BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ORDINARIA 47/2019
DEL 14 DE NOVIEMBRE DE 2019

En la Ciudad de México, a las trece horas con quince minutos del catorce de noviembre de dos mil diecinueve, en el edificio ubicado en avenida Cinco de Mayo, número dieciocho, colonia Centro, demarcación territorial Cuauhtémoc, se reunieron María Teresa Muñoz Arámburu, Titular de la Unidad de Transparencia; Edgar Miguel Salas Ortega, Gerente Jurídico Consultivo, en suplencia del Director Jurídico; José Ramón Rodríguez Mancilla, Gerente de Organización de la Información, en suplencia del Director de Seguridad y Organización de la Información, así como Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, en su carácter de Secretario de este 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 (RIBM), así como la Tercera, de las Reglas de Operación del Comité de Transparencia del Banco de México, publicadas en el Diario Oficial de la Federación el dos de junio de dos mil dieciséis (Reglas), las personas que se indican en la lista de asistencia que se adjunta a la presente como **"ANEXO 1"**, quienes también son servidores públicos del Banco de México. ----------

Al estar presentes los integrantes mencionados, quien ejerce en este acto las funciones de Secretariado del Comité de Transparencia manifestó que existe quórum para la celebración de la presente sesión, de conformidad con lo previsto en los artículos 43 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 64, párrafos segundo y tercero, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); 83 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 4o. del RIBM; así como Quinta y Sexta de las Reglas. Por lo anterior, se procedió en los términos siguientes: ----------

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

Quien ejerce en este acto las funciones de Secretariado del Comité de Transparencia, sometió a consideración de los integrantes 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 43, párrafo segundo, 44, fracción IX, de la LGTAIP; 64, párrafo segundo; 65, fracción IX, de la LFTAIP; 83 de la LGPDPPSO; 4o. y 31, fracciones III y XX, del RIBM, y Quinta, de las Reglas, por unanimidad, aprobó el orden del día en los términos del documento que se adjunta a la presente como **"ANEXO 2"** 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 6110000065819. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con número de referencia D04/192/19, suscrito por el titular de la Dirección de Política y Estudios de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, el cual se agrega a la presente acta como **"ANEXO 3"**, por medio del cual solicitó a este órgano colegiado 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 11, y 132, párrafo segundo, de la LGTAIP; 1, 9, 64, 65 fracción 11, y 135, párrafo segundo, de la LFTAIP; 31, fracción 111, del RIBM, 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 4"**.----------

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE AMPLIACIÓN DEL PLAZO DE RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000072919. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio de fecha cinco de noviembre de dos mil diecinueve, suscrito por el titular de la Dirección de Política y Estudios de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, el cual se agrega a la presente acta como **"ANEXO 5"**, por medio del cual solicitó a este órgano colegiado 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 11, y 132, párrafo segundo, de la LGTAIP; 1, 9, 64, 65 fracción 11, y 135, párrafo segundo, de la LFTAIP; 31, fracción 111, del RIBM, 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 6"**.----------

TERCERO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN E INFORME DE DESCLASIFICACIÓN REALIZADOS POR EL TITULAR DE LA DIRECCIÓN DE OPERACIÓN Y CONTINUIDAD DE LOS SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, RELACIONADOS CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000065919. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con número de referencia D40/051/19, suscrito por el titular de la Dirección de Operación y Continuidad de los Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, el cual se agrega a la presente acta como **"ANEXO 7"**, por medio del cual hizo del conocimiento de este Comité de Transparencia su determinación de clasificar diversa información contenida en el documento señalado en dicho oficio, conforme a la fundamentación y motivación señaladas en la carátula y en la prueba de daño puesta a disposición de este órgano colegiado en su momento, y solicitó a este órgano colegiado confirmar dicha clasificación y aprobar la referida versión pública. Asimismo, mediante el referido oficio, hizo del conocimiento de este Comité de Transparencia su determinación de desclasificar la información que se detalla en dicho oficio, cuya clasificación fue aprobada en su momento para la atención de una solicitud diversa, en términos de lo expresado, fundado y motivado en el mismo. ----------

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, de la LGTAIP; 1, 9, 64, 65 fracción II, de la LFTAIP; 31, fracción III, del RIBM; y Quinta de las Reglas, resolvió confirmar la clasificación de la información respectiva y aprobar la versión pública correspondiente, y tomó conocimiento de la desclasificación de la información respectiva, en términos de la resolución que se agrega al apéndice de la presente acta como **"ANEXO 8"**. ----------

CUARTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE OPERACIÓN Y CONTINUIDAD DE LOS SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000065919. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con número de referencia D40/050/19, suscrito por el titular de la Dirección de Operación y Continuidad de los Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, el cual se agrega a la presente acta como **"ANEXO 9"**, por medio del cual hizo del conocimiento de este Comité de Transparencia su determinación de clasificar la información señalada en dicho oficio, de conformidad con la fundamentación y motivación señaladas en el mismo, así como en la carátula y en la prueba de daño correspondientes, y solicitó a este órgano colegiado confirmar dicha clasificación y aprobar la referida versión pública. ----------

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, de la LGTAIP; 1, 9, 64, 65 fracción II, de la LFTAIP; 31, fracción III, del RIBM; y Quinta de las Reglas, resolvió confirmar la clasificación de la información respectiva y aprobar la versión pública correspondiente, en términos de la resolución que se agrega al apéndice de la presente acta como **"ANEXO 10"**. ----------

QUINTO. SOLICITUD DE CONFIRMACIÓN DE AMPLIACIÓN DEL PLAZO DE RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000071719. ----------

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con número de referencia V01.228.2019, suscrito por el titular de la Dirección de Recursos Humanos del Banco de México, el cual se agrega a la presente acta como **"ANEXO 11"**, por medio del cual solicitó a este órgano colegiado 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 11, y 132, párrafo segundo, de la LGTAIP; 1, 9, 64, 65 fracción 11, y 135, párrafo segundo, de la LFTAIP; 31, fracción 111, del RIBM, 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 12"**. ----------

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 quien ejerce en este acto las funciones de Secretariado. Conste. ----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

SERGIO ZAMBRANO HERRERA
Secretario

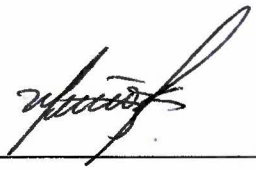
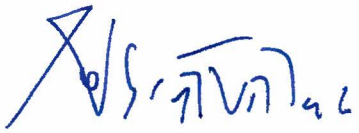
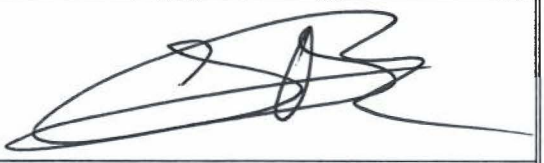
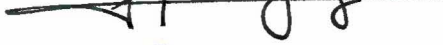
Anexo "1"

BANCO DE MÉXICO

LISTA DE ASISTENCIA
SESIÓN ORDINARIA 47/2019

14 DE NOVIEMBRE DE 2019

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU Directora de la Unidad de Transparencia	
ERIK MAURICIO SÁNCHEZ MEDINA Director Jurídico	
VICTOR MANUEL DE LA LUZ PUEBLA Director de Seguridad y Organización de la Información	
RODRIGO VILLA COLLINS Gerente de Análisis y Promoción de Transparencia	
EDGAR MIGUEL SALAS ORTEGA Gerente Jurídico Consultivo	
JOSÉ RAMÓN RODRÍGUEZ MANCILLA Gerente de Organización de la Información	
SERGIO ZAMBRANO HERRERA Subgerente de Análisis Jurídico y Promoción de Transparencia	
HECTOR GARCÍA MONDRAGÓN Jefe de Oficina de Análisis Jurídico y Promoción de Transparencia.	

BANCO DE MÉXICO

INVITADOS PERMANENTES

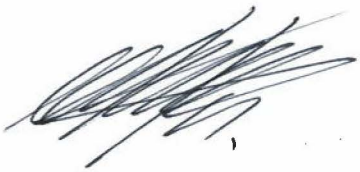
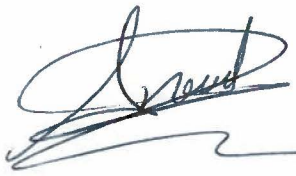
OSCAR JORGE DURÁN DÍAZ Dirección de Vinculación Institucional y Comunicación	
FRANCISCO CHAMÚ MORALES Director de Administración de Riesgos	

INVITADOS

ALAN CRUZ PICHARDO Subgerente de Apoyo Jurídico a la Transparencia	
JONATHAN NAVARRO VILLEGAS Abogado en Jefe en la Subgerencia de Apoyo Jurídico a la Transparencia	
LUIS ADOLFO CASTILLO REYEROS Abogado Especialista	
CARLOS FERNANDO ÁNGEL AMADOR Abogado	

RODRIGO MÉNDEZ PRECIADO Gerente de Enlace Institucional y Relaciones Públicas	
MARGARITA LISSETE PONCE GUARNEROS Gerente de Riesgos No Financieros	
CARLOS ALBERTO ARIAS VÁZQUEZ Subgerente de Seguimiento de Riesgos y Continuidad Operativa.	
MARTHA MARISOL CAPILLA GUTIÉRREZ Subgerente de Identificación y Evaluación de Riesgos Operativos.	
OTHON MARTINO MORENO GONZÁLEZ Director de Política y Estudios de Sistemas de Pagos e Infraestructuras de Mercados	
ÁNGEL MELESIO FUENTES Director de Operación y Continuidad de los Sistemas de Pagos e Infraestructura de Mercados	
XIMENA AIDEE DOMÍNGUEZ HERNÁNDEZ Jefa de la Oficina de Atención de Temas de Transparencia	

BANCO DE MÉXICO

EDSEL ALEJANDRO CARMONA SANABRIA Analista de Información	
JUN RODRIGO HINOKI ALCARAZ Director de Recursos Humanos	
ALEJANDRO DE LA PEÑA MONTOYA Subgerente de Gestión de Remuneraciones y Prestaciones	
ANAID PALACIOS HERNÁNDEZ Analista de Información	
BERNARDO VELASCO CORRAL Jefe de la Oficina de Análisis de Recursos Humanos	
VÍCTOR MANUEL MARTÍNEZ PÁEZ Especialista en Proyectos de Recursos Humanos	
VIRIDIANA IVONNE YUNES VALLE Estudios y Proyectos especiales	

BANCO DE MÉXICO

GUILLERMO ALBERTO MEDINA TOLENTINO Analista de Información	
MIGUEL DORAS FUENTES Analista de Información	
ADRIANA CAL Y MAYOR MOGUEL Analista de Información	
GERARDO VÁZQUEZ GRAJALES LÍDER DE ESPECIALIDAD DGCOR/DSR/GANF	
César Arturo Ortega Arias Subgerente de Continuidad y Gestión de los Sistemas de Pago	
Luis Lima Gómez Gerente de Continuidad y Control de Sistemas de Pagos e Infraestructuras de Mercado	

Anexo "2"

BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ORDEN DEL DÍA

Sesión Ordinaria 47/2019
14 de noviembre de 2019

PRIMERO. SOLICITUD DE CONFIRMACIÓN DE AMPLIACIÓN DEL PLAZO DE RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000065819.

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE AMPLIACIÓN DEL PLAZO DE RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000072919.

TERCERO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN E INFORME DE DESCLASIFICACIÓN REALIZADOS POR EL TITULAR DE LA DIRECCIÓN DE OPERACIÓN Y CONTINUIDAD DE LOS SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, RELACIONADOS CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000065919.

CUARTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE OPERACIÓN Y CONTINUIDAD DE LOS SISTEMAS DE PAGOS E INFRAESTRUCTURAS DE MERCADOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000065919.

QUINTO. SOLICITUD DE CONFIRMACIÓN DE AMPLIACIÓN DEL PLAZO DE RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000071719.

Anexo "3"

MÉXICO
RECIBIDO
2019
Comité de Transparencia
Por: JIS Hora: 14:38

Se recibe oficio constante en una página.

BANCO DE MÉXICO

ACUSE

Ciudad de México, a 8 de noviembre de 2019
D04/192/2019

COMITÉ DE TRANSPARENCIA
DEL BANCO DE MÉXICO
Presente

Me refiero a la solicitud de acceso a la información, identificada con el número de folio **6110000065819,** que nos turnó la Unidad de Transparencia el nueve de octubre del presente año, a través del sistema electrónico de atención a solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, que se transcribe a continuación:

> *"Expediente técnico mediante el cual el Banco de México otorgó la autorización para la organización y operación de una Cámara de Compensación para Pagos con Tarjetas a la empresa Promoción y Operación, SA de CV."*

Sobre el particular, solicitamos a ese Órgano Colegiado aprobar la ampliación del plazo de respuesta a la solicitud de acceso indicada en el párrafo anterior, toda vez que la información que se solicita, aún se encuentra en un proceso de revisión de diversas áreas, por lo que su atención supera los tiempos establecidos por la ley.

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 en todo momento el requerimiento de acceso a la información del particular, en aras de proporcionar la información de la forma más completa posible.

Por lo anterior, solicitó con fundamento en los artículos 132, segundo párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; 135, segundo párrafo, de la Ley Federal de Transparencia y Acceso a la Información Pública; y, Vigésimo Octavo de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública"; se apruebe la ampliación del tiempo de respuesta por los motivos y fundamentos anteriormente expuestos.

Sin otro particular, quedo a sus órdenes para cualquier aclaración al respecto.

Atentamente,

Othón Martino Moreno González
Director de Política y Estudios de Sistemas de Pagos
e Infraestructuras de Mercados

Anexo "4"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DE PLAZO
FOLIO: 6110000065819

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

RESULTANDO

PRIMERO. Que el nueve de octubre de dos mil diecinueve, la Unidad de Transparencia del Banco de México recibió la solicitud con folio citada al rubro, la cual se transcribe a continuación:

> *"Expediente técnico mediante el cual el Banco de México otorgó la autorización para la organización y operación de una Cámara de Compensación para Pagos con Tarjetas a la empresa Promoción y Operación, SA de CV."*

SEGUNDO. Que el diez de octubre del mismo año, la referida solicitud fue turnada a la Dirección General de Sistemas de Pagos e Infraestructuras de Mercados y a la Dirección de Autorizaciones y Sanciones de Banca Central, ambas del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información, previsto para esos efectos.

TERCERO. Que el dieciséis de octubre del año en curso, la Unidad de Transparencia requirió al solicitante, a efecto de que precisara la siguiente:

> *"... a que se refiere con -Expediente técnico mediante el cual el Banco de México otorgó la autorización para la organización y operación de una Cámara de Compensación para Pagos con Tarjetas a la empresa Promoción y Operación, SA de CV-."*

CUARTO. Que el treinta de octubre de dos mil diecinueve, el solicitante desahogó el requerimiento e información adicional, en los siguientes términos:

> *"Ciudad de México, a 30 de octubre de 2019.*
> ***Unidad de Transparencia del Banco de México:***
> *En respuesta a su escrito fechado el 16 de octubre de 2019, en el que me solicitan que aclare a qué me refiero con «expediente técnico mediante el cual el Banco de México otorgó la autorización para la organización y operación de una Cámara de Compensación para Pagos con Tarjetas a la empresa Promoción y Operación, SA de CV», les informo lo siguiente:*
> *En un oficio del Banco de México publicado en el Diario Oficial de la Federación el día 7 de octubre de 2014, bajo el encabezado «Autorización dirigida a Promoción y Operación, S.A. de C.V. (PROSA), para la organización y operación de una Cámara de Compensación para Pagos con Tarjetas», el Banco Central informa a la persona moral referida lo siguiente:*
> *«i) Que la documentación presentada por Promoción y Operación, S.A. de C.V., con motivo de su solicitud, cumple satisfactoriamente con los requisitos previstos en los artículos 19 y 19 Bis de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, así como en las "Reglas para la Organización, Funcionamiento y Operación de Cámaras de Compensación para Pagos con Tarjetas" contenidas en nuestra Circular 4/2014, publicada en el Diario Oficial de la Federación el 11 de marzo de 2014.*
> *«ii) Que Promoción y Operación, S.A. de C.V., cumplió satisfactoriamente con los requisitos solicitados por este Instituto Central mediante la visita efectuada en sus instalaciones los días 25 y 26 de agosto de 2014, con la finalidad de verificar que sus operaciones, registros y sistemas cumplían adecuadamente con el marco normativo aplicable a las cámaras de compensación para pagos con tarjetas.*

«iii) Que, del análisis de la información recibida, se concluyó que, desde el punto de vista legal, financiero y operativo es procedente que se otorgue la autorización solicitada por Promoción y Operación, S.A. de C.V.»

Asimismo, la 3ª de las Reglas aplicables a las cámaras de compensación para pagos con tarjetas, emitidas por el Banco de México, señalan que:

«Una vez que la solicitud a que se refiere la 2a. de las presentes Reglas reúna la documentación e información a que se refiere dicha Regla, el Banco de México analizará si, con base en esa documentación e información, resulta procedente otorgar la autorización al promovente de que se trate para actuar como Cámara de Compensación para Pagos con Tarjetas y deberá informar su decisión al solicitante en un plazo no mayor a noventa días naturales.»

Por último, la Ley para la transparencia y el ordenamiento de los servicios financieros, en su artículo 19 bis, señala que:

«Para organizarse y operar como Cámara de Compensación se requerirá autorización que corresponderá otorgar al Banco de México.

«Para tales efectos la interesada deberá presentar la información y documentación que dicho Banco Central señale a través de disposiciones de carácter general.»

Así pues,

1. El Banco de México está facultado para otorgar autorizaciones para operar como cámara de compensación para pagos con tarjeta.

2. Los interesados en obtener una autorización de este tipo deben presentar información y documentación que el Banco de México «señale a través de disposiciones de carácter general».

3. Según el oficio publicado en el Diario Oficial de la Federación en 7 de octubre de 2014, el Banco de México recibió documentación presentada por Promoción y Operación, SA de CV. Asimismo, efectuó una visita en las instalaciones de Promoción y Operación, SA de CV los días 25 y 26 de agosto de 2014, «con la finalidad de verificar que sus operaciones, registros y sistemas cumplían adecuadamente con el marco normativo aplicable a las cámaras de compensación para pagos con tarjetas». A partir de la documentación recibida, la información recabada y la verificación de sus operaciones, registros y sistemas, el Banco de México otorgó la autorización para la organización y operación de una cámara de compensación para pagos con tarjetas a Promoción y Operación, SA de CV (Prosa).

4. Es de suponer que el Banco de México cuenta con un archivo, expediente, expediente técnico, carpeta, dossier, registro detallado o conjunto de documentos que contienen la información a partir de la cual fue posible analizar la solicitud de Promoción y Operación, SA de CV y otorgar la autorización correspondiente.

5. Mi solicitud de información al Banco de México se refiere al archivo, expediente, expediente técnico, carpeta, dossier, registro detallado o conjunto de documentos (según el nombre por el cual el Banco de México los identifique), que constituyen el ***soporte documental*** *bajo el cual el Banco de México otorgó la autorización a Promoción y Operación, SA de CV para la organización y operación de una cámara de compensación para pagos con tarjetas."*

QUINTO. Que el titular de la Dirección de Política y Estudios de los Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, unidad administrativa adscrita a la referida Dirección General de Sistemas de Pagos e Infraestructuras de Mercados, mediante oficio con referencia D04/192/2019, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

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 (LGTAIP); 65, fracción II, y 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); 31, fracción III, del Reglamento Interior del Banco de México (RIBM), y Vigésimo octavo de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública" (Lineamientos), vigentes, 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 Quinto de la presente determinación, la unidad administrativa referida en dicho resultando, expuso las razones para ampliar el plazo de respuesta a la solicitud de acceso citada al rubro, las cuales se tienen aquí por reproducidas como si a la letra se insertasen, en obvio de repeticiones innecesarias.

TERCERO. Que de conformidad con los artículos 44, fracción II y 132, párrafo segundo de la LGTAIP; 65, fracción II y 135 de la LFTAIP; y Vigésimo Octavo de los Lineamientos, es necesario que dada la naturaleza y complejidad de la información solicitada, el área competente realice una verificación exhaustiva 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 la unidad administrativa mencionada, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 132, párrafo segundo, de la LGTAIP; 1, 9, 64, 65, fracción II, y 135, párrafo segundo, de la LFTAIP; 31, fracción III, del RIBM, y Vigésimo octavo de los Lineamientos, 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 citada al rubro, en términos de lo expuesto en el considerando 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 catorce de noviembre de dos mil diecinueve.----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

Anexo "5"

BANCO DE MÉXICO

BANCO DE MÉXICO
RECIBIDO
06 NOV 2019
Comité de Transparencia
Por: JIS383 Hora: 14:57

se recibe oficio constante en una página.

Ciudad de México, a 05 de noviembre de 2019

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 **6110000072919,** que nos turnó la Unidad de Transparencia el veintitrés de octubre del presente año, a través del sistema electrónico de atención a solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, que se transcribe a continuación:

> *"Solicito toda la información respecto a la plataforma CoDi, desarrollada por el Banco de México. Especialmente requiero los documentos que den cuenta del proceso de propuesta, creación, aplicación e implementación de la plataforma CoDi, como son Documentos sobre la planeación del proyecto de la plataforma (documentos, resúmenes ejecutivos, informes técnicos entre otros).Expresión documental sobre el personal que propuso, desarrolló, implementó y da mantenimiento a la plataforma CoDi. Los documentos que den cuenta de las certificaciones que tienen el personal antes referido. Los permisos, concesiones y toda expresión documental que contenga la información relativa de la aprobación de las autoridades correspondientes para la creación e implementación la plataforma CoDi .De existir, la información sobre los Estudios de Impacto Económico, Jurídico y Social realizados para llevados a cabo para la creación de esta plataforma."*

Sobre el particular, solicitamos a ese Órgano Colegiado aprobar la ampliación del plazo de respuesta a la solicitud de acceso indicada en el párrafo anterior, toda vez que dada la naturaleza y la complejidad de la misma, se está obteniendo y verificando la información que posee esta unidad administrativa, por lo que su atención supera los tiempos establecidos por la ley.

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 en todo momento el requerimiento de acceso a la información del particular, en aras de proporcionar la información de la forma más completa posible.

Por lo anterior, solicitó con fundamento en los artículos 132, segundo párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; 135, segundo párrafo, de la Ley Federal de Transparencia y Acceso a la Información Pública; y, Vigésimo Octavo de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública"; se apruebe la ampliación del tiempo de respuesta por los motivos y fundamentos anteriormente expuestos.

Sin otro particular, quedo a sus órdenes para cualquier aclaración al respecto.

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

Othón Martino Moreno González
Director de Política y Estudios de Sistemas de Pagos
e Infraestructuras de Mercados

Anexo "6"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DE PLAZO
FOLIO: 6110000072919

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

RESULTANDO

PRIMERO. Que el veintitrés de octubre de dos mil diecinueve, la Unidad de Transparencia del Banco de México recibió la solicitud con folio citada al rubro, la cual se transcribe a continuación:

> *"Solicito toda la información respecto a la plataforma CoDi, desarrollada por el Banco de México. Especialmente requiero los documentos que den cuenta del proceso de propuesta, creación, aplicación e implementación de la plataforma CoDi, como son*
> *Documentos sobre la planeación del proyecto de la plataforma (documentos, resumenes ejecutivos, informes técnicos entre otros).*
> *Expresión documental sobre el personal que propuso, desarrolló, implementó y da mantenimiento a la plataforma CoDi.*
> *Los documentos que den cuenta de las certificaciones que tienen el personal antes referido.*
> *Los permisos, concesiones y toda expresión documental que contenga la información relativa de la aprobación de las autoridades correspondientes para la creación e implementación la plataforma CoDi.*
> *De existir, la información sobre los Estudios de Impacto Económico, Jurídico y Social realizados para llevados a cabo para la creación de esta plataforma."*

SEGUNDO. Que el mismo veintitrés de octubre del año en curso, la referida solicitud fue turnada a la Dirección General de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información, previsto para esos efectos.

TERCERO. Que el titular de la Dirección de Política y Estudios de los Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, unidad administrativa adscrita a la referida Dirección General de Sistemas de Pagos e Infraestructuras de Mercados, mediante oficio con fecha de cinco de noviembre de dos mil diecinueve, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

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 (LGTAIP); 65, fracción II, y 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); 31, fracción III, del Reglamento Interior del Banco de México (RIBM), y Vigésimo octavo de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública" (Lineamientos), vigentes, 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 Tercero de la presente determinación, el titular de la Dirección de Política y Estudios de los Sistemas de Pagos e Infraestructuras de Mercados, expuso las razones

para ampliar el plazo de respuesta a la solicitud de acceso citada al rubro, las cuales se tienen aquí por reproducidas como si a la letra se insertasen, en obvio de repeticiones innecesarias.

TERCERO. Que de conformidad con los artículos 44, fracción II y 132, párrafo segundo de la LGTAIP; 65, fracción II y 135 de la LFTAIP; y Vigésimo Octavo de los Lineamientos, es necesario que dada la naturaleza y complejidad de la información solicitada, el área competente realice una verificación exhaustiva 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 la unidad administrativa mencionada, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 132, párrafo segundo, de la LGTAIP; 1, 9, 64, 65, fracción II, y 135, párrafo segundo, de la LFTAIP; 31, fracción III, del RIBM, y Vigésimo octavo de los Lineamientos, 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 citada al rubro, en términos de lo expuesto en el considerando 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 catorce de noviembre de dos mil diecinueve. ----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

Anexo "7"

BANCO DE MÉXICO
RECIBIDO
12 NOV 2019
Comité de Transparencia
Por: 715383 Hora: 12:00

Se recibe oficio constante en tres páginas y una carátula.

BANCO DE MÉXICO

Ciudad de México, a 8 de noviembre de 2019

D40/051/19

COMITÉ DE TRANSPARENCIA
DEL BANCO DE MÉXICO
Presente.

Nos referimos a la solicitud de acceso a la información, identificada con el número de folio **6110000065919**, que nos turnó la Unidad de Transparencia el nueve de octubre de 2019 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:

> *"Expediente técnico mediante el cual el Banco de México otorgó la autorización como Participante del Sistema de Pagos Electrónicos Interbancarios a la empresa Sistema de Transferencias y Pagos STP, SA de CV, Sofom, ENR."*

Sobre el particular, mediante oficio con fecha de 9 de febrero de 2017, se informó a ese Comité de Transparencia la determinación de clasificar como confidencial diversa información contenida en el documento *CONTRATO QUE DOCUMENTA LA PRESTACIÓN DE LOS SERVICIOS DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS QUE CELEBRAN POR UNA PARTE BANCO DE MÉXICO Y POR LA OTRA, SISTEMA DE TRANSFERENCIAS Y PAGOS STP, S.A. DE C.V., E.N.R.*, en los términos de la fundamentación y motivación expresados en el oficio y en la carátula respectiva; y diversa información como reservada, por el plazo de 5 años, en los términos de la fundamentación y motivación expresados en la carátula, y en la prueba de daño contenida en el cuerpo del referido oficio.

Lo anterior, con motivo de la atención de una solicitud de acceso a la información diversa. Dicha clasificación fue confirmada por ese Comité de Transparencia, mediante la resolución emitida en su Sesión Ordinaria de quince de febrero del año dos mil diecisiete. La información que fue clasificada es la que se señala en el siguiente cuadro:

TÍTULO DEL DOCUMENTO CLASIFICADO	CLASIFICACIÓN REALIZADA	INFORMACIÓN CLASIFICADA	PLAZO DE RESERVA
CONTRATO QUE DOCUMENTA LA PRESTACIÓN DE LOS SERVICIOS DEL	Confidencial	• Rúbricas de particulares personas físicas. • Nombre de Personas físicas.	N/A

SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS QUE CELEBRAN POR UNA PARTE BANCO DE MÉXICO Y POR LA OTRA, SISTEMA DE TRANSFERENCIAS Y PAGOS STP, S.A. DE C.V., E.N.R.		• Firmas autógrafas de personas físicas. • Nombres de las personas físicas designadas como operadores. • Certificados Digitales de los operadores.	
	Reservada	• Información relacionada con las especificaciones técnicas de la infraestructura de telecomunicaciones de la Red Financiera y las cuotas correspondientes a dicha estructura. • Información relacionada con los niveles de operación de los operadores. • Información relacionada con los niveles de operación en el Sistema de Pagos Electrónicos Interbancarios (SPEI)	• 15/02/2022

Al respecto, me permito manifestar a ese Comité de Transparencia que a raíz de una nueva reflexión realizada con motivo de la atención de la solicitud de acceso a la información materia del presente, se ha identificado que, al momento, no se actualizan las causas para mantener clasificada con el carácter de confidencial la informacion señalada como *"Rúbricas de particulares personas físicas, Nombre de Personas físicas y Firmas autógrafas de personas físicas"*, subsistiendo la clasificación de la información referida como *"Nombres de las personas físicas designadas como operadores, Certificados Digitales de los operadores"*, en los terminos de la fundamentación y motivación señalados en la caratula que se adjunta al presente. Respecto de la información clasificada como reservada, dicha clasificación subsiste en términos de la fundamentación y motivación expresados en la carátula que se adjunta al presente, y en la prueba de daño contenida en el referido oficio con fecha de 9 de febrero de 2017, que en su momento se puso a disposición de ese órgano colegiado.

BANCO DE MÉXICO

En consecuencia, de conformidad con lo dispuesto por los artículos 44, fracción II y 101, fracciones I y IV, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II y 99, fracciones I y IV, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México; así como el Quincuagésimo sexto, y Sexagésimo segundo de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, informo a ese Comité de Transparencia la desclasificación de la información referida, y solicito confirmar la clasificación de la información realizada, y aprobar la versión pública adjunta al presente.

Atentamente,

Ángel Melesio Fuentes
Director de Operación y Continuidad de los Sistemas de Pagos
e Infraestructura de Mercados

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 100, 106, fracción I, 109 y 111 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97, 98, fracción I, 106, 108 y 118 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción I, Quincuagésimo sexto y Sexagésimo segundo de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Lineamientos).

VERSIÓN PÚBLICA	
I. Área titular que clasifica la información	Dirección de Operación y Continuidad de los Sistemas de Pagos e Infraestructuras de los Mercados.
II. Identificación del documento del que se elabora la versión pública.	CONTRATO QUE DOCUMENTA LA PRESTACIÓN DE LOS SERVICIOS DEL SISTEMA DE PAGOS ELECTRÓNICOS INTERBANCARIOS QUE CELEBRAN POR UNA PARTE BANCO DE MÉXICO Y POR LA OTRA, SISTEMA DE TRANSFERENCIAS Y PAGOS STP, S.A. DE C.V. SOFOM, E.N.R.
III. Firma del titular del área y de quien clasifica.	**Ángel Melesio Fuentes** Director de Operación y Continuidad de los Sistemas de Pagos e Infraestructuras de Mercados
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia "ORDINARIA", número 47/2019, celebrada el 11 de NOVIEMBRE de 2019 Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México. Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México

BANCO DE MÉXICO

A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación y, en los supuestos de información clasificada como reservada, el periodo de reserva:

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Pág.**	**Información testada**	**Fundamento Legal**	**Motivación**
1	11 a 14	Nombre de Personas físicas designadas como operadores.	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracción IX, 6, 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que el nombre es la manifestación principal del derecho subjetivo a la identidad, hace que una persona física sea identificada o identificable, y consecuentemente es un dato personal. En efecto, el nombre de una persona física además de ser un atributo de la personalidad que por esencia sirve para distinguir y determinar a las personas en cuanto a su identidad, es el conjunto de signos que constituyen un elemento básico e indispensable de la identidad de cada persona sin el cual no puede ser reconocida por la sociedad, así como un derecho humano que protege el nombre propio y los apellidos. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible conocer información personal de su titular.
2	11 a 14	Certificados Digitales de los operadores.	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos; 7, 23,	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable.

			68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, 3, fracción IX, XIII, XXVIII, XXXI y XXXIII, 4, 16, 17, 18, párrafo primero, y 22, fracción IX de LGPDPPSO; 1, 6, 68, primer párrafo, 113, fracción I, de la LFTAIP; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas."	En efecto, los certificados digitales de los operadores se encuentran asignados a personas determinadas y está conformada y es posible identificar a estas últimas, a través de la herramienta de acceso público del Banco de México denominada "Web Sec", ya que la finalidad de dicho instrumento tecnológico de información es precisamente la identificación de personas a través de su certificado digital. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular. Adicionalmente a lo anterior, cabe señalar que de conformidad con los fundamentos expuestos, se considera como dato personal, entre otra, cualquier información concerniente a una persona física determinada o determinable, es decir, cuando su identidad pueda conocerse de manera directa o indirecta a través de cualquier información, respectivamente. En el caso que nos ocupa, el documento cuya versión pública se sustenta con la presente carátula los certificados digitales de los operadores del sistema, cuya revelación permitiría fácilmente la determinación la identidad de la persona física cuyos datos personales se pretenden proteger.

				En ese sentido, de conformidad con los fundamentos planteados, es necesario realizar una disociación de los datos personales a fin de que no puedan asociarse al titular ni permitir la identificación del mismo, lo cual se logra con el testado del certificado digital. Lo anterior, en razón de que para la publicación de la información testada no se cuenta con el consentimiento del titular de los datos personales clasificados para tratarlos en su modalidad de divulgación a un tercero. En consecuencia, debe prevalecer en este caso la protección de los datos personales de la persona cuya identidad se busca proteger a través de la elaboración de la versión pública que nos ocupa.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: cinco años				
Ref.	**Pág.**	**Información testada**	**Fundamento Legal**	**Motivación**
R1	10	Información relacionada con las especificaciones técnicas de la infraestructura de telecomunicaciones de la Red Financiera[1] y las cuotas correspondientes a dicha infraestructura.	Conforme a la prueba de daño adjunta.	Conforme a la prueba de daño adjunta.

[1] A la red de información financiera compuesta por infraestructura de cómputo, software y telecomunicaciones operada, mantenida y actualizada por el Banco de México, a través de la cual se brindan diversos servicios a instituciones públicas y privadas del sistema financiero mexicano para dar cumplimiento a las finalidades y funciones previstas en los artículos 2 y 3, fracciones III y IV de la Ley del Banco de México. El software incluye aquellos aplicativos necesarios para generar, procesar y transmitir la información financiera a que se refiere la red.

R2	11 a 14	Información relacionada con los niveles de operación de los operadores.	Conforme a la prueba de daño adjunta.	Conforme a la prueba de daño adjunta.
R3	11 a 14	Información relacionada con los niveles de operación en el Sistema de Pagos Electrónicos Interbancarios (SPEI).	Conforme a la prueba de daño adjunta.	Conforme a la prueba de daño adjunta.

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

DESCLASIFICACIÓN Y CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000065919
Unidad administrativa: Dirección de Operación y Continuidad de los Sistemas de Pagos e Infraestructura de Mercados del Banco de México.

VISTOS, para resolver sobre la desclasificación y la clasificación de información manifestada por la unidad administrativa al rubro citada; y

RESULTANDO

PRIMERO. Que el nueve de octubre de dos mil diecinueve, la Unidad de Transparencia del Banco de México recibió la solicitud con folio citado al rubro, la cual en su parte conducente refiere lo siguiente:

> *"Expediente técnico mediante el cual el Banco de México otorgó la autorización como Participante del Sistema de Pagos Electrónicos Interbancarios a la empresa Sistema de Transferencias y Pagos STP, SA de CV, Sofom, ENR."*

SEGUNDO. Que el mismo nueve de octubre de dos mil diecinueve, la referida solicitud fue turnada a la Dirección General de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información, previsto para esos efectos.

TERCERO. Que el titular de la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, unidad administrativa adscrita a la Dirección General de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, mediante oficio con número de referencia D04/047/2019, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

CUARTO. Que este órgano colegiado, mediante resolución de veintinueve de octubre de dos mil diecinueve, confirmó la ampliación del plazo de respuesta por diez días hábiles adicionales al plazo original, para la atención de la solicitud al rubro citada.

QUINTO. Que con motivo de la atención de una solicitud de acceso a la información diversa, la otrora Dirección de Sistemas de Pagos del Banco de México, clasificó diversa información contenida en el documento señalado en el oficio de nueve de febrero de dos mil diecisiete, en los términos de la fundamentación y motivación señalados en dicho oficio, así como en la carátula y en la prueba de daño, puestos a disposición de este órgano colegiado en su momento.

SEXTO. Que la clasificación señalada en el resultando precedente y la versión pública correspondiente fueron confirmadas por este Comité de Transparencia, mediante resolución emitida en su sesión ordinaria celebrada el quince de febrero de dos mil diecisiete, en términos de dicha resolución.

SÉPTIMO. Que el titular de la referida Dirección de Operación y Continuidad de los Sistemas de Pagos e Infraestructura de Mercados, mediante oficio con número de referencia D40/051/19, hizo del conocimiento de este órgano colegiado su determinación de desclasificar diversa información contenida en el documento señalado en dicho oficio, en términos de lo expresado, fundado y motivado en el mismo.

Asimismo, hizo del conocimiento de este órgano colegiado su determinación de clasificar la información señalada en el oficio referido, y solicitó a este Comité de Transparencia confirmar dicha clasificación toda vez que las causas de clasificación subsisten a la fecha, en términos de la fundamentación y motivación expresados en el oficio en comento, en la carátula correspondiente y en la prueba de daño puesta a disposición de este órgano colegiado en su momento, y aprobar la versión pública respectiva.

CONSIDERANDOS

PRIMERO. Este Comité de Transparencia y las unidades administrativas de este Banco central son competentes para llevar a cabo la desclasificación de la información, de conformidad con lo previsto en los artículos 101, de la LGTAIP; y 99, de la Ley Federal de Transparencia y Acceso a la información Pública (LFTAIP); así como el Décimo sexto, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" (Lineamientos), vigentes.

Asimismo, 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 (LGTAIP); 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); y 31, fracción II, del Reglamento Interior del Banco de México (RIBM). De igual modo, este órgano colegiado es competente para aprobar las versiones públicas que someten a su consideración, en términos del Quincuagésimo sexto y el Sexagésimo segundo, párrafos primero y segundo, inciso a), de los Lineamientos.

SEGUNDO. Tal como se señala en la resolución emitida por este órgano colegiado el quince de febrero de dos mil diecisiete, con motivo de la atención de una solicitud de acceso diversa, la unidad administrativa señalada en el resultando Quinto, determinó clasificar la información referida, en razón de lo fundado y motivado en el oficio puesto a disposición de este Comité de Transparencia en dicha ocasión, así como en la carátula y en la prueba de daño correspondientes.

Sin embargo, mediante el oficio señalado en el resultando Séptimo de la presente determinación, la Dirección de Operación y Continuidad de los Sistemas de Pagos e Infraestructura de Mercados, manifestó al Comité de Transparencia que a la fecha, no se actualizan las causas para mantener clasificada la información señalada en dicho oficio, por las razones señaladas en el mismo.

En consecuencia, este órgano colegiado **toma conocimiento de la desclasificación expresada en el oficio referido.**

TERCERO. Enseguida se analiza la clasificación referida en el resultando Séptimo de la presente determinación:

1. Es procedente la clasificación de la información referida como confidencial conforme a la fundamentación y motivación expresadas en el oficio referido en el resultando Séptimo.

Asimismo, este Comité advierte que no se actualiza alguno de los supuestos de excepción previstos en Ley para que el Banco de México se encuentre en posibilidad de permitir el acceso a la información señalada, en términos de los artículos 120 de la LGTAIP, 117 de la LFTAIP, y 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

En consecuencia, este Comité **confirma la clasificación de la información referida como confidencial** en el oficio señalado en el resultando Séptimo de la presente determinación.

2. Es procedente la clasificación de la información como reservada conforme a la fundamentación y motivación expresadas en la correspondiente prueba de daño, la cual se tiene aquí por reproducida como si a la letra se insertase en obvio de repeticiones innecesarias.

En consecuencia, este Comité **confirma la clasificación de la información señalada como reservada** en el oficio referido en el resultando Séptimo de la presente determinación.

En este sentido, **se aprueba la versión pública señalada en el oficio precisado en el resultando Séptimo de la presente determinación.**

Por lo expuesto, con fundamento en los artículos 44, fracciones II y IX, 101, y 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracciones II y IX, 99, y 102, párrafo primero, de la LFTAIP; 31, fracciones III y XX, del RIBM; el Décimo Sexto, de los Lineamientos vigentes; y la Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

PRIMERO. Este Comité **toma conocimiento de la desclasificación de la información** realizada por el Director de Operación y Continuidad de los Sistemas de Pagos e Infraestructura de Mercados, y que en su momento fue clasificada como confidencial por la Dirección de Sistemas de Pagos, en los términos del considerando Segundo de la presente resolución.

SEGUNDO. Se **confirma la clasificación de la información señalada como confidencial** en el oficio referido en el resultando Séptimo de la presente resolución, conforme a la fundamentación y motivación expresadas en dicho oficio, así como en la carátula correspondiente, en términos del numeral 1 del considerando Tercero de la presente determinación.

TERCERO. Se **confirma la clasificación de la información señalada como reservada** en el oficio referido en el resultando Séptimo de la presente resolución, conforme a la fundamentación y motivación expresadas en dicho oficio, así como en la carátula y en la prueba de daño correspondiente, en términos del numeral 2 del considerando Tercero de la presente determinación.

CUARTO. Se **aprueba la versión pública** señalada en el oficio precisado en el resultando Séptimo 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 catorce de noviembre de dos mil diecinueve. ----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

Anexo "9"

BANCO DE MÉXICO

BANCO DE MÉXICO
RECIBIDO
12 NOV 2019
Comité de Transparencia
Por: JI5363 Hora: 12:02

Se recibe oficio constante en dos páginas, una carátula y una prueba de daño.....

Ciudad de México, a 08 de noviembre de 2019
D40/050/19

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 **6110000065919** que nos turnó la Unidad de Transparencia el nueve de octubre del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

> *"Expediente técnico mediante el cual el Banco de México otorgó la autorización como Participante del Sistema de Pagos Electrónicos Interbancarios a la empresa Sistema de Transferencias y Pagos STP, SA de CV, Sofom, ENR."*

Al respecto, me permito informarles que esta unidad administrativa, de conformidad con los artículos 100, 106, fracción I, y 111, de la Ley General de Transparencia y Acceso a la Información Pública, 97, 98, fracción I, y 108, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, ha determinado clasificar diversa información contenida en el documento que se indica más adelante, de conformidad con la fundamentación y motivación señaladas en la carátula y en la prueba de daño correspondiente.

Para facilitar su identificación, en el siguiente cuadro encontrarán el detalle del título del documento clasificado, el cual coincide con el que aparece en la carátula que debidamente firmada se acompaña al presente.

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXO
Documentación relacionada con la autorización al Participante en el SPEI, específicamente de STP	1	2

Por lo expuesto, en términos de los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, de los Lineamientos, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de la información realizada por esta unidad administrativa, y aprobar la versión publica señalada en el cuadro precedente.

BANCO DE MÉXICO

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informo que el personal que por la naturaleza de sus atribuciones tiene acceso al referido documento clasificado es el adscrito a la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, así como a la Dirección de Disposiciones de Banca Central, Gerencia de Instrumentación de Operaciones y Gerencia de Autorizaciones y Consultas de Banca Central.

Atentamente,

Ángel Melesio Fuentes
Director de Operación y Continuidad de Sistemas de Pagos
e Infraestructuras de Mercados

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 100, 106, fracción I, 109 y 111 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97, 98, fracción I, 106, 108 y 118 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción I, Quincuagésimo sexto, Sexagésimo segundo y Sexagésimo tercero de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Lineamientos).

VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados
II. La identificación de los documentos del que se elaboran las versiones públicas.	Documentación relacionada con la autorización al Participante en el SPEI, específicamente de STP
III. Firma del titular del área y de quien clasifica.	**Ángel Melesio Fuentes** Director de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia "ORDINARIA", número 47/2019 celebrada el 14 de DICIEMBRE de 2019. **Secretaría del Comité de Transparencia** Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México. Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México

BANCO DE MÉXICO

A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación y, en los supuestos de información clasificada como reservada, el periodo de reserva:

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
1	2, 10 y11	Nombre de Personas físicas (terceros).	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracción IX, 6, 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que el nombre es la manifestación principal del derecho subjetivo a la identidad, hace que una persona física sea identificada o identificable, y consecuentemente es un dato personal. En efecto, el nombre de una persona física además de ser un atributo de la personalidad que por esencia sirve para distinguir y determinar a las personas en cuanto a su identidad, es el conjunto de signos que constituyen un elemento básico e indispensable de la identidad de cada persona sin el cual no puede ser reconocida por la sociedad, así como un derecho humano que protege el nombre propio y los apellidos. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible conocer información personal de su titular.
2	2	Número telefónico de persona física	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable.

			la LGTAIP; 1, 2, fracción V, 3, fracción IX, 6, 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	En efecto, el número de teléfono ya sea fijo o celular se encuentra asignado a una persona determinada para poder ser localizado a través de diversos aparatos de telecomunicación. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar vía telefónica a su titular.
3	2	Correo electrónico de persona física	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracción IX, 6, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable. En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a

				través de la misma es posible localizar e identificar a su titular.
4	2 y11	Firma autógrafa de persona física	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracción IX, 6, 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal que está intrínseca y objetivamente ligado a la persona. Existe un vínculo que une indisociablemente al firmante con el documento y, por extensión, al autor con su declaración. Este atributo de la persona identifica o hace identificable a su titular. Asimismo, en oposición a la firma mediante la cual los servidores públicos validan los actos que emiten, los particulares no lo hacen en virtud del cumplimiento de obligaciones que les correspondan en términos de las disposiciones jurídicas aplicables, mientras que los servidores públicos lo hacen en razón del cumplimiento de sus facultades.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
A	7 y 11	Información contenida en la documentación relacionada con la autorización al Participante en el SPEI, específicamente de STP	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO®

PRUEBA DE DAÑO

Información contenida en la documentación relacionada con la autorización al Participante en el SPEI, específicamente de STP

En términos de lo dispuesto por los artículos 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; 110, fracción IV, de la Ley Federal de Transparencia y Acceso a la Información Pública; 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" vigentes, debe clasificarse como información reservada, entre otra:

- Aquélla que menoscabe la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, y ponga en riesgo el funcionamiento de tales sistemas o, en su caso, de la economía nacional en su conjunto.

- Aquélla que comprometa las acciones encaminadas a proveer a la economía del país de moneda nacional, y dañe la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero o el buen funcionamiento de los sistemas de pagos; o bien,

Al respecto, revelar al público la información relativa a las especificaciones técnicas de la infraestructura del Sistema de Pagos Electrónicos Interbancarios (SPEI®), la cual está contenida en documentación relacionada con la autorización al Participante en el SPEI, específicamente de STP, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento del sistema de pagos denominado SPEI, crearía distorsiones en el sistema de pagos denominado SPEI y comprometería las acciones encaminadas a propiciar el buen funcionamiento del sistema de pagos denominado SPEI y podría generar el incumplimiento de obligaciones de un participante en el sistema de pagos denominado SPEI.

En relación con lo anterior, se exponen las consideraciones siguientes:

La documentación relacionada con la autorización al Participante en el SPEI, específicamente de STP, contiene información relativa a las especificaciones técnicas de la infraestructura del SPEI, esta información, en caso de divulgarse podría ser analizada y utilizada por una persona o grupo de personas malintencionadas para preparar o perpetrar ataques cibernéticos dirigidos específicamente al mencionado sistema de pagos, lo cual posibilitaría la creación de mecanismos que faciliten el acceso indebido al propio sistema, la substracción de información relativa 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 de pagos electrónicos interbancarios** y, en consecuencia, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento del sistema de pagos denominado SPEI, crearía distorsiones en el sistema de pagos denominado SPEI y comprometería las acciones encaminadas a propiciar el buen funcionamiento del sistema de pagos denominado SPEI.

La divulgación de la citada información representa un riesgo de perjuicio significativo al interés público, toda vez que dicho riesgo es:

1. **Real**, ya que los ataques informáticos son acciones encaminadas a ingresar sin autorización a computadoras, sistemas, aplicaciones, y redes de comunicación, entre otros elementos, con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes.

Al respecto, está documentado en la literatura especializada en la materia[1] 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.

Dentro de los elementos mencionados en el párrafo anterior, la documentación materia de la presente prueba de daño contiene **especificaciones técnicas** de la infraestructura de SPEI®por lo cual su divulgación podría habilitar un ataque a los servicios de la infraestructura de dicho sistema.

2. **Demostrable, 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 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,

---

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

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

3 Arreola Javier. "Ciberseguridad (casi) a prueba del enemigo 'invisible'". Forbes México. http://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/ consultado el 08 de noviembre 2019.

4 Informe Norton sobre Ciberseguridad 2016 - Comparaciones Globales https://now.symassets.com/content/dam/content/es-mx/collaterals/datasheets/norton-cyber-security-insights-report2016.pdf consultado el 08 de noviembre 2019.

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/d/%7B9ACA4DC8-2B96-8EB3-6FF3-F58DDFA3FE51%7D.pdf, consultado el 08 de noviembre 2019.

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 24 de julio 2019.

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 08 de noviembre 2019.

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 08 de noviembre 2019.

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 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

---

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 08 de noviembre 2019.

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 08 de noviembre 2019.

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 08 de noviembre 2019.

13 S21Sec. "COBALT: EL CIBERCRIMEN ORGANIZADO GOLPEA LOS CAJEROS AUTOMÁTICOS EUROPEOS." S21Sec, 23 de noviembre de 2016, https://www.s21sec.com/cobalt-cibercrimen-organizado-que-ataca-a-los-cajeros-automaticos-europeos/, consultado el 08 de noviembre de 2019.

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 08 de noviembre 2019.

15 Delta Airlines. "INFORMATION ON [24]7.AI CYBER INCIDENT." Information on [24]7.Ai Cyber Incident, 7 de abril de 2018, https://news.delta.com/updated-statement-247ai-cyber-incident consultado el 08 de noviembre de 2019.

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 08 de noviembre 2019.

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

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 Sistema de Pagos Electrónicos Interbancarios (SPEI®), el cual consistió en la alteración de sus aplicativos para conectarse a esta Infraestructura de Mercado Financiera (IMF), mediante código malicioso, el cual distribuyó dinero desde las cuentas concentradoras de los participantes a cuentas de usuarios específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero.[19] A la fecha de elaboración de la presente prueba de daño, se estima un daño a los participantes del SPEI® de aproximadamente 300 millones de pesos.[20]

Inclusive, uno de los *modus operandi* de los ciberataques es precisamente a través de la obtención de información pública, información fácilmente accesible o información inaccesible, lo cual puede 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 especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuyo rol no esté autorizado,**[23] 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.

3. **Identificable,** ya que independientemente del origen o finalidad de un ataque contra el SPEI o las tecnologías de la información, comunicaciones o infraestructura tecnológica bajo la cual opera dicho sistema, podrían resultar afectadas las órdenes de transferencia en las cuentas bancarias de los distintos participantes y 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

---

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 08 de noviembre 2019.

19 Banco de México. "Información sobre los ataques a los Participantes del SPEI". https://www.banxico.org.mx/spei/d/%7BFFC53F5A-CA04-3098-EBF6-B0F17E533183%7D.pdf, consultado el 08 de noviembre 2019.

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/spei/d/%7BB806F1E8-686D-B9F1-0452-EC375543C801%7D.pdf, consultado el 08 de noviembre 2019.

21 El Economista, *El sistema financiero mexicano fue víctima de una campaña de ciberataques*, 15 de mayo de 2018. https://www.eleconomista.com.mx/sectorfinanciero/El-sistema-financiero-mexicano-fue-victima-de-una-campana-de-ciberataques-20180515-0097.html consultado el 08 de noviembre 2019.

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 08 de noviembre 2019.

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 08 de noviembre 2019.

financieras del país y demás participantes del SPEI, sino en perjuicio de la población usuaria de los pagos electrónicos interbancarios, es decir millones de personas físicas y personas morales.

Adicionalmente, una disrupción en los servicios provistos por los sistemas de pagos o de sus participantes, producto de un ataque contra estos o sus tecnologías de la información y de comunicaciones, tendría repercusiones directas para **una gran cantidad de empresas y comercios**, cuyas obligaciones a cubrir a través de pagos electrónicos interbancarios se verían afectadas durante el tiempo de la interrupción de estos servicios. Asimismo, **la población en general** que utiliza estos medio de pago, vería afectada su capacidad para realizar o cumplir con el pago de bienes y servicios, y **las instituciones bancarias y no bancarias participantes de los sistemas de pagos**, que 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 perpetrado directamente al SPEI® o a sus participantes, ocasionado por dar a conocer **información,** representa un perjuicio significativo para **el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias**, pues de acuerdo con la información del Banco de México, de agosto de 2018 a agosto de 2019, **se realizaron aproximadamente 636 millones de pagos electrónicos interbancarios por un monto de 207 billones de pesos;** ahora bien y específicamente para el mes de agosto 2019 se realizaron aproximadamente 81 **mil operaciones por hora, por un monto de 23 mil millones de pesos, únicamente para lo que respecta al SPEI® en un mes.**[24]

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

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, 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 IMF 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**, esto es, que permita planear y perpetrar ataques cibernéticos dirigidos específicamente a los sistemas de pagos administrados por el Banco de México y a la infraestructura relacionada con estos, los cuales tengan como resultado la creación de mecanismos que faciliten el acceso indebido, la substracción de información - como

---

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.

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.

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* **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 previstas en la Leyes aplicables**, 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, 107, 108, último párrafo, 109, 113, fracción IV, y 114 de la LGTAIP; 97, 100, 102, 103, 104, 105. Último párrafo, 110, fracción 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, 12 Bis y 20 Ter del Reglamento Interior del Banco de México; Segundo, fracción XVII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como, Primero, Cuarto, Quinto, Sexto, párrafo segundo, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I, II y IV, de los Lineamientos, **se clasifica como reservada, por el plazo de 5 años a partir de la fecha de clasificación,** *la información contenida en la documentación relacionada con la autorización al Participante en el SPEI, específicamente de STP,* 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 pagos, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques informáticos, lo cual traería como consecuencia el que se 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, así como comprometería las acciones encaminadas a propiciar el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

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

Order Code RL32331

The Economic Impact of Cyber-Attacks

April 1, 2004

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

REFERENCIA 3

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/)
mayo 20, 2016 @ 2:00 pm

Ciberseguridad (casi) a prueba del enemigo 'invisible'

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

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

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

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

MÁS COBERTURA

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

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

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

REFERENCIA 4

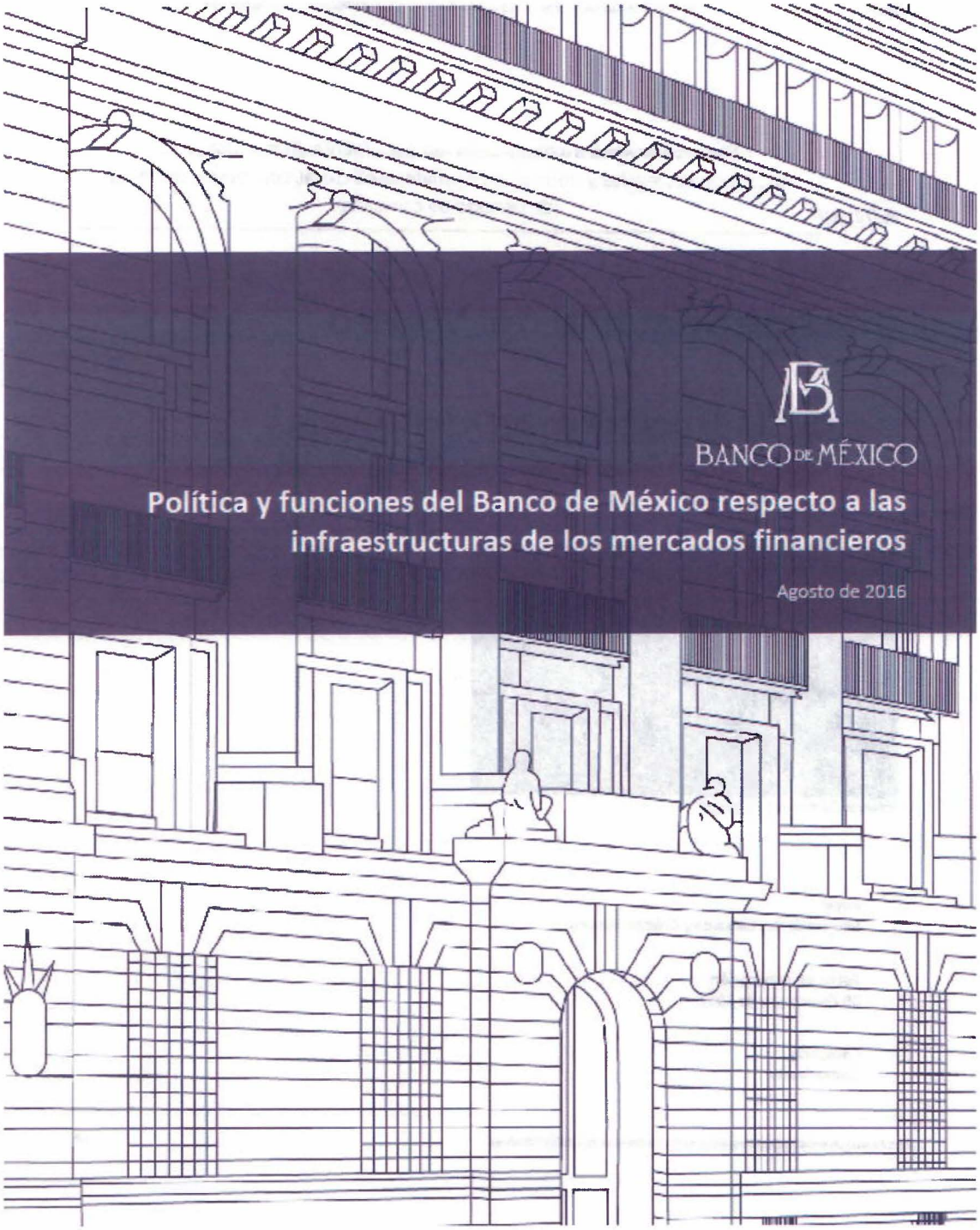
Informe Norton sobre Ciberseguridad 2016

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

REFERENCIA 5



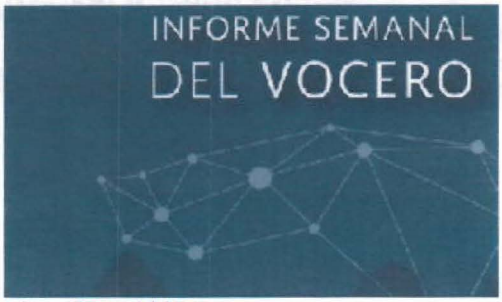
REFERENCIA 6

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

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

Más gotliana@gmail.com Escritorio Cerrar sesión

BAE SYSTEMS THREAT RESEARCH BLOG

Resources Contact us

Home Products Solutions News & Events Partners About Us Careers

SEARCH

Home » Threat Research » Lazarus & Watering-hole attacks

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

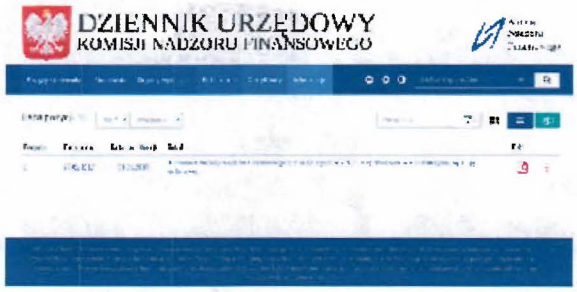
LAZARUS & WATERING-HOLE ATTACKS

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

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

ANALYSIS

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



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

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin.

Sign up

POPULAR POSTS


TWO BYTES TO $951M


WANACRYPTOR RANSOMWORM


CYBER HEIST ATTRIBUTION

CONTACT

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

team@baesystems.com

Contact

REFERENCIA 9

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

Article in **World Neurosurgery** · June 2017

DOI: 10.1016/j.wneu.2017.06.104

CITATION
1

READS
142

1 author:

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

SEE PROFILE

REFERENCIA 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

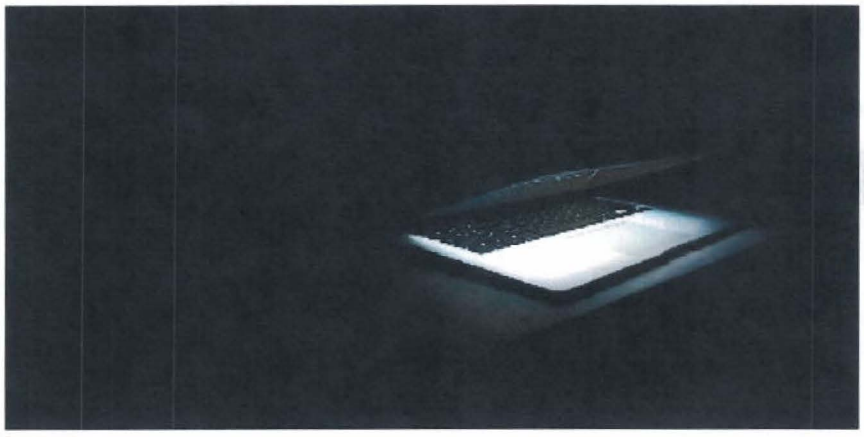


Imagen: Björn Olsson, bajo licencia Creative Commons.

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 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.

REFERENCIA 15

DELTA

MY TRIPS BOOK A TRIP FLIGHT STATUS CHECK IN SIGN UP LOG IN

INFORMATION ON [24]7.AI CYBER INCIDENT

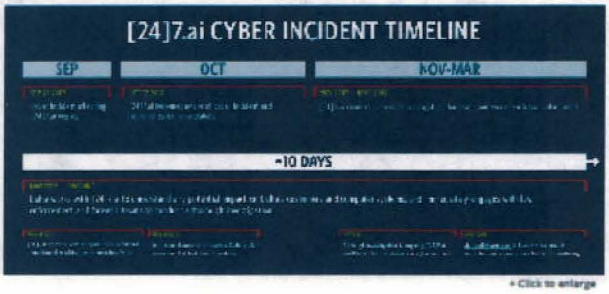
OVERVIEW

Last updated on April 7, 2018 9:00am 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.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

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 Vanquen*

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

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

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

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

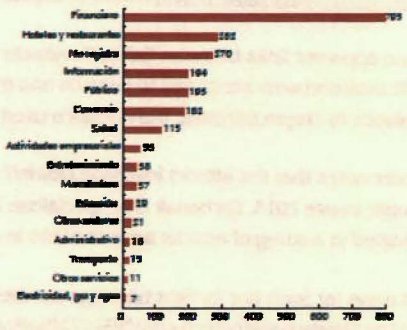
* Los autores pertenecen al Departamento de Estabilidad Financiera del Banco de la República. Sus opiniones no comprometen al Banco de la República ni a su Junta Directiva. Los errores u omisiones que persistan son responsabilidad exclusiva de los autores.

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).

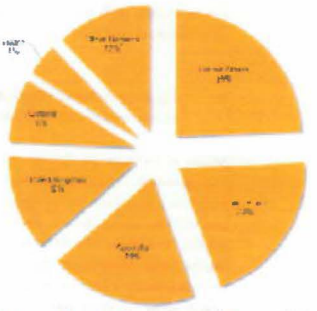
REFERENCIA 18

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.



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

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 (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

REFERENCIA 19

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.

REFERENCIA 21

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, 14:34

Algunas instituciones del sistema financiero en México sufrieron una campaña de ciberataques, a principios del 2017, que afectó los aplicativos y la infraestructura de tecnologías de la información que dan soporte a los servicios de banca en línea, y que contó con elementos similares a los que se describen en la información que se conoce hasta el momento sobre el hackeo a las instituciones bancarias que afectó la operación del Sistema de Pagos Electrónicos Interbancarios (SPEI) las últimas semanas.

De acuerdo con Eduardo Espina, director de Ciberseguridad de Mnemo-CERT, ciertos elementos y tendencias de esta campaña de ataques de ciberseguridad que ocurrió durante varios meses del 2017 tiene elementos en común con el ciberataque ocurrido desde el pasado 27 abril. La nueva afrenta a los bancos fue calificada como un ataque que " no tiene precedentes en el país", de acuerdo con Alejandro Díaz de León, gobernador del Banco de México.

REFERENCIA 22

+2
2 Votes

Social Engineering Fundamentals, Part I: Hacker Tactics

By: Ω

Created 18 Dec 2001 0 Comments

0 0

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

/connect/forward?path=node/125624)

by Sarah Granger

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

A True Story

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

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

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 de bajo valor
Transferencias SPEI por monto operado

Fecha de consulta: 09/09/2019 01:19:06

Título	Pagos tercero a tercero - SPEI, Total, Número de operaciones	Pagos tercero a tercero - SPEI, Total, Monto total
Periodo disponible	Ene 2010 - Ago 2019	Ene 2010 - Ago 2019
Periodicidad	Mensual	Mensual
Cifra	No Homogénea	No Homogénea
Unidad	Sin Unidad	Sin Unidad
Base		
Aviso		
Tipo de información	Niveles	Niveles
Fecha	SF273317	SF273318
Ago 2018	42,300,962	16,952,190,978,481
Sep 2018	38,247,948	14,874,360,565,848
Oct 2018	45,753,277	16,639,787,747,717
Nov 2018	44,807,576	15,646,789,635,198
Dic 2018	48,478,611	16,214,002,019,976
Ene 2019	44,039,343	16,458,387,585,724
Feb 2019	43,644,739	14,219,566,527,833
Mar 2019	47,940,478	15,245,324,607,574
Abr 2019	54,229,918	15,183,622,594,779
May 2019	56,603,945	16,447,959,850,726
Jun 2019	51,495,023	15,875,529,025,074
Jul 2019	60,288,327	17,322,095,269,961
Ago 2019	58,538,163	16,679,241,168,508

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000065919
Unidad administrativa: Dirección de Operación y Continuidad de los Sistemas de Pagos e Infraestructura de Mercados del Banco de México.

VISTOS, para resolver sobre la clasificación de información manifestada por la unidad administrativa al rubro citada; y

RESULTANDO

PRIMERO. Que el nueve de octubre de dos mil diecinueve, la Unidad de Transparencia del Banco de México recibió la solicitud con folio citado al rubro, la cual en su parte conducente refiere lo siguiente:

> *"Expediente técnico mediante el cual el Banco de México otorgó la autorización como Participante del Sistema de Pagos Electrónicos Interbancarios a la empresa Sistema de Transferencias y Pagos STP, SA de CV, Sofom, ENR."*

SEGUNDO. Que el mismo nueve de octubre de dos mil diecinueve, la referida solicitud fue turnada a la Dirección General de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información, previsto para esos efectos.

TERCERO. Que el titular de la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados, unidad administrativa adscrita a la Dirección General de Sistemas de Pagos e Infraestructuras de Mercados del Banco de México, mediante oficio con número de referencia D04/047/2019, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

CUARTO. Que este órgano colegiado, mediante resolución de veintinueve de octubre de dos mil diecinueve, confirmó la ampliación del plazo de respuesta por diez días hábiles adicionales al plazo original, para la atención de la solicitud al rubro citada.

QUINTO. Que el titular de la referida Dirección de Operación y Continuidad de los Sistemas de Pagos e Infraestructura de Mercados, mediante oficio con número de referencia D40/050/19, hizo del conocimiento de este órgano colegiado su determinación de clasificar la información señalada en dicho oficio, en términos de la motivación y fundamentación expresadas en el mismo, así como en la carátula y en la prueba de daño correspondiente, y solicitó a este Comité de Transparencia confirmar dicha clasificación y aprobar la versión pública respectiva.

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 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 (LGTAIP); 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); y 31, fracción II, del Reglamento Interior del Banco de México (RIBM).

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

SEGUNDO. Enseguida se analiza la clasificación referida en el resultando Quinto de la presente determinación:

1. Es procedente la clasificación de la información referida como confidencial conforme a la fundamentación y motivación expresadas en el oficio referido en el resultando Quinto.

Asimismo, este Comité advierte que no se actualiza alguno de los supuestos de excepción previstos en Ley para que el Banco de México se encuentre en posibilidad de permitir el acceso a la información señalada, en términos de los artículos 120 de la LGTAIP, 117 de la LFTAIP, y 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

En consecuencia, este Comité **confirma la clasificación de la información referida como confidencial** en el oficio señalado en el resultando Quinto de la presente determinación.

2. Es procedente la clasificación de la información como reservada conforme a la fundamentación y motivación expresadas en la correspondiente prueba de daño, la cual se tiene aquí por reproducida como si a la letra se insertase en obvio de repeticiones innecesarias.

En consecuencia, este Comité **confirma la clasificación de la información señalada como reservada** en el oficio referido en el resultando Quinto de la presente determinación.

En este sentido, **se aprueba la versión pública señalada en el oficio precisado en el resultando Quinto de la presente determinación.**

Por lo expuesto, con fundamento en los artículos 44, fracciones II y IX, 101, y 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracciones II y IX, 99, y 102, párrafo primero, de la LFTAIP; 31, fracciones III y XX, del RIBM; el Décimo Sexto, de los Lineamientos vigentes; y la Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

PRIMERO. Se **confirma la clasificación de la información señalada como confidencial** en el oficio referido en el resultando Quinto de la presente resolución, conforme a la fundamentación y motivación expresadas en dicho oficio, así como en la carátula correspondiente, en términos del numeral 1 del considerando Tercero de la presente determinación.

SEGUNDO. Se **confirma la clasificación de la información señalada como reservada** en el oficio referido en el resultando Quinto de la presente resolución, conforme a la fundamentación y motivación

expresadas en dicho oficio, así como en la carátula y en la prueba de daño correspondiente, en términos del numeral 2 del considerando Tercero de la presente determinación.

TERCERO. Se **aprueba la versión pública** señalada 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 catorce de noviembre de dos mil diecinueve. ----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

BANCO DE MÉXICO
RECIBIDO
13 NOV 2019
Comité de Transparencia
Por: B17035 Hora: 18:00

Se recibe oficio constante en una página....

Anexo "11"

BANCO DE MÉXICO

Ciudad de México, a 13 de noviembre de 2019
REF.V01.228.2019

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 **6110000071719**, recibida el dieciocho de octubre de dos mil diecinueve, 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, en su parte conducente:

> *"Solicito conocer el número de ex funcionarios que reciben y recibieron pensiones vitalicias y/o sueldos vitalicios y/o haberes de retiro (o cualquier nombre técnico con el que se le conozca). Favor de indicar: 1. Nombre (o versión pública) 2. Cargo que desempeñó 3. Años de servicio 4. Si a la fecha recibe los recursos o ya dejó de recibirlos 5. De haber dejado de recibirlos indicar la fecha y el motivo. 6.Monto asignado por mes. 7. Fecha en la que comenzó a recibir dicha pensión vitalicia, sueldo vitalicio o haber de retiro. Precisar si el ex funcionario cuenta con derecho a otros ingresos, como gastos de alimentación; vehículos para su transportación(indicar número de vehículos y monto asignado); gasolina (indicar monto)y aditivos (indicar monto); asistentes y sueldo para asistentes (en caso de se afirmativa la respuesta, indicar el número de asistentes y el monto asignado para sus sueldos) o cualquier otro derecho de ingreso (precisar cuál y el monto por cada uno de ellos así como la periodicidad)."*

Sobre el particular, requerimos a ese órgano colegiado aprobar la ampliación del plazo de respuesta a la solicitud de acceso indicada ya que, dada la naturaleza y cúmulo de información se está obteniendo y verificando la información que posee esta unidad administrativa. Lo anterior, con la finalidad de que la información que se entregue al solicitante sea accesible, confiable, verificable, veraz y oportuna.

Esta solicitud de ampliación 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, 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; Vigésimo Octavo de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública".

Sin otro particular, quedo a sus órdenes para cualquier aclaración al respecto,

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

JUN RODRIGO HINOKI ALCARAZ
Director de Recursos Humanos

Anexo "12"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DE PLAZO
FOLIO: 6110000071719

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

RESULTANDO

PRIMERO. Que el dieciocho de octubre de dos mil diecinueve, la Unidad de Transparencia del Banco de México recibió la solicitud con folio citada al rubro, la cual se transcribe a continuación:

> *"Solicito conocer el número de ex funcionarios que reciben y recibieron pensiones vitalicias y/o sueldos vitalicios y/o haberes de retiro (o cualquier nombre técnico con el que se le conozca). Favor de indicar: 1. Nombre (o versión pública) 2. Cargo que desempeñó 3. Años de servicio 4. Si a la fecha recibe los recursos o ya dejó de recibirlos 5. De haber dejado de recibirlos indicar la fecha y el motivo. 6.Monto asignado por mes. 7. Fecha en la que comenzó a recibir dicha pensión vitalicia, sueldo vitalicio o haber de retiro. Precisar si el ex funcionario cuenta con derecho a otros ingresos, como gastos de alimentación; vehículos para su transportación(indicar número de vehículos y monto asignado); gasolina (indicar monto)y aditivos (indicar monto); asistentes y sueldo para asistentes (en caso de se afirmativa la respuesta, indicar el número de asistentes y el monto asignado para sus sueldos) o cualquier otro derecho de ingreso (precisar cuál y el monto por cada uno de ellos así como la periodicidad). "*

SEGUNDO. Que el mismo dieciocho de octubre del año en curso, la referida solicitud fue turnada a la Dirección de Recursos Humanos del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información, previsto para esos efectos.

TERCERO. Que el titular de la Dirección de Recursos Humanos, mediante oficio referencia V01.228.2019, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

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 (LGTAIP); 65, fracción II, y 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); 31, fracción III, del Reglamento Interior del Banco de México (RIBM), y Vigésimo octavo de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública" (Lineamientos), vigentes, 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 Tercero de la presente determinación, el titular de la Dirección de Recursos Humanos, expuso las razones para ampliar el plazo de respuesta a la solicitud de acceso citada al rubro, las cuales se tienen aquí por reproducidas como si a la letra se insertasen, en obvio de repeticiones innecesarias.

TERCERO. Que de conformidad con los artículos 44, fracción II y 132, párrafo segundo de la LGTAIP; 65, fracción II y 135 de la LFTAIP; y Vigésimo Octavo de los Lineamientos, es necesario que dada la naturaleza y complejidad de la información solicitada, el área competente realice una verificación exhaustiva 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 la unidad administrativa mencionada, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 132, párrafo segundo, de la LGTAIP; 1, 9, 64, 65, fracción II, y 135, párrafo segundo, de la LFTAIP; 31, fracción III, del RIBM, y Vigésimo octavo de los Lineamientos, 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 citada al rubro, en términos de lo expuesto en el considerando 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 14 de noviembre de dos mil diecinueve. ----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente