BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ORDINARIA 30/2018
DEL 26 DE JULIO DE 2018

En la Ciudad de México, a las trece horas del veintiséis de julio de dos mil dieciocho, en el edificio ubicado en avenida Cinco de Mayo, número seis, colonia Centro, delegación Cuauhtémoc, se reunieron Claudia Álvarez Toca, Directora de la Unidad de Transparencia, Humberto Enrique Ruiz Torres, Director Jurídico, y José Ramón Rodríguez Mancilla, Gerente de Organización de la Información, suplente del Director de Coordinación de la Información, todos integrantes del Comité de Transparencia de este Instituto Central, así como Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, en su carácter de Prosecretario de dicho órgano colegiado.----------

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

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

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

El Prosecretario del Comité sometió a consideración de los integrantes presentes de ese órgano colegiado el documento que contiene el orden del día- ----------

Este Comité de Transparencia del Banco de México, con fundamento en los artículos 51, párrafo segundo, y 83 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 43, párrafo segundo, 44, fracción IX, de la Ley General de Transparencia y Acceso a la Información Pública; 4o. y 31, fracciones III y XX, del Reglamento Interior del Banco de México, y Quinta, párrafo primero, inciso e), de las Reglas de Operación del Comité de Transparencia del Banco de México, por unanimidad, aprobó el orden del día en los términos del documento que se adjunta a la presente como **ANEXO "B"** y procedió a su desahogo, conforme a lo siguiente: ----------

PRIMERO. SOLICITUD DE CONFIRMACIÓN DE AMPLIACIÓN DEL PLAZO DE RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000034618. ----------

El Prosecretario dio lectura al oficio de veinte de julio de dos mil dieciocho, suscrito por los titulares de la Gerencia de Procesos Preventivos, unidad administrativa a la Dirección de Regulación y Supervisión, y de la Gerencia de Información del Sistema Financiero, unidad administrativa adscrita a la Dirección de Información del Sistema Financiero, que se agrega a la presente acta como **ANEXO "C",** por medio del cual dichas unidades administrativas solicitaron a este Comité de Transparencia confirmar la ampliación del plazo ordinario de respuesta para la solicitud de acceso a la información citada, por los motivos expuestos en el oficio referido.

BANCO DE MÉXICO

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

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

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE SISTEMAS DE PAGOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO CTC-BM-24183.----------

El Prosecretario dio lectura al oficio con referencia D01/C370/2018, suscrito por el titular de la Dirección de Sistemas de Pagos del Banco de México, que se agrega a la presente acta como **ANEXO "E"**, por virtud del cual dicha unidad administrativa hace del conocimiento de este Comité que ha determinado clasificar la información que se señala en dicho oficio, conforme a la fundamentación y motivación expresadas en la prueba de daño contenida en el cuerpo de dicho oficio, por lo que solicitó a este órgano colegiado confirmar tal clasificación.----------

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

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

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

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

SERGIO ZAMBRANO HERRERA
Prosecretario

ANEXO "A"

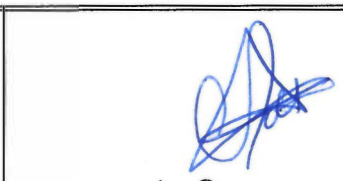
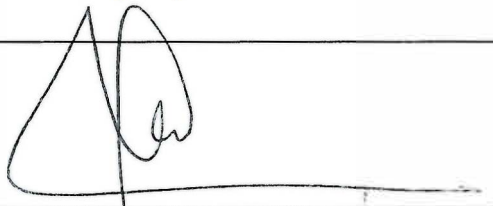
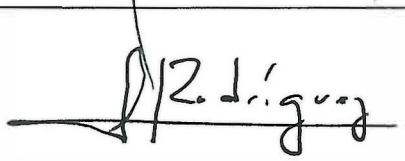
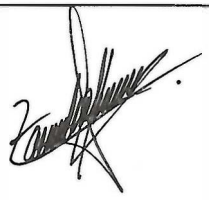
BANCO DE MÉXICO

LISTA DE ASISTENCIA

SESIÓN ORDINARIA 30/2018

26 DE JULIO DE 2018

COMITÉ DE TRANSPARENCIA

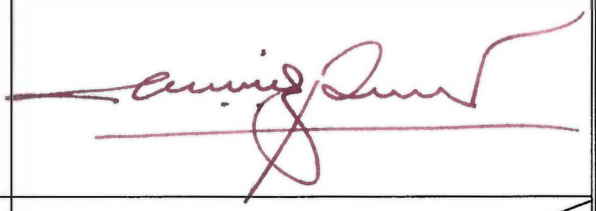
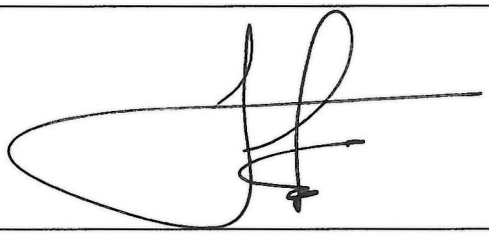
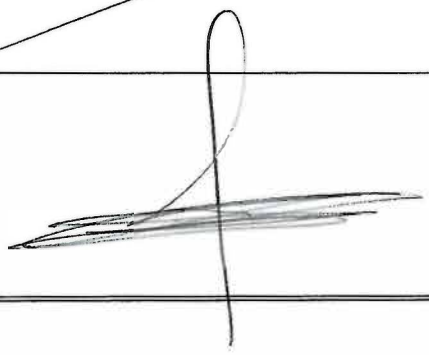
CLAUDIA ÁLVAREZ TOCA Directora de la Unidad de Transparencia Presidenta	
HUMBERTO ENRIQUE RUIZ TORRES Director Jurídico Integrante	
JOSÉ RAMÓN RODRÍGUEZ MANCILLA Gerente de Organización de la Información Integrante suplente	
SERGIO ZAMBRANO HERRERA Prosecretario del Comité de Transparencia	

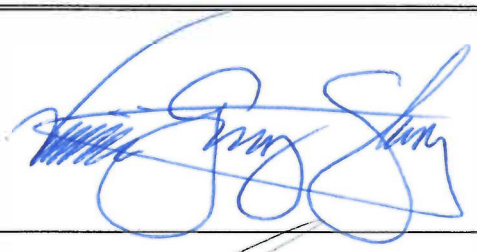
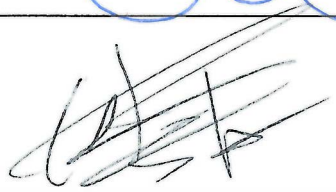
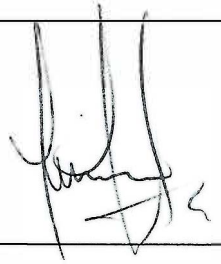
INVITADOS PERMANENTES

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

INVITADOS

ERIK MAURICIO SÁNCHEZ MEDINA Gerente Jurídico Consultivo	
ALAN CRUZ PICHARDO Subgerente de Apoyo Jurídico a la Transparencia	
CARLOS EDUARDO CICERO LEBRIJA Gerente de Gestión de Transparencia Integrante suplente	

RODRIGO MÉNDEZ PRECIADO Gerente de Enlace Institucional y Relaciones Públicas	
MARGARITA LISSETE PONCE GUARNEROS Subgerente de Identificación y Evaluación de Riesgos Operativos	
MARIO ALBERTO REYNA CERECERO Gerente de Información del Sistema Financiero	
JORGE FRANCISCO DE LA VEGA GÓNGORA Gerente de Arquitectura de Información del Sistema Financiero	
JORGE LUIS GARCÍA RAMÍREZ Gerente de Estabilidad Financiera	
CARLOS ALEJANDRO SAUCEDO QUINTANA Subgerente Técnico de Estabilidad Financiera	
RODOLFO GUTIÉRREZ SALAS Gerente de Procesos Preventivos	

VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión	
RICARDO GARCÍA BENÍTEZ Estudios y Proyectos Especiales de la Dirección General de Asuntos del Sistema Financiero	
QUIROZ ROBLES JORGE ERIK Analista de Estudios y Proyectos Especiales	
LILIANA GARCÍA OCHOA Líder de Especialidad	
XIMENA AIDEE DOMÍNGUEZ HERNÁNDEZ Investigador	
HÉCTOR GARCÍA MONDRAGÓN Jefe de la Oficina de Análisis Jurídico y Promoción de Transparencia	

ANEXO "B"

BANCO DE MÉXICO

Comité de Transparencia

ORDEN DEL DÍA
Sesión Ordinaria 30/2018
26 de julio de 2018

PRIMERO. SOLICITUD DE CONFIRMACIÓN DE AMPLIACIÓN DEL PLAZO DE RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000034618.

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE SISTEMAS DE PAGOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO CTC-BM-24183.

ANEXO "C"

BANCO DE MÉXICO

Ciudad de México, a 20 de julio de 2018

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

Me refiero a la solicitud de acceso a la información, identificada con el número de folio **6110000034618,** que nos turnó la Unidad de Transparencia el seis de julio 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 en su parte conducente:

> *"... solicito del Banco de México lo siguiente:1. Informe si existe alguna disposición normativa emitida por ese Instituto Central que establezca a las instituciones financieras que prestan el servicio de banca múltiple límites en el monto de dinero en efectivo que pueden tener en la bóveda y/o caja de sus sucursales. En caso afirmativo, exprese el artículo y el cuerpo normativo que lo contiene.2. Informe si existe alguna disposición normativa emitida por ese Instituto Central que establezca una clasificación de las sucursales de las instituciones financieras que prestan el servicio de banca múltiple en razón del monto máximo de efectivo que pueden tener en su bóveda y/o caja. En caso afirmativo, mencione el artículo y el cuerpo normativo que lo contiene.3. En caso de que la respuesta anterior sea afirmativa, exponga los términos de dicha clasificación.4. Informe si existe alguna disposición normativa expedida por el Banco Central que obligue a las instituciones financieras que prestan el servicio de banca múltiple a informar a ese Instituto el monto de dinero en efectivo que mantienen en la bóveda y/o caja de sus sucursales. En caso afirmativo, detalle el artículo y el cuerpo normativo que lo contiene.5. Informe si las instituciones de banca múltiple informan al Banco de México el monto de dinero en efectivo que mantienen diariamente en la bóveda y/o caja de sus sucursales al cierre de operaciones.6. En caso afirmativo a la pregunta anterior, informe con qué periodicidad rinden esa información las instituciones de banca múltiple.7. De ser afirmativa la respuesta de la quinta interrogante, informe si Banca Mifel, S.A., Institución de Banca Múltiple, Grupo Financiero Mifel, rinde el reporte del monto en efectivo que tiene diariamente en sus sucursales ante el Banco Central.8. En el evento de que exista una clasificación de sucursales bancarias, en razón del monto máximo de efectivo que pueden tener en su bóveda y/o caja, informe como se encuentra clasificada la sucursal Plaza Santa Teresa número 022, en la Ciudad de México de Banca Mifel, S.A., Institución de Banca Múltiple, Grupo Financiero Mifel.9. En el supuesto de que Banca Mifel, S.A., Institución de Banca Múltiple, Grupo Financiero Mifel, presente ante ese Banco Central el reporte del monto de efectivo que mantiene diariamente en sus sucursales, se sirva informar los montos de efectivo que reportó durante el periodo del 2 de mayo al 29 de junio del presente año, la sucursal Plaza Santa Teresa número 022 en la Ciudad de México, de dicha institución. Finalmente, solicito que la información me sea proporcionada por medios electrónicos a la dirección de correo señalada anteriormente..."*

BANCO DE MÉXICO

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, **por diez días más**, ya que dada la naturaleza y complejidad de la misma, se continúa verificando la información y documentación correspondiente. Lo anterior, con la finalidad de que se realice un cuidadoso ejercicio de análisis y valoración, para determinar si en el caso en concreto se actualiza alguno de los supuestos de clasificación previstos en la Ley General de Transparencia y Acceso a la Información Pública y en la Ley Federal de Transparencia y Acceso a la Información Pública.

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; 66, del Reglamento Interior del Banco de México; Vigésimo Octavo de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", vigentes; así como el punto Segundo del "Acuerdo por el que se determina el nivel jerárquico de los titulares de las unidades administrativas que deben clasificar información", emitido por el Comité de Transparencia en su sesión de veinticinco de enero de dos mil diecisiete.

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

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

Rodolfo Gutiérrez Salas
Gerente de Procesos Preventivos
En suplencia por ausencia de la Directora de Regulación y Supervisión, Viviana Garza Salazar , en términos del artículo 66 del Reglamento Interior del Banco de México

Mario Alberto Reyna Cerecero
Gerente de Información del Sistema Financiero
En suplencia por ausencia del Director de Información del Sistema Financiero, Mario Alejandro Gaytán González, en términos del artículo 66 del Reglamento Interior del Banco de México

BANCO DE MÉXICO
RECIBIDO
20 JUL 2018
Comité de Transparencia
Por: 15383 Hora: 12:35

Se recibe oficio constante en dos páginas.

ANEXO "D"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DE PLAZO
Folio: 6110000034618

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

RESULTANDO

PRIMERO. Que el seis de julio de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000034618**, la cual en su parte conducente refiere lo siguiente:

> *"... solicito del Banco de México lo siguiente:*
>
> *1. Informe si existe alguna disposición normativa emitida por ese Instituto Central que establezca a las instituciones financieras que prestan el servicio de banca múltiple límites en el monto de dinero en efectivo que pueden tener en la bóveda y/o caja de sus sucursales. En caso afirmativo, exprese el artículo y el cuerpo normativo que lo contiene.*
>
> *2. Informe si existe alguna disposición normativa emitida por ese Instituto Central que establezca una clasificación de las sucursales de las instituciones financieras que prestan el servicio de banca múltiple en razón del monto máximo de efectivo que pueden tener en su bóveda y/o caja. En caso afirmativo, mencione el artículo y el cuerpo normativo que lo contiene.*
>
> *3. En caso de que la respuesta anterior sea afirmativa, exponga los términos de dicha clasificación.*
>
> *4. Informe si existe alguna disposición normativa expedida por el Banco Central que obligue a las instituciones financieras que prestan el servicio de banca múltiple a informar a ese Instituto el monto de dinero en efectivo que mantienen en la bóveda y/o caja de sus sucursales. En caso afirmativo, detalle el artículo y el cuerpo normativo que lo contiene.*
>
> *5. Informe si las instituciones de banca múltiple informan al Banco de México el monto de dinero en efectivo que mantienen diariamente en la bóveda y/o caja de sus sucursales al cierre de operaciones.*

6. En caso afirmativo a la pregunta anterior, informe con qué periodicidad rinden esa información las instituciones de banca múltiple.

7. De ser afirmativa la respuesta de la quinta interrogante, informe si Banca Mifel, S.A., Institución de Banca Múltiple, Grupo Financiero Mifel, rinde el reporte del monto en efectivo que tiene diariamente en sus sucursales ante el Banco Central.

8. En el evento de que exista una clasificación de sucursales bancarias, en razón del monto máximo de efectivo que pueden tener en su bóveda y/o caja, informe como se encuentra clasificada la sucursal Plaza Santa Teresa número 022, en la Ciudad de México de Banca Mifel, S.A., Institución de Banca Múltiple, Grupo Financiero Mifel.

9. En el supuesto de que Banca Mifel, S.A., Institución de Banca Múltiple, Grupo Financiero Mifel, presente ante ese Banco Central el reporte del monto de efectivo que mantiene diariamente en sus sucursales, se sirva informar los montos de efectivo que reportó durante el periodo del 2 de mayo al 29 de junio del presente año, la sucursal Plaza Santa Teresa número 022 en la Ciudad de México, de dicha institución."

SEGUNDO. Que la Unidad de Transparencia del Banco de México remitió para su atención a la Dirección General de Asuntos del Sistema de Financiero, la Dirección General de Emisión, Dirección Disposiciones de Banca Central y la Dirección Jurídica, del Banco de México, el mismo seis de julio del presente año, la solicitud de acceso a la información referida en el resultando anterior, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que el titular de la Gerencia de Procesos Preventivos y el titular de la Gerencia de Información del Sistema Financiero, mediante oficio de veinte de julio del año en curso, sometieron a la consideración del Comité de Transparencia la determinación de ampliación del plazo de respuesta a la referida solicitud de acceso a la información. Al respecto, en dicho documento manifestaron de manera medular lo siguiente:

"... solicitamos a ese órgano colegiado aprobar la ampliación del plazo de respuesta a la solicitud de acceso indicada en el párrafo anterior, por diez días más, ya que dada la naturaleza y complejidad de la misma, se continúa verificando la información y documentación correspondiente. Lo anterior, con la finalidad de que se realice un cuidadoso ejercicio de análisis y valoración, para determinar si en el caso en concreto se actualiza alguno de los supuestos de clasificación previstos en la Ley General de Transparencia y Acceso a la Información Pública y en la Ley Federal de Transparencia y Acceso a la Información Pública."

CONSIDERANDO

PRIMERO. De conformidad con lo previsto en los artículos 44, fracción II, 131 y 132, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, y 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Vigésimo octavo de los *"Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública"*, este Comité de Transparencia cuenta con facultades para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las unidades administrativas del Banco.

SEGUNDO. Mediante el oficio referido en la sección de resultandos de la presente determinación, el titular de la Gerencia de Procesos Preventivos y el titular de la Gerencia de Información del Sistema Financiero del Banco de México, expusieron las razones para ampliar el plazo de respuesta a la solicitud de acceso a la información citada al rubro, particularmente, debido a que dada la naturaleza y complejidad de la misma, resulta necesario realizar un análisis de la misma para verificar si se actualiza alguna de las causales de clasificación previstas en la Ley General de Transparencia y Accesos a la Información Pública, para que se atienda en todo momento el requerimiento de acceso a la información del particular.

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

Por lo anterior, atendiendo a las razones expuestas por el área mencionada, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 132, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 9, 64, 65, fracción II, y 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Vigésimo octavo de los *"Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública"*, vigentes, este Comité de Transparencia:

RESUELVE

ÚNICO. Se confirma la ampliación del plazo de respuesta, por **diez días hábiles adicionales** al plazo original, respecto de la solicitud de acceso a la información citada al rubro, en términos de lo expuesto en los considerandos Segundo y Tercero de la presente determinación.

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

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidente

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

BANCO DE MÉXICO
RECIBIDO
20 JUL 2018
Comité de Transparencia
Por: JIS383 Hora: 14:02

Se recibe oficio constante en diez páginas y una prueba de daño.

ANEXO "E"

BANCO DE MÉXICO

Ciudad de México, a 20 de julio de 2018
D01/C370/2018

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

Me refiero a la solicitud de acceso a la información identificada con el número de folio **CTC-BM-24183** que nos turnó la Unidad de Transparencia el tres de julio 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 para pronta referencia se transcribe a continuación:

> *"Solicito por favor el documento: Guía para elaborar la certificación de requisitos de seguridad informática y gestión de riesgo operacional de participantes y potenciales participantes al SPID"*

Al respecto, me permito hacer de su conocimiento que esta unidad administrativa, de conformidad con los artículos 100, y 106, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública; 97, y 98,m fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Cuarto 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 como reservado la totalidad del documento que se indica más adelante,** de conformidad con la fundamentación y motivación señaladas en la prueba de daño correspondiente.

Para facilitar su identificación, en el siguiente cuadro encontrarán el detalle del título del documento clasificado.

TÍTULO DEL DOCUMENTO CLASIFICADO	PRUEBA DE DAÑO NÚMERO DE ANEXO
* Guía para elaborar la certificación de requisitos de seguridad informática y gestión del riesgo operacional de participantes y potenciales participantes al SPID	1

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 Cuarto, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de la información realizada por esta unidad administrativa.

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 Gerencia de Política y Vigilancia de los Sistemas de Pagos, a la Gerencia de Operación y Continuidad de Negocio de los Sistemas de Pagos y a la Gerencia de Tecnología de los Sistemas de Pagos.

Atentamente,

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

BANCO DE MÉXICO

PRUEBA DE DAÑO

Información relacionada con la seguridad informática que soporta el funcionamiento de los sistemas de pagos

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

a) Menoscabe la efectividad de las medidas implementadas en relación con las políticas en materia del sistema financiero del país, y ponga en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país;

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

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

En ese sentido, la "***Información relacionada con la seguridad informática que soporta el funcionamiento de los sistemas de pagos***" afectaría el interés público ya que menoscabaría la efectividad de las medidas implementadas en relación con las políticas en materia del sistema financiero del país, y pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; comprometería las acciones encaminadas a propiciar el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos; otorgaría ventaja a los cibercriminales para diseñar estrategias de ataques cibernéticos a los participantes de las Infraestructuras de los Mercados Financieros (IMF), entre ellas el Sistema de Pagos Interbancarios en Dólares (SPID), generando distorsiones en la estabilidad de los mercados financieros; o bien, podría generar el incumplimiento de las obligaciones de un participante en el sistema de pagos que dé lugar a que otros participantes incumplan, a su vez, con sus respectivas obligaciones afectando al sistema financiero o generando irregularidades en los sistemas de pagos; lo anterior, toda vez que dicho riesgo es:

a) **Real,** pues facilita a una persona o grupo de personas con intenciones delincuenciales identificar, y diseñar ataques focalizados sobre los elementos y especificaciones referidos o aquellos no considerados o especificados en la supuesta guía que pudieran ser utilizados y realizar acciones hostiles dirigidas al SPID o alguno de sus participantes; asimismo, podría guiar a potenciales ciberdelincuentes a diseñar estrategias, basadas en técnicas de ingeniería social o de suplantación de identidad como el phishing, dirigidas a las personas que derivado de sus funciones, ya sea en este Instituto Central, con cualquiera de sus participantes o a través de sus proveedores de servicios, y

obtener esta información de forma fraudulenta para, de igual manera diseñar ataques cibernéticos focalizados y acciones hostiles dirigidas al SPID o alguno de sus participantes.

En caso materializarse un ataque cibernético al SPID o alguno de sus participantes como consecuencia de divulgar la información referida, podría menoscabar la efectividad del SPID y su interconexión con otras IMF a tal grado, que afectaría seriamente la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, arriesgando el funcionamiento de esos sistemas y, en consecuencia, de la economía nacional en su conjunto.

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

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

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

Inclusive, la divulgación de la información en comento, facilita que mediante la explotación de las vulnerabilidades actuales, terceros logren acceder a información financiera o personal, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a dichas tecnologías.

Está documentado en la literatura especializada en la materia que los principales elementos de información que requiere conocer un cibercriminal son: las vulnerabilidades a las que ha sido objeto el sistema o institución, la arquitectura de los sistemas, sus especificaciones técnicas, horarios de operación, funcionalidad general, protocolos de comunicación, aspectos de seguridad informática instrumentados, entre otros, para descubrir y aprovechar los puntos débiles que pudieran existir en estos elementos y atacar a los sistemas.

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

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

Esta serie de ataques se encuentra en una fase avanzada por lo cual es totalmente demostrable que divulgar la información en comento permitiría a los delincuentes o grupos delictivos llevar a cabo ciberataques focalizados que pudieran dañar de forma más severa las IMF, entre ellas, el SPID del cual depende el sistema financiero mexicano.

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

En relación con lo anterior, es importante señalar que México ocupa el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica 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. Por lo anterior, este Instituto Central y autoridades como la Secretaría de Hacienda y Crédito Público 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 , el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada;

ii) El ataque del ransomware de WannaCry, que aprovechó una vulnerabilidad inherente de Microsoft Windows, para cifrar la información contenida en las máquinas y exigir el pago de un “rescate” para devolver el contenido a su forma original, el cual interrumpió significativamente la operación rutinaria de varias instituciones comerciales y gubernamentales, incluidas Fedex, Deutsche Bahn, Megafon, Telefónica, el Banco Central de Rusia, Ferrocarriles de Rusia y el Ministerio del Interior de Rusia;

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;

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;

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;

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;

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;

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.

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. O como el caso del Banco del Austro en Ecuador, en el que los atacantes utilizaron un método muy similar al de Bangladesh, para robar 12 millones de dólares. Respecto de lo anterior, a la fecha SWIFT continúa siendo objeto de ataques por diferentes grupos de delincuentes informáticos, y expertos en seguridad informática consideran que este tipo de actividades es susceptible de expandirse a otros servicios y sistemas financieros.

x) El ataque ocurrido a las instituciones financieras participantes del SPEI, el cual consistió en la alteración de sus aplicativos para conectarse a esta IMF, mediante código malicioso, el cual distribuyó dinero desde las cuentas concentradoras de los participantes a cuentas de usuarios específicas, los cuales fueron utilizados como “mulas” para la extracción del dinero. 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.

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.

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.

Por lo anterior, los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar cualquier información que potencialice la materialización de un riesgo de ciberseguridad, en el entendido de que dicha información, al estar en malas manos, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central de la Nación, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

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

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

Adicionalmente, una disrupción en los servicios provistos por los participantes del SPID, producto de un ataque contra estos o sus tecnologías de la información y de comunicaciones, tendría repercusiones directas para una gran cantidad de empresas y comercios, cuyas obligaciones a cubrir a través de pagos electrónicos interbancarios se verían afectadas durante el tiempo de la interrupción de estos servicios. Asimismo, la población en general que utiliza estos medio de pago,

vería afectada su capacidad para realizar o cumplir con el pago de bienes y servicios, y las instituciones bancarias y no bancarias participantes del SPID, 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.

Por lo anterior, un ataque informático perpetrado derivado de la divulgación de la información referida representa un perjuicio significativo para el sistema financiero del país y para los usuarios de los servicios de transferencias electrónicas interbancarias en dólares, pues de acuerdo con la información del Banco de México, de julio de 2017 a junio de 2018, se realizaron aproximadamente 2 millones de pagos electrónicos interbancarios en dólares por un monto de 234 mil millones de pesos.

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

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

En efecto, la información clasificada referida tiene como finalidad que el Banco de México pueda cumplir con las funciones que les fueron encomendadas en el texto constitucional, pues este Instituto Central tiene como función la de regular la intermediación y los servicios financieros, en términos del artículo 28, párrafo séptimo, de la Constitución, dentro de los cuales se encuentran los sistemas de pagos, incluido el SPID, pues así lo dispone el artículo 10 de la Ley del Sistema de Pagos.

En segundo lugar, la medida es idónea pues el fin constitucional de proteger el cumplimiento de las funciones constitucionales del Banco de México se protege a través de la clasificación pues, de otro modo, personas o grupos delictivos contarían con la información necesaria y suficiente para perpetrar un ataque en contra de las IMF con las que opera el Banco de México, generando así distorsiones en la estabilidad de los mercados financieros; o bien, el incumplimiento de las obligaciones de un participante en el sistema de pagos, dando lugar a que otros participantes

incumplan, a su vez, con sus respectivas obligaciones afectando al sistema financiero, o generando irregularidades en los sistemas de pagos.

En tercer lugar, reservar la información referida representa el medio menos restrictivo disponible para evitar el perjuicio, en aras de 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 Ley, tal y como se demostró en el presente caso.

En cuarto lugar, la divulgación de la información, no aporta un beneficio mayor a la transparencia y rendición de cuentas que sea comparable con el perjuicio que implicaría el hecho de los efectos derivados de dicha divulgación, pues ello permitiría a personas o grupos con intenciones delictivas planear y perpetrar ataques cibernéticos dirigidos específicamente a alguno de los participantes del SPID o alguna de las IMF administradas y operadas por el Banco de México, los cuales tendrían como resultado el acceso indebido, la substracción de información -como datos personales referente a sus usuarios y las operaciones que realizan-, la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios proporcionados por los participantes o las IMF. En este sentido, el riesgo de perjuicio antes señalado supera claramente el interés general de que se difunda la información.

Finalmente, la limitación se adecua al principio de proporcionalidad, toda vez que debe prevalecer el interés que más beneficie a la colectividad, y como se ha dicho, reservar la "***Información relacionada con la seguridad informática que soporta el funcionamiento de los sistemas de pagos"*** evitará poner en riesgo el buen funcionamiento de los sistemas de pagos, del sistema financiero y de la economía nacional en su conjunto, lo cual sería claramente mayor al beneficio del interés que pudiera existir en proporcionar dicha información.

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; 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, 20, del Reglamento Interior del Banco de México; Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como, Primero, Cuarto, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I, II y IV, de los Lineamientos, se clasifica como reservada la "***Información relacionada con la seguridad informática que soporta el funcionamiento de los sistemas de pagos"*** por el plazo de 5 años a partir de la fecha de clasificación, toda vez que es muy probable que se siga operando bajo las directrices y lineamientos establecidos en el documento que se clasifica, y así se podrían evitar intrusiones que puedan inhabilitar los sistemas de tecnologías de la información y comunicaciones, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques informáticos, no solo de las vulnerabilidades identificadas sino de aquellas que no se encuentran reconocidas provocando afectaciones a las infraestructuras de los mercados financieros que opera y administra este Instituto

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

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

BANCO DE MÉXICO

REFERENCIA 2

Order Code RL32331

CRS Report for Congress
Received through the CRS Web

The Economic Impact of Cyber-Attacks

April 1, 2004

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

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

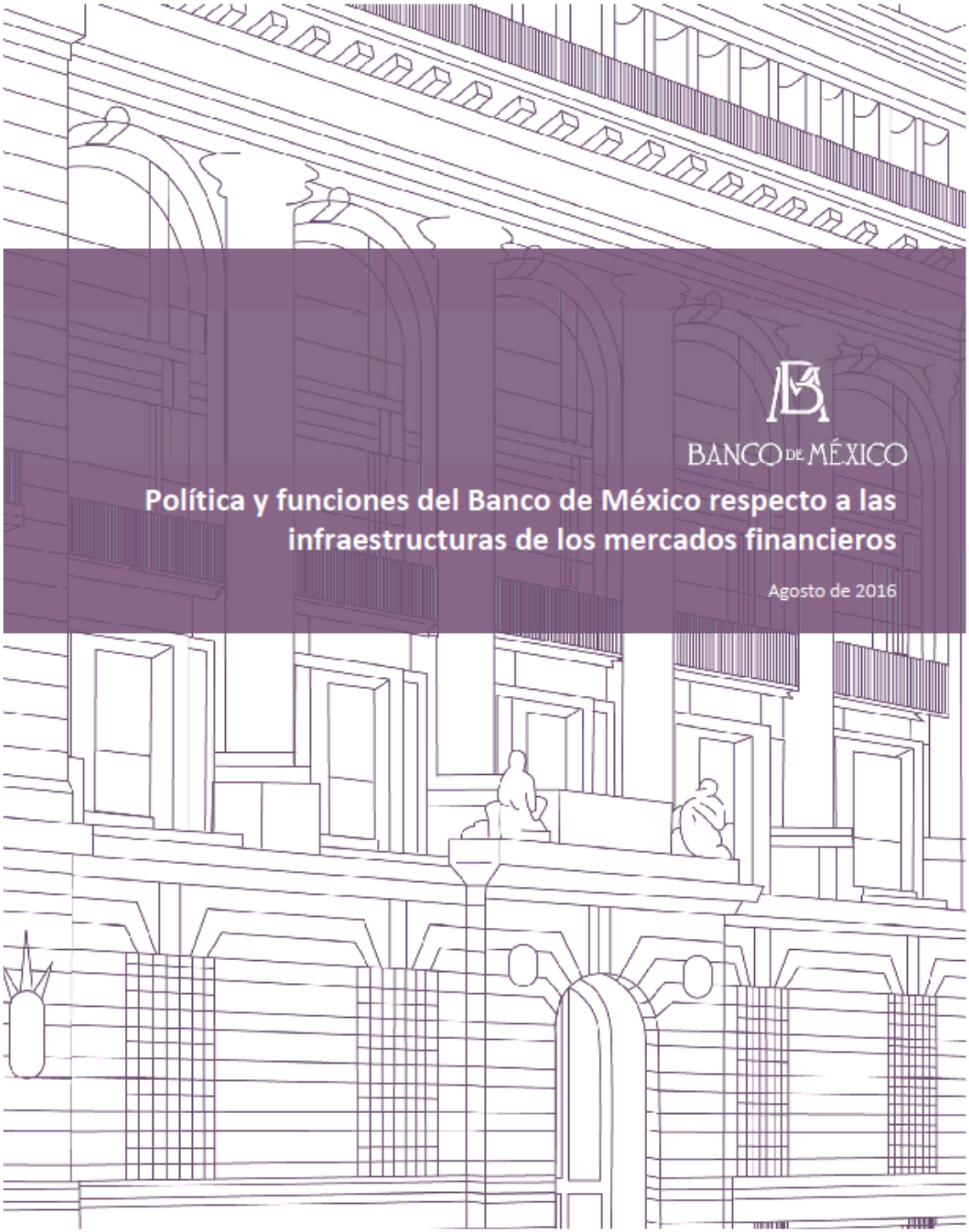
Informe Norton sobre Ciberseguridad 2016

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

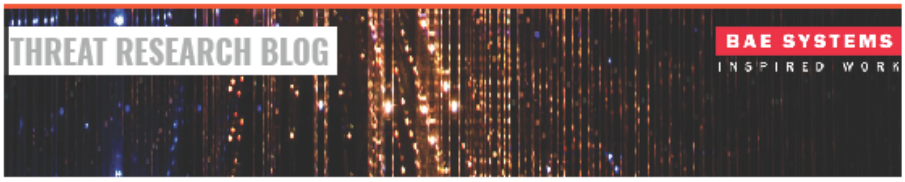
Más golliana@gmail.com Escritorio Cerrar sesión

BAE SYSTEMS THREAT RESEARCH BLOG

Resources Contact us

Home Products Solutions News & Events Partners About Us Careers

SEARCH



Home » Threat Research » Lazarus & Watering-hole attacks

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

LAZARUS & WATERING-HOLE ATTACKS

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

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

ANALYSIS

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

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

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin.

Sign up

POPULAR POSTS


TWO BYTES TO $951M


WANACRYPTOR RANSOMWORM


CYBER HEIST ATTRIBUTION

CONTACT

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

learn@baesystems.com

Contact

REFERENCIA 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.

BANCO DE MÉXICO

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?ln=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, 8:00am ET

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

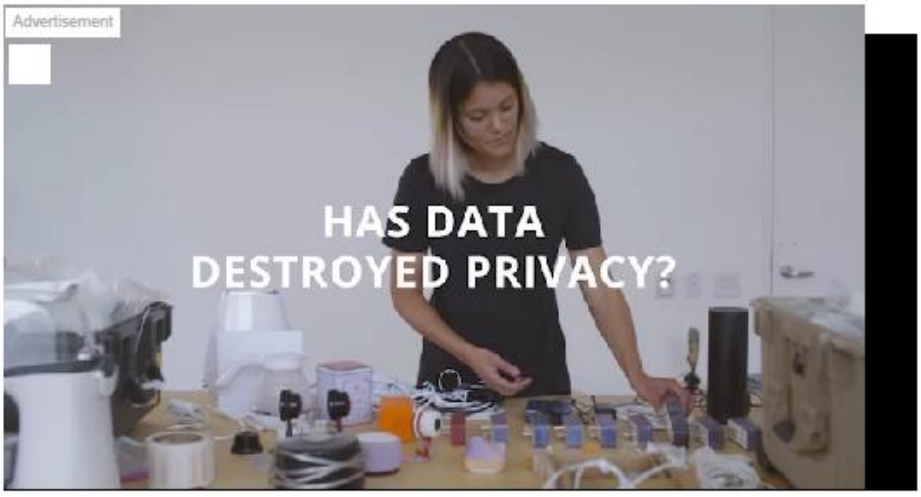
REFERENCIA 16

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 Yanquen*

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

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

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

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

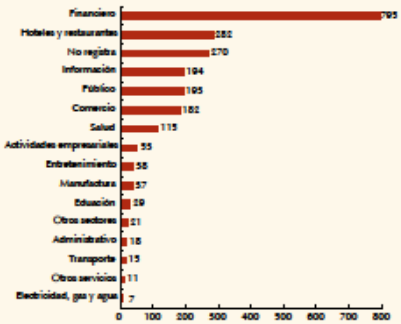
* Los autores pertenecen al Departamento de Estabilidad Financiera del Banco de la República. Sus opiniones no comprometen al Banco de la República ni a su Junta Directiva. Los errores u omisiones que persistan son responsabilidad exclusiva de los autores.

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

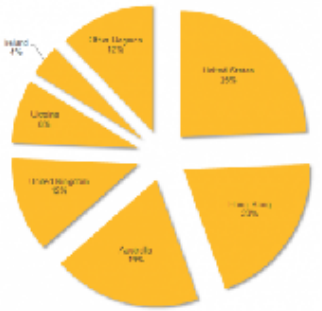
News

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.

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



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

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

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

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

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

REFERENCIA 19

BANCO DE MÉXICO

REFERENCIA 20

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.**

Página 1 de 3

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, 16:34

REFERENCIA 22

+2
2 Votes

Social Engineering Fundamentals, Part I: Hacker Tactics

By: ()

Created 18 Dec 2001 | 0 Comments

0 0

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

(/connect/forward?path=node/1236241) Like 2

by Sarah Granger

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

A True Story

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

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

BANCO DE MÉXICO

REFERENCIA 23

WaterISAC
Security Information Center

10 Basic Cybersecurity Measures

Best Practices to Reduce Exploitable Weaknesses and Attacks

June 2015

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

BANCO DE MÉXICO

REFERENCIA 24

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real.

Fecha de consulta: 20/07/2018 01:35:09

Título	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios en Dólares SPID®, Número de operaciones	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios en Dólares SPID®, Importe (millones de dólares)
Periodo disponible	Jul 2017 - Jun 2018	Jul 2017 - Jun 2018
Periodicidad	Mensual	Mensual
Cifra	Volumen	Flujos
Unidad	Operaciones	Millones de Dólares
Base		
Aviso		
Tipo de información	Niveles	Niveles
Fecha	**SF309374**	**SF309375**
Jul 2017	132,275.00	11,309.4
Ago 2017	155,260.00	11,817.0
Sep 2017	147,745.00	10,970.9
Oct 2017	164,888.00	18,997.8
Nov 2017	167,074.00	25,110.0
Dic 2017	160,109.00	21,774.8
Ene 2018	163,138.00	22,218.0
Feb 2018	157,298.00	18,199.0
Mar 2018	172,945.00	19,778.6
Abr 2018	181,715.00	28,874.0
May 2018	162,278.00	15,336.7
Jun 2018	164,315.00	30,129.2

ANEXO "F"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: CTC-BM-24183

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

RESULTANDO

PRIMERO. Que el tres de julio de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **CTC-BM-24183,** la cual se transcribe a continuación:

> *"Solicito por favor el documento: Guía para elaborar la certificación de requisitos de seguridad informática y gestión de riesgo operacional de participantes y potenciales participantes al SPID"*

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

TERCERO. Que la Dirección de Sistemas de Pagos del Banco de México, mediante oficio de veinte de julio de dos mil dieciocho, informó a este Comité de Transparencia que han determinado clasificar la información solicitada como información reservada, respecto del cual se elaboró la correspondiente prueba de daño, y solicitó a este órgano colegiado confirmar tal clasificación.

CONSIDERANDO

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

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

Este órgano colegiado advierte que es procedente la clasificación como reservado de la totalidad del documento señalado en el oficio en comento, al tratarse de: *"Información relacionada con la seguridad informática que soporta el funcionamiento de los sistemas de pagos"* toda vez que se ubica en los supuestos de reserva previstos en los artículos 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 y Vigésimo segundo, fracciones I, II y IV, de los Lineamientos, ya

que su divulgación puede menoscabar la efectividad de las medidas implementadas en relación con las políticas en materia del sistema financiero del país, y ponga en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; comprometer las acciones encaminadas a propiciar el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos; y generar el incumplimiento de las obligaciones de un participante en un sistema de pagos que dé lugar a que otros participantes incumplan, a su vez, con sus respectivas obligaciones y pueda afectar al sistema financiero.

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

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

RESUELVE

ÚNICO. Se **confirma la clasificación de la información referida como reservada,** conforme a la fundamentación y motivación expresadas en la correspondiente prueba de daño, señalada en el oficio precisado en la sección de resultandos de la presente determinación, en los términos del considerando Segundo.

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

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente