, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la solicitud de acceso a la información.

CUARTO. Que este órgano colegiado, mediante resolución emitida en su sesión celebrada el siete de junio 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 Regulación y Supervisión, unidad administrativa adscrita a la Dirección General de Asuntos del Sistema Financiero, 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 del presente año, informaron a este órgano colegiado su determinación de clasificar la información precisada en dicho escrito, en los términos ahí señalados, respecto de la cual se elaboró la correspondiente prueba de daño, contenida en el cuerpo del oficio en comento, y solicitaron a este órgano colegiado confirmar tal clasificación.

CONSIDERANDO

PRIMERO. 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, este Comité de Transparencia cuenta con facultades 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 unidades administrativas del Banco.

SEGUNDO. Enseguida se analiza la clasificación realizada por las unidades administrativas señaladas en el resultando Quinto de la presente determinación, conforme a lo siguiente:

Este órgano colegiado advierte que es procedente la clasificación de la información señalada como **reservada,** toda vez que se ubica en los supuestos de reserva, en términos de **la fundamentación y motivación expresada en la prueba de daño** contenida en el 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 expresada en la correspondiente prueba de daño, contenida en el cuerpo del respectivo 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 expresada en la prueba de daño contenida en el oficio precisado en el resultando Quinto 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 veintiuno de junio dos mil dieciocho.----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

ANEXO "K"

BANCO DE MÉXICO

Ciudad de México, a 15 de junio 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 **6110000026618,** que ingresó el dieciséis de mayo 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 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. En caso de que la información contenga información personal, solicito versiones públicas."*
>
> ***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"*

Sobre el particular, 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 VIII, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 110, fracción VI y VIII, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); 1o., 2o., 35 Bis y 36 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; Segundo, fracciones I y VI del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Vigésimo cuarto y Vigésimo séptimo, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas (Lineamientos), nos permitimos manifestarles que 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 dicha clasificación, en su caso, sea confirmada por ese órgano colegiado. Lo anterior, en virtud de que dicha información se encuentra directamente vinculada con un procedimiento en trámite que este Instituto Central se encuentra llevando a cabo como parte de sus actividades de verificación e inspección del cumplimiento de leyes y, a su vez, forma parte de un proceso deliberativo de los servidores públicos, respecto del cual aún no ha sido adoptada la decisión definitiva. En efecto, la información en cuestión ha sido recabada en ejercicio de sus facultades de inspección, supervisión o vigilancia y contiene opiniones, recomendaciones o puntos de vista relativos al procedimiento y proceso en comento, así como otra directamente relacionada con los mismos, por lo que su divulgación representa un riesgo:

1. Real. Lo anterior en virtud de que la información relacionada con el tema que nos ocupa está siendo analizada por el personal involucrado de las áreas competentes del Banco de México, por lo que su divulgación durante la existencia de un procedimiento de verificación del cumplimiento de leyes y de un proceso deliberativo puede conllevar percepciones erróneas o equívocas que pudieran afectar a las entidades financieras, la realización de actividades de inspección, supervisión y vigilancia, o la toma de decisiones en el proceso deliberativo por parte de este Instituto Central o de otras autoridades financieras que, en el ámbito de sus respectivas competencias, pueden llevar a cabo procedimientos o procesos similares relacionados con la información en comento.

Asimismo, de conformidad con los artículos vigésimo cuarto y vigésimo séptimo de los Lineamientos, se cumplen con los siguientes elementos:

a. **La existencia de un procedimiento de verificación del cumplimiento de las leyes en trámite y un proceso deliberativo en curso, precisando la fecha de inicio.** En efecto, en el año 2017, este Instituto Central llevó a cabo visitas de supervisión a diversos participantes del SPEI con el fin de verificar el cumplimiento a las disposiciones relativas al SPEI, mismas que se detallan más adelante, respecto de las cuales los procesos deliberativos se encuentran en curso.

b. **La vinculación directa con las actividades que realiza la autoridad en el procedimiento de verificación del cumplimiento de las leyes.** La información que los participantes del SPEI han proporcionado a este Instituto Central, relacionada con el cumplimiento de los requerimientos establecidos por el Banco en materia de ciberseguridad, específicamente sobre el SPEI, es objeto de un minucioso análisis y revisión a fin de supervisar el cumplimiento de dichos requerimientos.

c. **La difusión de la información impida u obstaculice las actividades de inspección, supervisión o vigilancia que realicen las autoridades en el procedimiento de verificación del cumplimiento de las leyes.** Esto se actualiza, toda vez que en caso de divulgación de la información, esta puede ser utilizada de forma incorrecta o errónea, modificada o alterada, impidiendo la evaluación de los procesos de la instituciones sujetos a las actividades de inspección, supervisión o vigilancia, por parte del Banco de México o de cualquier otra autoridad financiera con facultades similares en el ámbito de su competencia, ya sea, entre otros objetivos, para verificar el cumplimiento de

disposiciones emitidas o el análisis de prácticas de mercado que afecten a los usuarios de los servicios financieros.

d. **La información consista en opiniones, recomendaciones o puntos de vista de los servidores públicos que participan en el proceso deliberativo.** En efecto, la información solicitada, contiene opiniones, recomendaciones y puntos de vista de los servidores públicos de diversas unidades administrativas del Banco de México, los cuales aún no son definitivos y están sujetos a cambios y modificaciones.

   En tal sentido, es importante mencionar que Banco de México debe analizar la información disponible para que su opinión esté debidamente fundada y motivada. Para realizar esta función, los servidores públicos de las unidades administrativas competentes deben examinar la información desde varios puntos de vista, opinando o recomendando sobre la conveniencia o inconveniencia de la toma de la decisión final. Dichas opiniones y recomendaciones son contrastadas, argumentadas y discutidas entre los mismos servidores públicos, hasta que finalmente llegan a un consenso para adoptar la determinación final.

e. **La información se encuentre relacionada, de manera directa, con el proceso deliberativo.** La información que posee Banco de México relacionada con el cumplimiento de los requerimientos emitidos por el Banco en materia de ciberseguridad, específicamente sobre el SPEI, está directamente relacionada con la observancia de las "Reglas del Sistema de Pagos Electrónicos Interbancarios", dadas a conocer por medio de la Circular 17/2010, publicadas en el Diario Oficial de la Federación (DOF) el 15 de junio de 2010 y sus modificaciones, así como de la Circular 14/2017 publicada en el DOF el 4 de julio de 2017.

f. **Con su difusión se pueda llegar a interrumpir, menoscabar o inhibir el diseño, negociación, determinación o implementación de los asuntos sometidos a deliberación.** Cabe señalar que la información que se reserva consiste en insumos necesarios para el proceso deliberativo, puesto que es a través de tal información que podrá adoptarse una decisión definitiva respecto de la observancia de las disposiciones emitidas por este Banco Central.

   Lo anterior, toda vez que revelar la información solicitada menoscabaría la determinación de los asuntos sometidos a deliberación del Banco de México, ya que la divulgación de una decisión que no es la definitiva mandaría señales erróneas o equívocas sobre el cumplimiento del marco legal a las propias instituciones de crédito, a sus clientes, inversionistas, empleados, otras entidades con las que operan, principalmente, los demás participantes del SPEI y sus usuarios, así como en general, respecto del sistema financiero mexicano, pudiendo poner en riesgo su estabilidad y funcionamiento, considerando que el SPEI, siendo el sistema de pagos más importante del país, es un elemento fundamental de la infraestructura financiera. También es importante mencionar que esperar a la decisión definitiva brinda seguridad jurídica a todas las partes. Esta finalidad podría no conseguirse de revelarse la información requerida por el particular con anterioridad a la toma de la opinión final del Banco de México.

   Cabe señalar que si bien el solicitante únicamente requiere la información para sí mismo, el hecho de entregarla equivaldría a hacer pública la información, por lo que el Banco de México tendría que tomar medidas para que sus opiniones en el proceso deliberativo no se tomen como las definitivas, para que no se genere confusión entre las entidades del sistema financiero referidas, las autoridades en la materia y demás personas relacionadas con ellas.

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 un sistema de pagos sistémicamente importante 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.

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.

Efectivamente, en la inteligencia de que la clasificación de la información solicitada se lleva a cabo en términos de lo dispuesto por los artículos 113, fracciones VI y VIII, de la LGTAIP y 110, fracciones VI y VIII, de la LFTAIP, toda vez que la información solicitada forma parte de un procedimiento de verificación del cumplimiento de las leyes que se encuentra en trámite y un proceso deliberativo respecto del cual aún no ha sido adoptada una decisión definitiva, dicha determinación es proporcional considerando que la difusión de la información solicitada generaría un riesgo de daño o perjuicio significativo, esto es, la interrupción o menoscabo de la determinación o su implementación, así como de las medidas y actos jurídicos que derivarían de la misma, lo cual sería claramente mayor a que se privilegiara el interés particular que pudiera existir en conocer dicha información.

En este orden de ideas, la clasificación como reservada respecto de la información solicitada, resulta el medio menos restrictivo disponible para evitar el perjuicio señalado anteriormente, así como la generación de percepciones erróneas o equívocas que pudieran afectar a la entidad financiera en particular, a sus clientes, inversionistas, empleados, otras entidades con las que operan, principalmente, los demás participantes del SPEI y sus usuarios, así como en general el sistema financiero mexicano, incluyendo a las autoridades financieras.

En atención a las consideraciones antes expuestas, concurren elementos que acreditan la existencia de un riesgo real, demostrable e identificable en el evento de que se divulgue la información solicitada. Asimismo, se considera que han quedado acreditadas también las circunstancias de modo, tiempo y lugar del daño o perjuicio significativo que se generaría al interés público con la divulgación de la información solicitada, las cuales pueden resumirse en los términos siguientes:

i. La información solicitada aún no es definitiva, pues forma parte de un procedimiento de verificación en trámite y un proceso deliberativo cuya decisión final aún no ha sido adoptada y, por lo tanto, su divulgación podría dar lugar a percepciones erróneas o equívocas.

ii. El riesgo de perjuicio por la publicidad de la información solicitada rebasa el interés público de que se dé a conocer su contenido, toda vez que se podría generar una percepción equivocada, por tratarse de un procedimiento de verificación en trámite y un proceso deliberativo inconcluso sujeto al análisis del Banco de México y sin menoscabar las facultades de otras autoridades financieras del país, en el ámbito de sus respectivas competencias, que podría afectar no solo a la institución de crédito en cuestión, sino también a otros participantes del SPEI y a sus respectivos usuarios.

Por lo anteriormente expuesto, con fundamento en lo establecido en 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; 100, 101, párrafo segundo, 103, 104, 105, 106, fracción I, 108, último párrafo, 109, 113, fracciones VI y VIII, y 114 de la LGTAIP; 97, párrafos primero, segundo y último, 98, fracción I, 99, párrafo segundo, 100, 102, 103, 105, último párrafo, 106, 110, fracciones VI y VIII, y 111 de la LFTAIP; 1o., 2o. y 35 Bis y 36 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; Segundo, fracciones I y VI del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Vigésimo cuarto y Vigésimo séptimo, de los Lineamientos, 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 dicha clasificación, en su caso, sea confirmada por ese órgano colegiado.

Atentamente,

BANCO DE MÉXICO

VIVIANA GARZA SALAZAR
Directora de Regulación y Supervisión

OTHÓN MARTINO MORENO GONZÁLEZ
Gerente de Política y Vigilancia de los Sistemas de Pagos

BANCO DE MÉXICO
RECIBIDO
15 JUN 2018
Comité de Transparencia
Por: B12322 Hora: 15:57
Recibo este oficio en cinco páginas.

ANEXO "L"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000026618

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

RESULTANDO

PRIMERO. Que el diecisiete de mayo de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000026618,** la cual se transcribe a continuación:

> ***Descripción:*** *"Solicito 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. En caso de que la información contenga información personal, solicito versiones públicas."*
>
> ***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 la solicitud de información mencionada en el resultando anterior, fue turnada para su atención a la Dirección General de Asuntos del Sistema Financiero, y a la Dirección de Sistemas de Pagos, el mismo diecisiete de mayo del presente año, 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 con referencia D01/C352/2018, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la solicitud de acceso a la información.

CUARTO. Que este órgano colegiado, mediante resolución emitida en su sesión celebrada el siete de junio 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 Regulación y Supervisión, unidad administrativa adscrita a la Dirección General de Asuntos del Sistema Financiero, 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 del presente año, informaron a este órgano colegiado su determinación de clasificar la información precisada en dicho escrito, en los términos ahí señalados, respecto de la cual se elaboró la correspondiente prueba de daño, contenida en el cuerpo del oficio en comento, y solicitaron a este órgano colegiado confirmar tal clasificación.

CONSIDERANDO

PRIMERO. 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, este Comité de Transparencia cuenta con facultades 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 unidades administrativas del Banco.

SEGUNDO. Enseguida se analiza la clasificación realizada por las unidades administrativas señaladas en el resultando Quinto de la presente determinación, conforme a lo siguiente:

Este órgano colegiado advierte que es procedente la clasificación de la información señalada como **reservada,** toda vez que se ubica en los supuestos de reserva, en términos de **la fundamentación y motivación expresada en la prueba de daño** contenida en el 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 expresada en la correspondiente prueba de daño, contenida en el cuerpo del respectivo 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 expresada en la prueba de daño contenida en el oficio precisado en el resultando Quinto 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 veintiuno de junio dos mil dieciocho. ----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

ANEXO "M"

BANCO DE MÉXICO

Ciudad de México, a 15 de junio de 2018
D01/C366/2018

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

En relación con la solicitud de acceso a la información identificada con el número de folio **61100000029418** que nos hizo llegar la Unidad de Transparencia el treinta de mayo 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, así como de la Ley Federal de Transparencia y Acceso a la Información Pública, la cual para pronta referencia se transcribe a continuación:

> *"En su Información sobre los ataques a participantes del SPEI, informaron que el 17 de abril UN PARTICIPNTE del SPEI registró un ataque cibernético y que a partir de esa fecha se han identificado 4 eventos adicionales de ataque cibernético: dos el 24 de abril, uno el 26 de abril y uno más el 8 de mayo. Quiero saber si BANAMEX fue ese participante que estuvo involucrado en estos ataques cibernéticos."*

Así como la siguiente información adicional que se nos proporcionó:

> *"Quiero saber si BANAMEX fue el participante que estuvo involucrado en os ataques cibernéticos de ABRIL y MAYO del 2018."*

Al efecto, me permito hacer de su conocimiento que, esta unidad administrativa **ha clasificado como reservado el pronunciamiento respecto de confirmar o refutar los ataques a un participante específico del Sistema de Pagos Electrónicos Interbancarios (SPEI),** en atención a las siguientes consideraciones:

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

   a) Menoscabe 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;

   b) Comprometa las acciones encaminadas a propiciar el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos, y

c) Genere 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.

2) En ese sentido, pronunciarse respecto de **confirmar o refutar los ataques a un participante específico del 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 propiciar el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos; otorgaría ventaja indebida a los cibercriminales para diseñar estrategias de ataques cibernéticos a los participantes de las Infraestructuras de los Mercados Financieros (IMF), entre ellas el SPEI, generando distorsiones en la estabilidad de los mercados financieros; 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 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 estos riesgos cibernéticos puede perturbar considerablemente al sistema financiero por su efecto directo en la información y operaciones relativas a los usuarios de los sistemas de pagos -tanto de las instituciones financieras como de las personas físicas y morales-.

   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.

---

[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.

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 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 código malicioso a más de 20 bancos

---

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. http://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/ consultado el 13 de junio de 2018.

4 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 junio 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, consultado el 13 de junio de 2018.

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=es consultado el 13 de junio de 2018.

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]

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 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;[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 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 automáticos basado en red, es decir que no se requiere acceso físico al cajero

---

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 junio 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 junio 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.

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 junio 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 junio 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 junio de 2018.

para perpetrarlos, sino que la infección se lleva a cabo desde la propia red interna del banco;[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 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.[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]

x) 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

---

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-cajeros-automaticos-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 junio de 2018.

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 junio 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 junio de 2018.

17 Clavijo R. Felipe, Osorio 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 junio 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/%7B2B9BB8CB-D66B-38C4-CC90-F72A7BC335C9%7D.pdf, consultado el 13 de junio de 2018.

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 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

---

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

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

[22] 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 junio 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 junio de 2018.

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 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 marzo de 2017 a marzo de 2018, se realizaron aproximadamente 544 millones de pagos electrónicos interbancarios por un monto de 293 billones de pesos;[24] lo anterior equivale a más de 62 mil operaciones por un monto de 33 mil millones de pesos por hora, únicamente para lo que respecta al SPEI.

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,

[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

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, 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, segundo párrafo, 104, 105, 106, fracción III, 107, 108, último párrafo, 109, 113, fracciones IV, y 114 de la LGTAIP; 110, fracciones IV, y 111 de la LFTAIP, 1o., 2o. y 3o., fracción I, de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, y tercero, 10, párrafo primero, 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, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I, II y IV, de los Lineamientos, **se clasifica como reservado el pronunciamiento respecto de confirmar o refutar los ataques a un participante específico del SPEI 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 informática, con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de tecnologías de la información y comunicaciones, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques informáticos, no solo de las 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.

Atentamente,

Dr. Manuel Miguel Ángel Díaz Díaz
Director de Sistemas de Pagos

United States Government Accountability Office

GAO

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

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

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

David A. Powner, Director
Information Technology Management Issues

GAO-10-230T

BANCO DE MÉXICO

REFERENCIA 2

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, 2015 @ 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 4

Informe Norton sobre Ciberseguridad 2016

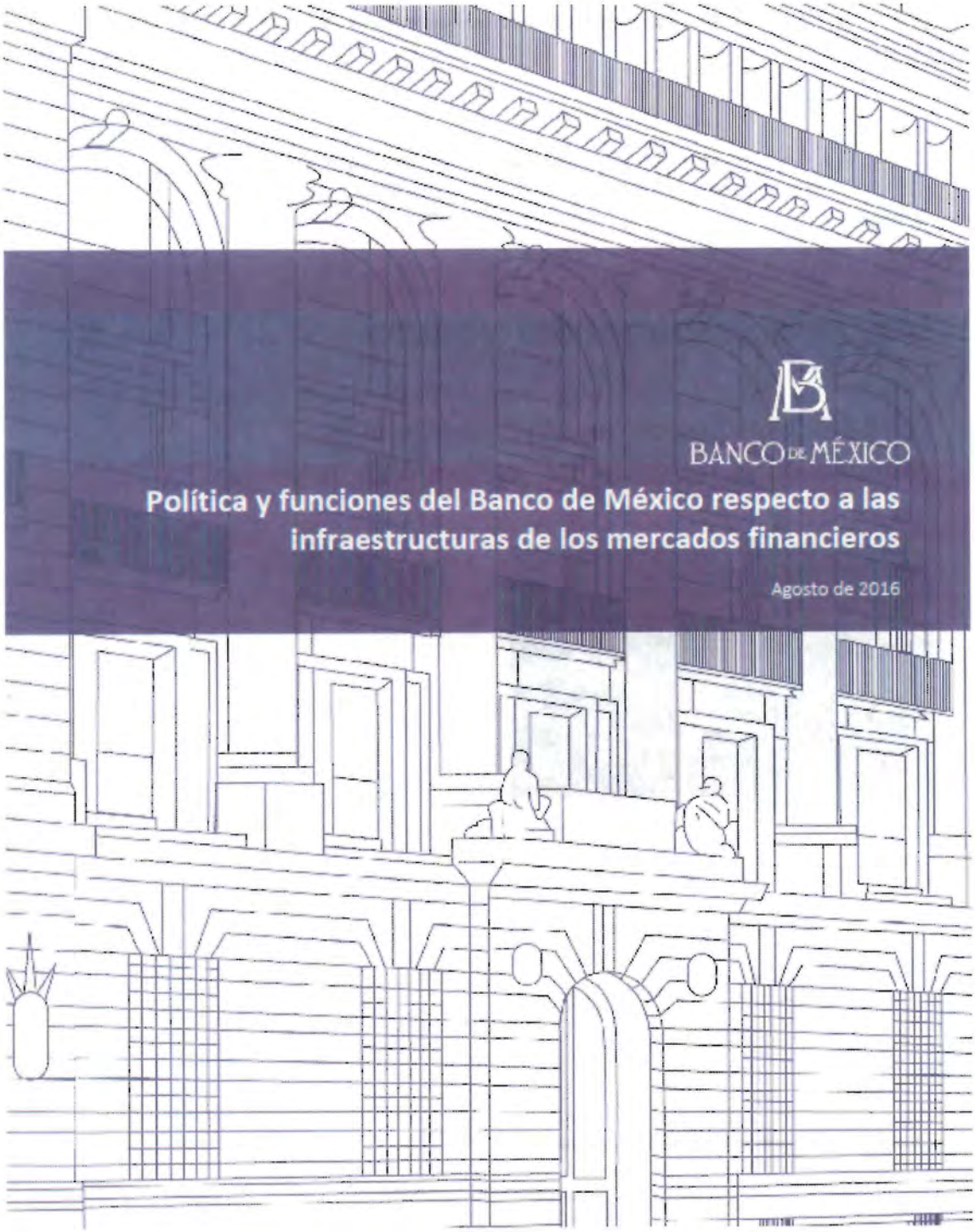
Comparaciones Globales

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 by Symantec

BANCO DE MÉXICO

REFERENCIA 5



BANCO DE MÉXICO

REFERENCIA 6

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 8

BAE SYSTEMS THREAT RESEARCH BLOG

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

WANACRYPTOR 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

DOI: 10.1016/j.wneu.2017.08.164

CITATION
1

READS
142

1 author:

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

SEE PROFILE

REFERENCIA 10

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.

REFERENCIA 11

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

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

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

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

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

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

Teléfono de Comunicación Social: 15551024

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

REFERENCIA 12

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

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 2, 2018 8:00am 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.alclearid.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, CVV 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.

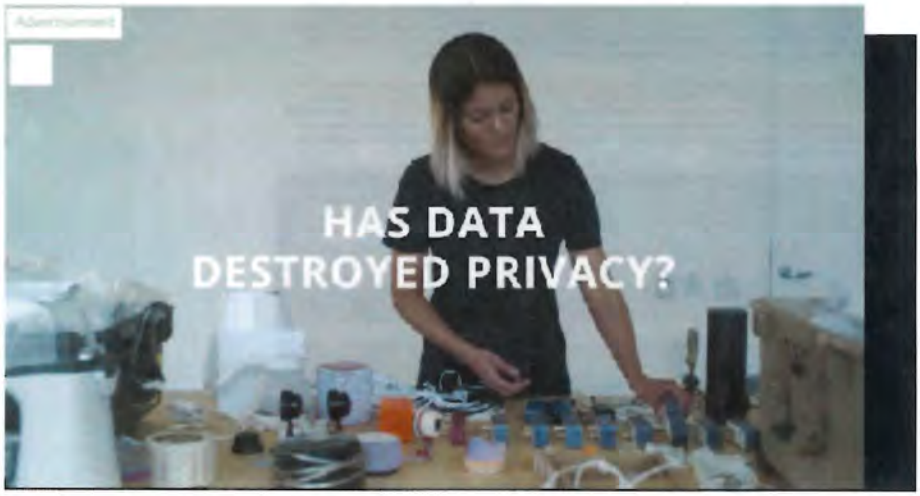
REFERENCIA 16

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.

REFERENCIA 17

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.

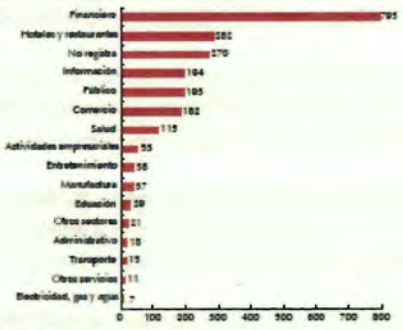
La forma más común como se ha materializado el riesgo cibernético en años recientes ha sido mediante lo que se conoce como ataques cibernéticos. En esencia, estos son acciones ilegales realizadas por *hackers*, con el objetivo principal de obtener cierto beneficio, al generar daños en los sistemas tecnológicos 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 *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.

REFERENCIA 18

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 19

BANCO DE MÉXICO

REFERENCIA 20

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: ()

Created 18 Dec 2001 0 Comments

0 0

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

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

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 23

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 24

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real.

Fecha de consulta: 27/04/2018 11:04:05

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 - Mar 2018	Ene 1992 - Mar 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

ANEXO "N"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000029418

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

RESULTANDO

PRIMERO. Que el treinta de mayo de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000029418,** la cual se transcribe a continuación:

> ***Descripción:*** *"En su Información sobre los ataques a participantes del SPEI, informaron que el 17 de abril UN PARTICIPNTE del SPEI registró un ataque cibernético y que a partir de esa fecha se han identificado 4 eventos adicionales de ataque cibernético: dos el 24 de abril, uno el 26 de abril y uno más el 8 de mayo. Quiero saber si BANAMEX fue ese participante que estuvo involucrado en estos ataques cibernéticos."*
>
> ***Datos adicionales:*** *"Quiero saber si BANAMEX fue el participante que estuvo involucrado en os ataques cibernéticos de ABRIL y MAYO del 2018."*

SEGUNDO. Que la solicitud de información mencionada en el resultando anterior, fue turnada para su atención a la Dirección de Sistemas de Pagos, el mismo treinta de mayo del presente año, 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, mediante oficio con referencia D01/C366/2018, informó a este órgano colegiado su determinación de clasificar la información precisada en dicho escrito, en los términos ahí señalados, respecto de la cual se elaboró la correspondiente prueba de daño, contenida en el cuerpo del oficio en comento, y solicitó a este órgano colegiado confirmar tal clasificación.

CONSIDERANDO

PRIMERO. 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, este Comité de Transparencia cuenta con facultades 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 unidades administrativas del Banco.

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

Este órgano colegiado advierte que es procedente la clasificación de la información señalada como **reservada,** toda vez que se ubica en los supuestos de reserva, en términos de **la fundamentación y motivación expresada en la prueba de daño** contenida en el 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 expresada en la correspondiente prueba de daño, contenida en el cuerpo del respectivo 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

ÚNICO. Se **confirma la clasificación de la información referida como reservada,** conforme a la fundamentación y motivación expresada en la prueba de daño contenida en el 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 veintiuno de junio dos mil dieciocho. ----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

ANEXO "Ñ"

BANCO DE MÉXICO

Ciudad de México, a 15 de junio de 2018
D01/ C363/2018

COMITÉ DE TRANSPARENCIA
DEL BANCO DE MÉXICO
Presente

Me refiero a la solicitud de acceso a la información, identificada con el número de folio **6110000029618**, que nos turnó la Unidad de Transparencia el treinta de mayo 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, que se transcribe a continuación:

> *"Las Recomendaciones de los reportes correspondientes a las pruebas de penetración de 5 años a la fecha del Sistema SPEI. Los resultados de los últimos 5 años de las auditorías externas e internas de la Unidad de Auditoría de BANXICO y que se mandan a realizar por medio de la misma UNIDAD a unidades externas."*

Y de la cual se proporcionó como información adicional:

> *"Resultados de auditorias internas y externas a SPEI de los últimos 5 años y resultados de pruebas de penetración a SPEI de los últimos 5 años."*

Al respecto, me permito informarles que con motivo de la publicación de información de obligaciones de transparencia, ese órgano colegiado aprobó y confirmó la clasificación de la información que a continuación se detallará, la cual se fundamentó y motivó en la prueba de daño respectiva.

A este respecto, hago de su conocimiento que los documentos que se detallan en el siguiente cuadro se ubican en el supuesto del párrafo precedente, materia de la presente solicitud, y en ellos subsisten las causas que dieron origen a su clasificación.

TÍTULO DEL DOCUMENTO CLASIFICADO	PLAZO DE RESERVA	VENCIMIENTO DEL PLAZO DE RESERVA	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)	SESIÓN DEL COMITÉ
Consultoría PT SPEI 2015	5 años	06 de febrero 2023	http://archivo/sitio/atac/DocumentosBM/Unidad%20de%20Transparencia/Versiones%20públicas/2018/Especiales/VP%20Esp%2006-18/3901.%20Consultoria%20PT%20SPEI%202015.pdf	Sesión especial 06/2018
Consultoría PT SPEI 2016	5 años	13 de diciembre 2018	http://archivo/sitio/atac/DocumentosBM/Forms/AllItems.aspx?RootFolder=%2Fsitio%2Fatac%2FDocumentosBM%2FDGTI%2FAdministraci%C3%B3n%20de%20servicios%20de%20la%20DGTI%2FSeguridad%20inform%C3%A1tica%2FConfidenciales%2FConsultorias%20de%20Seguridad%2F2016%2FPentest%20SPEI%20%2D%20Deloitte&InitialTabId=Ribbon%2EDocument&VisibilityContext=WSSTabPersistence	Sesión especial 15/2017
Consultoría PT SPEI 2017	5 años	06 de febrero 2023	http://archivo/sitio/atac/DocumentosBM/Unidad%20de%20Transparencia/Versiones%20públicas/2018/Especiales/VP%20Esp%2006-18/3903.%20Consultoria%20PT%20SPEI%202017.pdf	Sesión especial 06/2018

BANCO DE MÉXICO

Por otro lado, esta área ha determinado clasificar de manera total la información contenida en el documento que se indica más adelante, y en consecuencia, se ha elaborado la correspondiente prueba de daño, que se adjuntan al presente. Dichos documentos se encuentran disponibles a partir de esta fecha en la carpeta compartida ubicada en la red interna del Banco de México, a la que se puede acceder a través de la siguiente liga:

I:\A13 Dir Unidad de Transparencia\Comité de Transparencia Compartida\2018\Sesiones Ordinarias 2018\Asuntos para sesión

Para facilitar su identificación, en el siguiente cuadro encontrarán el detalle del título del documento clasificado y la liga respectiva al repositorio institucional en el que reside la versión digitalizada de dicho documento original. Es importante señalar que, por tratarse de información altamente sensible, dichas ligas son de acceso restringido; no obstante lo anterior, dichos documentos se pondrán a disposición de los miembros del Comité de Transparencia, en caso de que lo requieran.

TÍTULO DEL DOCUMENTO CLASIFICADO	PRUEBA DE DAÑO NÚMERO DE ANEXO	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)
Informe de Resultados de Auditoría GATIE-26/13 denominada "Sistema de Pagos Electrónicos Interbancarios (SPEI)"	Anexo único	http://archivo/otrs/static/DocumentosBM/Direccion%20de%20Auditoria/Practicas%20de%20auditoria/Confidenciales/Carpeta%20Sistemas%20de%20Gobierno%20de%20Pagos/Informes%20GATIE-26-13%20Sistema%20de%20Pagos%20Electronicos%20Interbancarios%20SPEI.pdf

Atento a lo anterior, y con fundamento 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; solicito a ese órgano colegiado confirme la subsistencia de la clasificación de los documentos que se detallaron, y se confirme la clasificación del documento fundamentado y motivado en la respectiva prueba de daño.

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 señalado es el adscrito a la Unidad de Auditoría, la Gerencia de Operación y Continuidad de Negocio de los Sistemas de Pagos y la Gerencia de Tecnología de los Sistemas de Pagos, las dos últimas adscritas a la Dirección de Sistemas de Pagos.

Atentamente,

Dr. Manuel Miguel Ángel Díaz Díaz
Director de Sistemas de Pagos

BANCO DE MÉXICO
RECIBIDO
15 JUN 2018
Comité de Transparencia
Por: B12322 Hora: 15:38
Recibo este oficio en dos páginas y una prueba de daño.

BANCO DE MÉXICO

PRUEBA DE DAÑO

Información relacionada con las auditorías internas realizadas al Sistema de Pagos Electrónicos Interbancarios (SPEI)

En términos de lo dispuesto 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; 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, II y IV, 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 materia del sistema financiero o económico del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto; y

- Comprometa las acciones encaminadas a proveer el sano desarrollo del sistema financiero o el buen funcionamiento de los sistemas de pago.

- Genere 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.

Por lo que la ***Información relacionada con las auditorías internas realizadas al Sistema de Pagos Electrónicos Interbancarios (SPEI)*** contenida en el documento que ampara la presente prueba de daño, es clasificada como reservada, en virtud de lo siguiente:

La **divulgación** de la citada información representa **un riesgo de perjuicio significativo** al interés público ya que menoscabaría la efectividad de las medidas implementadas en materia del sistema financiero o económico del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto; asimismo, comprometería las acciones encaminadas a proveer el sano desarrollo del sistema financiero o el buen funcionamiento de los sistemas de pago, en este caso el Sistema de Pagos Electrónicos Interbancarios (SPEI), toda vez que dicho riesgo es:

1. **Real**, en razón de **revelar o divulgar la *Información relacionada con las auditorías internas realizadas al Sistema de Pagos Electrónicos Interbancarios (SPEI),*** facilitaría a una persona o grupo de personas con intenciones delincuenciales identificar aspectos de seguridad informática, entre ellos, aquellos relacionados con el control de acceso y seguridad de la información a los programas fuente y ejecutables, funcionalidad, actualización tecnológica, control de cambios, manejo de incidentes y problemas, continuidad operativa, segregación de funciones, seguimiento de observaciones en caso de que existan, y en general, información relacionada con el SPEI y su infraestructura informática, lo cual posibilita la

realización de acciones hostiles en contra de las tecnologías de la información que administra, opera y supervisa este Banco Central, en específico el SPEI.

Lo anterior, podría menoscabar la efectividad de la mencionada infraestructura a tal grado, que su destrucción o inhabilitación provocaría un impacto debilitador a la seguridad nacional, y a las medidas implementadas en materia del sistema financiero o económico del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto; asimismo, comprometería las acciones encaminadas a proveer el sano desarrollo del sistema financiero o el buen funcionamiento de los sistemas de pago, en este caso el SPEI.

Los riesgos aludidos tienen mayor probabilidad de materializarse con la entrega de la información, debido a que **los delincuentes podrían diseñar estrategias para llevar a cabo ataques cibernéticos** dirigidos específicamente al SPEI; dichos ataques focalizados podrían tener mayor probabilidad de éxito debido a que los delincuentes tendrían la posibilidad de dedicar todos sus recursos a ataques específicos identificados con base en la información en cuestión.

Por lo anterior, exponer al SPEI a estos riesgos cibernéticos **puede perturbar considerablemente al sistema financiero por su efecto directo en la información y operaciones relativas a los usuarios de los sistemas de pagos -tanto de las instituciones financieras como de las personas físicas y morales-**.

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

En efecto, proporcionar la información materia de la presente prueba de daño, **facilitaría que terceros logren acceder a información financiera o personal**, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a dichas tecnologías.

Asimismo, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se fundamentan en descubrir y aprovechar vulnerabilidades de dichos sistemas, basando cada descubrimiento en el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, seguridad informática, especificaciones técnicas en materia de seguridad, procesos de continuidad operativa y, en general, información relacionada con los sistemas correspondientes e infraestructura informática.

Está documentado en la literatura especializada en la materia que los principales elementos de información que requiere conocer un cibercriminal son: la arquitectura de los sistemas,

sus especificaciones técnicas, horarios de operación, funcionalidad general, protocolos de comunicación, aspectos de seguridad informática instrumentados, entre otros, para descubrir y aprovechar los puntos débiles que pudieran existir en estos elementos y atacar a los sistemas.[1]

En el caso en concreto, la ***Información relacionada con las auditorías internas realizadas al Sistema de Pagos Electrónicos Interbancarios (SPEI),*** contiene información relacionada con el control de acceso y seguridad de la información a los programas fuente y ejecutables, funcionalidad, actualización tecnológica, control de cambios, manejo de incidentes y problemas, continuidad operativa, segregación de funciones, seguimiento de observaciones en caso de que existan, y en general, información relacionada con el SPEI, por lo que su divulgación proporcionaría elementos de información que facilitarían a los cibercriminales aprovechar los puntos débiles de este sistema de pago, 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 esta infraestructura.

2. **Demostrable, ya que es un hecho notorio que los sistemas de pagos de Bancos Centrales han sufrido ataques cibernéticos a través de estas infraestructuras**, como SWIFT, la cual ha sido utilizada para realizar robos de capital, uno de estos casos es el del Banco Central de Bangladesh, que sufrió un robo de 81 millones de dólares.[2] 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.[3] 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.[4] Asimismo, los sistemas de empresas como Google, Facebook, PayPal y el New York Times se han visto comprometidos por ataques cibernéticos.[5] 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.[6]

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

---

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 Michael Riley, Alan Katz. "Swift Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh". Bloomberg. 26 Mayo 2016.

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

4 Antony Peyton. "Symantec reveals more hack attempts on Swift network". Banking Technology. 11 de octubre de 2016.

5 Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.

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

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

b) 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]

c) 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]

d) 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;[11]

e) 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]

f) 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

---

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 14 de junio de 2018.

8 BAE Systems Applied Intelligence. "BAE Systems Threat Research Blog." Lazarus & Watering-Hole Attacks, 1 de enero de 1970, http://baesystemsai.blogspot.mx/2017/02/lazarus-watering-hole-attacks.html . consultado el 2 de mayo de 2018. consultado el 14 de junio 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.

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 14 de junio de 2018.

11 BANCOMEXT. "Acción oportuna de BANCOMEXT salvaguarda intereses de clientes y la institución", http://www.bancomext.com/comunicados/18443, consultado el 14 de junio 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, consultada el 14 de junio 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;[13]

g) 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]

h) 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.[15]

i) El ataque ocurrido a las instituciones financieras participantes del SPEI, el cual consistió en la alteración de sus aplicativos para conectarse al SPEI de algunos participantes, 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.[16] 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.[17]

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

---

13 S21Sec. "COBALT: EL CIBERCRIMEN ORGANIZADO GOLPEA LOS CAJEROS AUTOMÁTICOS EUROPEOS." S21Sec, 23 Nov. 2016, www.s21sec.com/es/blog/2016/11/cobalt-cibercrimen-organizado-que-ataca-a-los-cajeros-automaticos-europeos consultado el 14 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 14 de junio de 2018.

15 Delta Airlines. "INFORMATION ON [24]7.AI CYBER INCIDENT." Information on [24]7.Ai Cyber Incident, 7 de abril 2018, www.delta.com/content/www/en_US/response.html consultado el 14 de junio de 2018.

16 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 14 de junio de 2018.

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

sofisticados ataques dirigidos contra sus sistemas de información derivado de la aplicación de técnicas de ingeniería social.[18]

Por lo anterior, los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuyo rol no esté autorizado,[19] en el entendido de que dicha información, al estar en posesión de personas no autorizadas, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central de la Nación, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

En este sentido, la divulgación de la información materia de la presente prueba de daño, potencializaría que hechos como los mencionados ocurran en las infraestructuras de los mercados financieros, entre ellas, el SPEI que administra y opera el Banco de México, puesto que de divulgarse la información requerida por el solicitante, los cibercriminales contarían con los elementos necesarios para perpetrar un ataque informático directo a este Instituto Central, y en específico al SPEI. Lo anterior, puede conducir al incumplimiento de sus obligaciones hacia los participantes del sistema financiero y/o provocar que a su vez, estos no puedan cumplir con sus propias obligaciones, y en consecuencia, generar un colapso del sistema financiero nacional o de los sistemas de pagos, lo que iría en contravención a lo establecido en el artículo 2o. de la Ley del Banco de México.

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 estos ataques no han logrado irrumpir o vulnerar el SPEI, infraestructura que administra y opera el Banco de México, puede concluirse que existe la probabilidad de que el objeto de dichos ataques considere a esta infraestructura, 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 relacionada con las auditorías internas realizadas al Sistema de Pagos Electrónicos Interbancarios (SPEI),* 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

---

18 Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, 18 de diciembre de 2001.

19 Ver por ejemplo las 10 medidas básicas de ciberseguridad de la Security Information Center, en partícular 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 junio de 2018.

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 el SPEI 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 del SPEI**, que obtienen parte de sus ingresos del cobro de comisiones por la prestación del servicio de pagos a través de éste, también resultarían gravemente perjudicadas, lo cual provocaría una seria afectación al sistema financiero. Finalmente, **las personas que reciben pagos del Gobierno Federal** mismos que son dispersados por este Instituto Central en su carácter de Agente Financiero de la Tesorería de la Federación, se verían seriamente comprometidos.

Por lo anterior, un ataque perpetrado directamente al SPEI o a sus participantes, ocasionado por dar a conocer la *Información relacionada con las auditorías internas realizadas al Sistema de Pagos Electrónicos Interbancarios (SPEI),* 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 marzo de 2017 a marzo de 2018, se realizaron aproximadamente 544 millones de pagos electrónicos interbancarios por un monto de 293 billones de pesos; lo anterior equivale a más de 62 mil operaciones por un monto de 33 mil millones de pesos por hora, únicamente para lo que respecta al SPEI.[20]

Con base en estas cifras, es evidente que un ataque cibernético que vulnere la operación de este sistema 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.

---

20 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

En relación con lo anterior, es importante señalar que **México ocupa el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica**[21] 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.[22] Por lo anterior, este Instituto Central[23] y autoridades como la Secretaría de Hacienda y Crédito Público[24] se han pronunciado sobre la importancia de fortalecer la ciberseguridad para la estabilidad del sistema financiero.

Adicionalmente, **el riesgo de perjuicio que supondría la divulgación de la información materia de esta prueba de daño, supera el interés público general de que se difunda**, pues el interés público se centra en que no se comprometa la efectividad en las medidas implementadas en los sistemas financiero y económico, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto, la estabilidad en los mercados financieros y en los sistemas de pagos. Por lo que, la *Información relacionada con las auditorías internas realizadas al Sistema de Pagos Electrónicos Interbancarios (SPEI)*, no satisface un interés público, por el contrario, es información que pone en riesgo el buen funcionamiento de los sistemas de pagos y de la economía nacional en su conjunto. Asimismo al realizar una interpretación sobre la alternativa que más satisface dicho interés, se puede concluir que debe prevalecer el derecho más favorable a las personas, esto es, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste, en particular el SPEI, el cual es la infraestructura de los mercados financieros más importante del país.

En consecuencia, **proporcionar la información en cuestión, no aporta un beneficio mayor a la transparencia y rendición de cuentas que sea comparable con el perjuicio que implicaría el hecho de divulgarla,** y que en un momento dado, permita planear y perpetrar ataques cibernéticos dirigidos específicamente al SPEI y a otras infraestructuras relacionada con éste, los cuales tengan como resultado la creación de mecanismos que faciliten el acceso indebido, la substracción de información, como datos personales referente a sus usuarios y las operaciones que realizan, la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción en éstos. En este sentido, el riesgo de perjuicio antes señalado supera claramente el interés general de que se difunda la información.

---

21 Arreola Javier. "Ciberseguridad (casi) a prueba del enemigo 'invisible'". Forbes México. http://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/ consultado el 11 de octubre de 2017.

22 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 9 de octubre de 2017.

23 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

24 Secretaría de Hacienda y Crédito Público. "Comunicado No. 212. Clave Para El Desarrollo De México, Fortalecer La Ciberseguridad: Meade Kuribreña." Gob.mx, 23 Oct. 2017, www.gob.mx/shcp/es/prensa/comunicado-no-212-clave-para-el-desarrollo-de-mexico-fortalecer-la-ciberseguridad-meade-kuribrena?idiom=es consultado el 23 de noviembre de 2017.

Por otra parte, la limitación se adecua al principio de proporcionalidad, toda vez que debe prevalecer el interés que más beneficie a la colectividad, y como se ha dicho, proteger la ***Información relacionada con las auditorías internas realizadas al Sistema de Pagos Electrónicos Interbancarios (SPEI)*** evitará poner en riesgo el buen funcionamiento de los sistemas de pagos, del sistema financiero y de la economía nacional en su conjunto.

Asimismo, **reservar la información en cuestión representa el medio menos restrictivo disponible para evitar el perjuicio**, en aras salvaguardar el buen funcionamiento de los sistemas de pagos, así como la estabilidad del sistema financiero, **puesto que el propio legislador determinó que el medio menos restrictivo es la clasificación de la información cuando actualice las causales 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, segundo párrafo, 104, 105, 106, fracción III, 107, 108, último párrafo, 109, 113, fracciones IV, y 114 de la LGTAIP; 110, fracciones IV, y 111 de la LFTAIP, 1o., 2o. y 3o., fracción I, de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, y tercero, 10, párrafo primero, 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, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I, II y IV, de los Lineamientos, **se clasifica como reservada la *Información relacionada con las auditorías internas realizadas al Sistema de Pagos Electrónicos Interbancarios (SPEI)* 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 informática, con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de tecnologías de la información y comunicaciones, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques informáticos, no solo de las 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.

BANCO DE MÉXICO

REFERENCIA 1

United States Government Accountability Office

GAO

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

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

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

David A. Powner, Director
Information Technology Management Issues

GAO

Accountability * Integrity * Reliability

GAO-10-230T

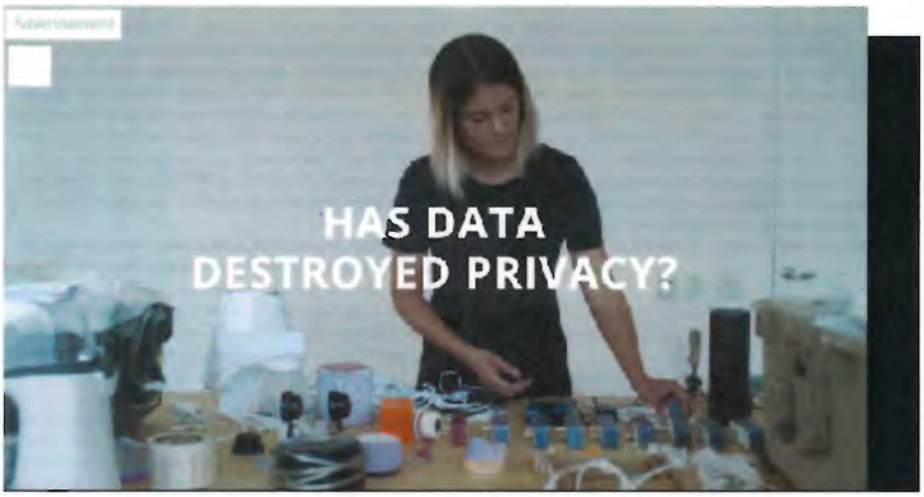
REFERENCIA 2

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.

REFERENCIA 3

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.

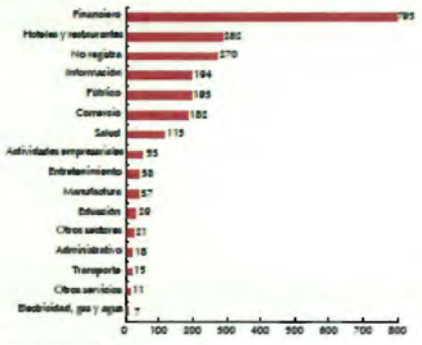
La forma más común como se ha materializado el riesgo cibernético en años recientes ha sido mediante lo que se conoce como ataques cibernéticos. En esencia, estos son acciones ilegales realizadas por *hackers*, con el objetivo principal de obtener cierto beneficio, al generar daños en los sistemas tecnológicos 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 *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.

REFERENCIA 4

18 May, 2017

banking technology

tec reveals more hack attempts on Swift network

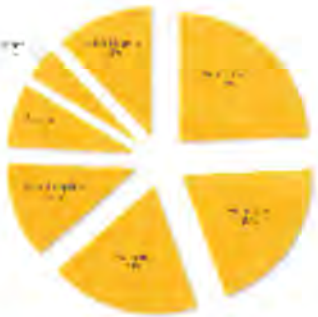
banking techno, 2016 Written by Antony Peyton

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.

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 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.



Odinaff attacks by region (IMAGE: Symantec) Click to enlarge

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 on the subject and recently unveiled SwiftSmart 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 launched in May 2016. That five-part plan was a result of various hacking incidents.

It's not just Swift

Symantec says that since January 2016, discreet campaigns involving malware called Trojan.Odinaff have targeted a number of financial organisations worldwide. These attacks appear to be "extremely focused" on organisations operating in the banking, securities, trading and payroll sectors. Organisations who provide support services to these industries are "also of interest".

REFERENCIA 5

Advanced Social Engineering Attacks*

Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl
SBA Research, Favoritenstraße 16, AT-1040 Vienna, Austria

Abstract

Social engineering has emerged as a serious threat in virtual communities and is an effective means to attack information systems. The services used by today's knowledge workers prepare the ground for sophisticated social engineering attacks. The growing trend towards *BYOD* (bring your own device) policies and the use of online communication and collaboration tools in private and business environments aggravate the problem. In globally acting companies, teams are no longer geographically co-located, but staffed just-in-time. The decrease in personal interaction combined with a plethora of tools used for communication (e-mail, IM, Skype, Dropbox, LinkedIn, Lync, etc.) create new attack vectors for social engineering attacks. Recent attacks on companies such as the New York Times and RSA have shown that targeted spear-phishing attacks are an effective, evolutionary step of social engineering attacks. Combined with zero-day-exploits, they become a dangerous weapon that is often used by advanced persistent threats. This paper provides a taxonomy of well-known social engineering attacks as well as a comprehensive overview of advanced social engineering attacks on the knowledge worker.

Keywords: security, privacy, social engineering, attack scenarios, knowledge worker, bring your own device

1. Introduction

The Internet has become the largest communication and information exchange medium. In our everyday life, communication has become distributed over a variety of online communication channels. In addition to e-mail and IM communication, Web 2.0 services such as Twitter, Facebook, and other social networking sites have become a part of our daily routine in private and business communication. Companies expect their employees to be highly mobile and flexible concerning their workspace [10] and there is an increasing trend towards expecting employees and knowledge workers to use their own devices for work, both in the office and elsewhere. This increase in flexibility and, conversely, reduction in face-to-face communication and shared office space means that increasing amounts of data need to be made available to co-workers through online channels. The development of decentralized data access and cloud services has brought about a paradigm shift in file sharing as well as communication, which today is mostly conducted over a third party, be it a social network or any other type of platform. In this world of ubiquitous communication, people freely publish information in online communication and collaboration tools, such as cloud services and social networks, with very little thought of security and privacy. They share highly sensitive documents and information in cloud services with other virtual users around the globe. Most of the time, users consider their interaction partners as trusted, even though the only identification is an e-mail address or a virtual profile. In recent years, security vulnerabilities in online communication and data sharing channels have often been misused to leak sensitive information. Such vulnerabilities can be fixed and the security of the channels can be strengthened. However, even security-enhancing methods are powerless when users are manipulated by social engineers. The term *knowledge worker* was coined by Peter Drucker more than 50 years ago and still describes the basic characteristics of a worker whose main capital is knowledge [17]. The most powerful tool an attacker can use to access this knowledge is *Social Engineering*: manipulating a person into giving information to the social engineer. It is superior to most other forms of hacking in that it can breach even the most secure systems, as the users themselves are the most vulnerable part of the system. Research has shown that social engineering is easy to automate in many cases and can therefore be performed on a large scale. Social engineering has become an emerging threat in virtual communities. Multinational corporations and news agencies have fallen victim to sophisticated targeted attacks on their information systems. Google's internal system was compromised in 2009 [2], the RSA security token system was broken in 2011 [1], Facebook was compromised in 2013 [4], as was the New York Times [40]. Many *PayPal* costumers have received phishing e-mails [45] and many have given the attackers private information such as credit card numbers. These recent attacks on high-value assets are commonly referred to as

*This paper is an extended version of the conference paper [31]

Order Code RL32331

CRS Report for Congress

The Economic Impact of Cyber-Attacks

April 1, 2004

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

REFERENCIA 7

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 8

BAE SYSTEMS THREAT RESEARCH BLOG

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


WANACRYPTOR RANSOMWORM


CYBER HEIST ATTRIBUTION

CONTACT

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

REFERENCIA 9

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 10

GIZMODO CIENCIA PELÍCULAS VIDEOJUEGOS SMARTPHONES ESPACIO

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.

REFERENCIA 11

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

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

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

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

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

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

Teléfono de Comunicación Social: 15551024

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

REFERENCIA 12

NENA (/)

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

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.

REFERENCIA 13

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**.

REFERENCIA 14

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

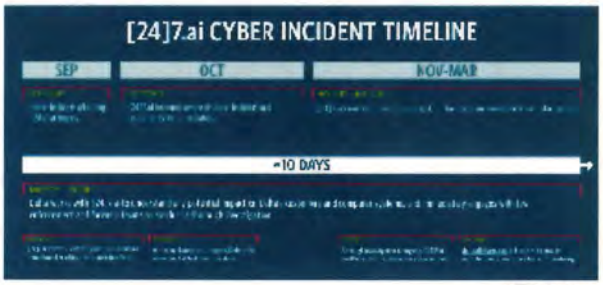
OVERVIEW

Last updated on April 7, 2018 8:00pm 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.allclearid.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, CVV 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.

REFERENCIA 16

BANCO DE MÉXICO

REFERENCIA 17

BANCO DE MÉXICO

22 de mayo de 2018

Puntos Importantes sobre la Situación Actual del SPEI.

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

REFERENCIA 18

Social Engineering Fundamentals, Part I: Hacker Tactics

Sarah Granger 2001-12-18

Social Engineering Fundamentals, Part I: Hacker Tactics

by Sarah Granger

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.

In this case, the strangers were network consultants performing a security audit for the CFO without any other employees' knowledge. They were never given any privileged information from the CFO but were able to obtain all the access they wanted through social engineering. (This story was recounted by Kapil Raina, currently a security expert at Verisign and co-author of mCommerce Security: A Beginner's Guide, based on an actual workplace experience with a previous employer.)

Definitions

Most articles I've read on the topic of social engineering begin with some sort of definition like

BANCO DE MÉXICO

REFERENCIA 19

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 20

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real.

Fecha de consulta: 27/04/2018 11:04:05

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 - Mar 2018	Ene 1992 - Mar 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

REFERENCIA 21

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/)
May 23rd, 2016 @ 12:59 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.

Share Tweet +

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

EDO

MÁS COBERTURA

Petro-7 invertirá 700 millones de pesos en México este año (https://www.forbes.com.mx/petro-7-invertira-700-millones-pesos-mexico-este-ano/)

Muere el vocalista Chris Cornell a los 52 años de edad (https://www.forbes.com.mx/muer chris-cornell-a-los-52-anos-de-edad/)

Así busca Movistar reposicionarse ante la competencia (https://www.forbes.com.mx/asi-busca-telefonica-movistar-reposicionarse-en-mexico/)

Últimas Noticias

México lidera el sector Telecom en Latinoamérica, pero... (https://www.forbes.com.mx/mexi lidera-el-sector-telecom-en-latinoamerica-pero/)
MAYO 18, 2017

General Motors se despide de Sudáfrica (https://www.forbes.com.mx/gener motors-se-despide-sudafrica/)
MAYO 18, 2017

Éstas son las zonas más conflictivas de la Ciudad de México (https://www.forbes.com.mx/estas son-las-zonas-mas-conflictivas-de-la-ciudad-de-mexico/)
MAYO 18, 2017

REFERENCIA 22

Informe Norton sobre Ciberseguridad 2016

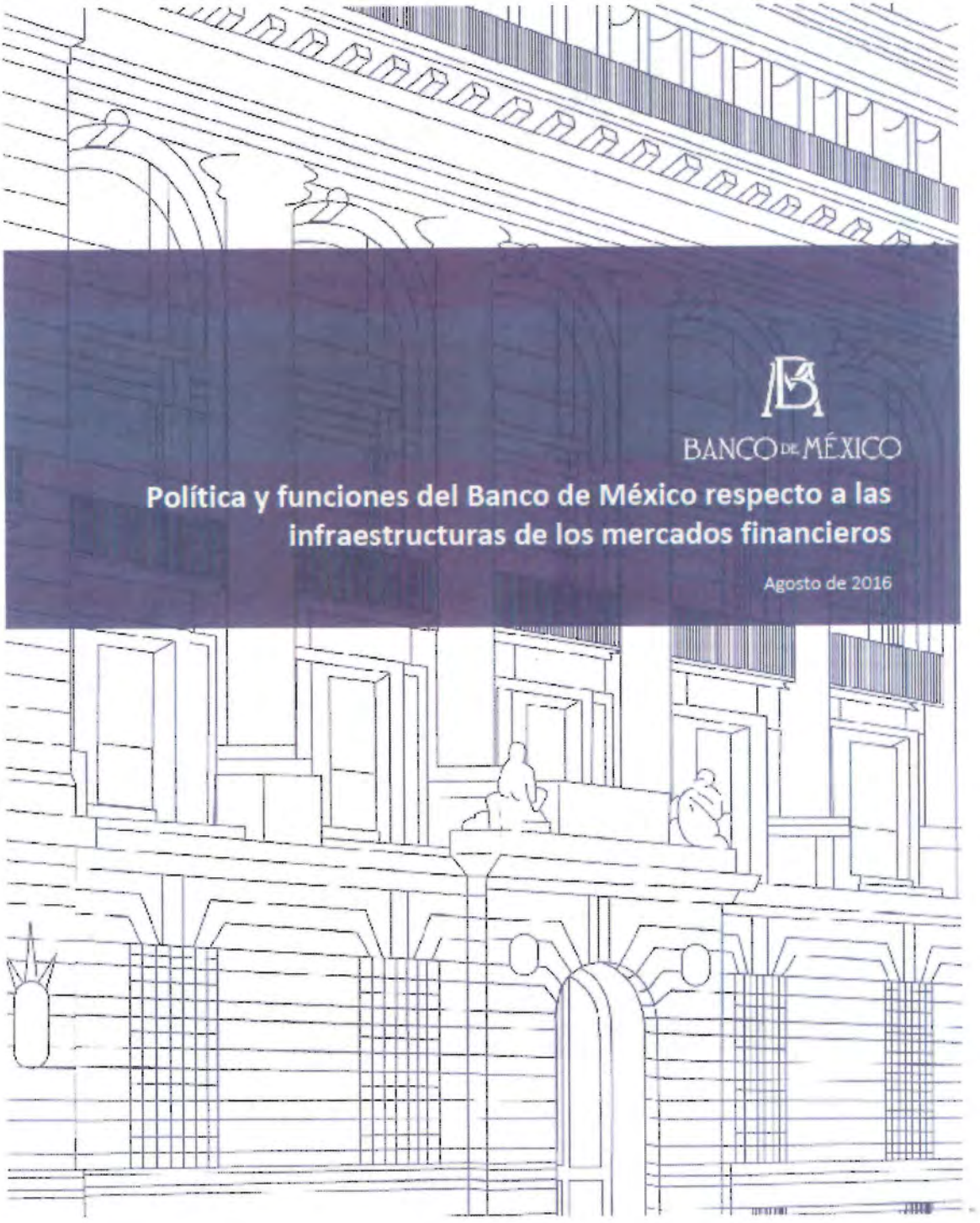
Comparaciones Globales

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 by Symantec

BANCO DE MÉXICO

REFERENCIA 23



REFERENCIA 24

Comunicado No. 212. Clave para el desarrollo de México, fortalecer la ciberseguridad: Meade Kuribreña

El secretario de Hacienda y Crédito Público llamó a generar una cultura de prevención en materia cibernética.

Inauguración del Foro Fortaleciendo la Ciberseguridad para la Estabilidad del Sistema Financiero Mexicano

Autor
Secretaría de Hacienda y Crédito Público

Fecha de publicación
23 de octubre de 2017

Categoría
Comunicado

Contesta nuestra encuesta de satisfacción

Fue testigo de honor en la firma de la Declaración de Principios para el fortalecimiento de la ciberseguridad para la estabilidad del sistema financiero mexicano

El secretario de Hacienda y Crédito Público, José Antonio Meade Kuribreña, destacó hoy la importancia de fortalecer la infraestructura cibernética, ya que la ciberseguridad es un bien público que se debe salvaguardar ante cualquier ataque.

ANEXO "O"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000029618

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

RESULTANDO

PRIMERO. El treinta de mayo de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000029618,** la cual se transcribe a continuación:

> ***Descripción:*** *"Las Recomendaciones de los reportes correspondientes a las pruebas de penetración de 5 años a la fecha del Sistema SPEI. Los resultados de los últimos 5 años de las auditorías externas e internas de la Unidad de Auditoría de BANXICO y que se mandan a realizar por medio de la misma UNIDAD a unidades externas."*
>
> ***Datos adicionales:*** *"Resultados de auditorias internas y externas a SPEI de los últimos 5 años y resultados de pruebas de penetración a SPEI de los últimos 5 años."*

SEGUNDO. El mismo treinta de mayo, la solicitud de información mencionada en el resultando anterior, fue turnada para su atención a la Dirección de Sistemas de Pagos, unidad administrativa adscrita a la Dirección General de Operaciones y Sistemas de Pagos del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. El titular de la Dirección de Sistemas de Pagos, mediante oficio con referencia D01/C363/2018, hizo del conocimiento de este Comité de Transparencia que subsisten las causas que dieron origen a la clasificación de los documentos señalados en dicho oficio, en términos de la motivación y fundamentación señaladas en la prueba de daño que en su momento pusieron a disposición de este órgano colegiado. Asimismo, señaló que dichos documentos son materia de la solicitud señalada al rubro, y solicitaron a este Comité de Transparencia confirmar la clasificación de la información.

En adición a lo anterior, mediante el oficio de mérito, hizo del conocimiento de este órgano colegiado que ha determinado clasificar como reservado el documento señalado en el segundo cuadro del oficio referido, en términos de la motivación y fundamentación señalados en la prueba de daño correspondiente, misma que acompañaron al oficio correspondiente, y solicitaron a este Comité de Transparencia 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.

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

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

Este órgano colegiado advierte que es procedente la clasificación de la información señalada como **reservada,** toda vez que se ubica en los supuestos de reserva, en términos de la fundamentación y motivación expresada en la correspondiente prueba de daño, misma que se tiene por reproducida a la letra, en obvio de repeticiones innecesarias, y además, subsisten las causas que dieron origen a tal clasificación, en el caso de los documentos ubicados en dicho supuesto.

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, señalada en el respectivo 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, 101, fracciones I y IV, 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, 99, fracciones I y IV, 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 expresada 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 veintiuno de junio de dos mil dieciocho.----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente