BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ORDINARIA 29/2017
DEL 26 DE OCTUBRE DE 2017

En la Ciudad de México, a las doce horas del veintiséis de octubre de dos mil diecisiete, en la Sala de Juntas del tercer piso del edificio ubicado en avenida Cinco de Mayo, número seis, colonia Centro, delegación Cuauhtémoc, se reunieron Claudia Álvarez Toca, Directora de la Unidad de Transparencia, y Abdón Sánchez Arroyo, Director de Coordinación de la Información, 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 XIII, 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, quien fungió como 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 64, párrafos segundo y tercero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 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 de ese órgano colegiado el documento que contiene el orden del día.----------
Este Comité de Transparencia del Banco de México, con fundamento en los artículos 4o. y 31, fracción XIV, del Reglamento Interior del Banco de México; 43, párrafo segundo, y 44, fracción IX, de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafo segundo, y 65, fracción IX, de la Ley Federal de Transparencia y Acceso a la Información Pública 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 LA CLASIFICACIÓN REALIZADA POR EL GERENTE DE POLÍTICA Y VIGILANCIA DE LOS SISTEMAS DE PAGOS, EN SUPLENCIA POR AUSENCIA DEL DIRECTOR DE SISTEMAS DE PAGOS DEL BANCO DE MÉXICO, Y APROBACIÓN DE LAS VERSIONES

BANCO DE MÉXICO

PÚBLICAS RELACIONADAS CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO CTC-BM-20783.----------

El Prosecretario dio lectura al oficio de veinte de octubre de dos mil diecisiete, suscrito por el Gerente de Política y Vigilancia de los Sistemas de Pagos, en suplencia por ausencia del Director de Sistemas de Pagos del Banco de México, que se agrega a la presente acta como **ANEXO "C"**, por medio del cual dicha unidad administrativa solicitó a este órgano colegiado confirmar la clasificación de la información y aprobar las versiones públicas materia de la solicitud de acceso a la información identificadas con el número de folio **CTC-BM-20783**, en virtud de los motivos expuestos en el citado oficio.----------

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 1o., 23, 43, 44, fracción II, 106, fracción I, y 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, 65, fracción II, 98, fracción I, y 140, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción II, del Reglamento Interior del Banco de México, y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, resolvió confirmar la clasificación de la información realizada por el Gerente de Política y Vigilancia de los Sistemas de Pagos, en suplencia por ausencia del Director de Sistemas de Pagos del Banco de México, mediante la elaboración de las versiones públicas a que se refiere el oficio de veinte de octubre de dos mil diecisiete, relacionado con la solicitud de acceso a la información con folio **CTC-BM-20783,** y aprobó las versiones públicas respectivas, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "D".**----------

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN REALIZADA POR EL GERENTE DE POLÍTICA Y VIGILANCIA DE LOS SISTEMAS DE PAGOS, EN SUPLENCIA POR AUSENCIA DEL DIRECTOR DE SISTEMAS DE PAGOS DEL BANCO DE MÉXICO, Y APROBACIÓN DE LA VERSIÓN PÚBLICA RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO CTC-BM-20852.----------

El Prosecretario dio lectura al oficio de fecha veinte de octubre de dos mil diecisiete, suscrito por el Gerente de Política y Vigilancia de los Sistemas de Pagos, en suplencia por ausencia del Director de Sistemas de Pagos del Banco de México, que se agrega a la presente acta como **ANEXO "E"**, por medio del cual dicha unidad administrativa solicitó a este Comité de Transparencia confirmar la clasificación de la documentación y aprobar la versión pública materia de la solicitud de acceso a la información identificada con el número de folio **CTC-BM-20852,** por los motivos expuestos en el oficio referido.----------

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

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1o., 23, 43, 44, fracción II, 106, fracción I, y 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, 65, fracción II, 98, fracción I, y 140, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción II, del Reglamento Interior del Banco de México, y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, resolvió confirmar la clasificación de la información realizada por el Gerente de Política y Vigilancia de los Sistemas de Pagos, en

BANCO DE MÉXICO

suplencia por ausencia del Director de Sistemas de Pagos del Banco de México, mediante la elaboración de la versión pública a que se refiere el oficio de veinte de octubre de dos mil diecisiete, relacionado con la solicitud de acceso a la información con folio **CTC-BM-20852,** y aprobó la versión pública respectiva, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "F",** lo anterior, en atención a las causas que dieron lugar a la previa clasificación de la información confirmada por el Comité de Transparencia en esta misma sesión, señalada en el punto **"PRIMERO"** la cual se detalla, fundamenta y motiva en la prueba de daño que en su momento fue exhibida, correspondiente al "Manual de Operación del SPEI® versión 5.0". ----------

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 del Comité de Transparencia que asistieron a la sesión, así como por su Prosecretario. Conste.----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

ABDÓN SÁNCHEZ ARROYO
Integrante

SERGIO ZAMBRANO HERRERA
Prosecretario

BANCO DE MÉXICO

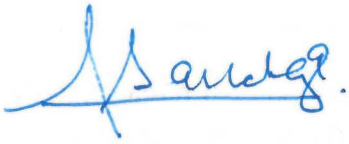
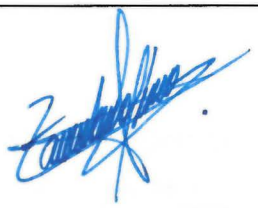
ANEXO "A"

LISTA DE ASISTENCIA

SESIÓN ORDINARIA 29/2017

26 DE OCTUBRE DE 2017

COMITÉ DE TRANSPARENCIA

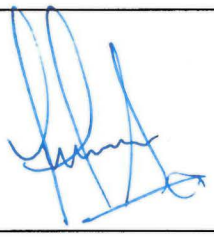
MTRA. CLAUDIA ÁLVAREZ TOCA Directora de la Unidad de Transparencia Integrante	
DR. ABDÓN SÁNCHEZ ARROYO Director de Coordinación de la Información Integrante	
LIC. SERGIO ZAMBRANO HERRERA Prosecretario del Comité de Transparencia	

INVITADOS PERMANENTES

MTRO. OSCAR JORGE DURÁN DÍAZ Director de Vinculación Institucional	
DR. FRANCISCO CHAMÚ MORALES Director de Administración de Riesgos	

INVITADOS

LIC. MARÍA DEL CARMEN REY CABARCOS Gerente de Riesgos No Financieros	
LIC. RODRIGO MÉNDEZ PRECIADO Abogado Especialista en la Dirección General de Relaciones Institucionales	
DR. OTHÓN MARTINO MORENO GONZÁLEZ Gerente de Política y Vigilancia de los Sistemas de Pagos	

LIC. EDUARDO TEJEDA DOMÍNGUEZ Subgerente de Continuidad de la Operación de Sistemas de Pagos	
MTRA. LILIANA GARCÍA OCHOA Líder de Especialidad de la Gerencia de Estudios de Sistemas de Pagos	
LIC. XIMENA AIDEE DOMÍNGUEZ HERNÁNDEZ Investigador	
LIC. HÉCTOR GARCÍA MONDRAGÓN Líder de Especialidad en la Subgerencia de Análisis Jurídico y Promoción de Transparencia	

ANEXO "B"

BANCO DE MÉXICO

Comité de Transparencia

ORDEN DEL DÍA
Sesión 29/2017
26 de octubre de 2017

PRIMERO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN REALIZADA POR EL GERENTE DE POLÍTICA Y VIGILANCIA DE LOS SISTEMAS DE PAGOS, EN SUPLENCIA POR AUSENCIA DEL DIRECTOR DE SISTEMAS DE PAGOS DEL BANCO DE MÉXICO, Y APROBACIÓN DE LAS VERSIONES PÚBLICAS RELACIONADAS CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO CTC-BM-20783.

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN REALIZADA POR EL GERENTE DE POLÍTICA Y VIGILANCIA DE LOS SISTEMAS DE PAGOS, EN SUPLENCIA POR AUSENCIA DEL DIRECTOR DE SISTEMAS DE PAGOS DEL BANCO DE MÉXICO, Y APROBACIÓN DE LA VERSIÓN PÚBLICA RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO CTC-BM-20852.

ANEXO "C"

BANCO DE MÉXICO

"Año del Centenario de la Promulgación de la Constitución Política de los Estados Unidos Mexicanos"

BANCO DE MÉXICO
RECIBIDO
20 OCT 2017
Comité de Transparencia
Por: 215383 Hora: 13:41

se recibe oficio constante de dos páginas, dos carátulas y una prueba de daño.----

REF.: D10/214/2017

Ciudad de México, a 20 de octubre de 2017

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
PRESENTE

Me refiero a la solicitud de acceso a la información identificada con el número de folio **CTC-BM-20783,** que nos turnó la Unidad de Transparencia el dieciocho de septiembre del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, que se transcribe a continuación:

> *"Por medio del presente solicito por favor sea enviado o permita el acceso a los manuales: spei y spid última versión.*
>
> *Gracias"*

Sobre el particular, con fundamento en los artículos 100, 106, fracción I y 111, de la Ley General de Transparencia y Acceso a la Información Pública, 97, 98, fracción I y 108, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" (Lineamientos), vigentes, me permito informarles que esta unidad administrativa ha determinado clasificar diversa información contenida en los documentos que se indican más adelante.

En consecuencia, esta área ha generado las versiones públicas respectivas, junto con las carátulas que las distinguen e indican los datos concretos que han sido clasificados, al igual que los motivos y fundamentos respectivos. Asimismo, se ha elaborado la correspondiente prueba de daño, que se adjunta al presente. Dichos documentos se encuentran disponibles a partir de esta fecha en la carpeta compartida ubicada en la red interna del Banco de México, a la que se puede acceder a través de la siguiente liga:

I:\A13 Dir Unidad de Transparencia\Comité de Transparencia Compartida\2017\Sesiones Ordinarias 2017\Asuntos para sesión

Para facilitar su identificación, en el siguiente cuadro encontrarán el detalle de los títulos de los documentos clasificados, los cuales coinciden con los que aparecen en las carátulas que debidamente firmadas se acompañan al presente. Asimismo, en dicho cuadro encontrarán las ligas respectivas al repositorio institucional en el que residen las versiones digitalizadas de cada uno de los documentos originales respecto de los cuales se elaboraron las versiones públicas.

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXO	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)
Manual de Operación del SPEI® versión 5.0	1	2	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Sistemas%20de%20pagos/Web%20Externo/Manuales/SPEI-MANUAL_Ver-5_0.pdf
Manual de Operación del Sistema de Pagos Interbancarios en Dólares (SPID) Versión 3.1	3	2	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Sistemas%20de%20pagos/Web%20Externo/Manuales/SPID-MANUALv3_1.pdf

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 II, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto y Sexagésimo segundo, de los Lineamientos, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de la información realizada por esta unidad administrativa, y aprobar las versiones públicas señaladas en el cuadro precedente.

Asimismo, de conformidad con el Décimo de los señalados Lineamientos, informo que el personal que por la naturaleza de sus atribuciones tiene acceso a los referidos documentos clasificados es el adscrito a la Dirección de Sistemas de Pagos.

ATENTAMENTE,

DR. OTHÓN MARTINO MORENO GONZÁLEZ

GERENTE DE POLÍTICA Y VIGILANCIA DE LOS SISTEMAS DE PAGOS

En conformidad con lo establecido en el Art. 66 del Reglamento Interior del Banco de México

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

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

Versión Pública		
I.	Área titular que clasifica la información	Dirección de Sistemas de Pagos
II.	La identificación del documento del que se elabora la versión pública.	Manual de Operación del SPEI® versión 5.0
III.	Firma del titular del área y de quien clasifica.	**Dr. Othón Martino Moreno González** Gerente de Política y Vigilancia de los Sistemas de Pagos En conformidad con lo establecido en el Art. 66 del Reglamento Interior del Banco de México
IV.	Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia "Ordinaria", número 29/2017, celebrada el 26 de octubre de 2017. Secretaría del Comité de Transparencia Sergio Zamarano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: cinco años				
Ref.	**Pág.**	**Información testada**	**Fundamento Legal**	**Motivación**
1	Primera y segunda páginas del histórico de revisiones Tercera, cuarta, sexta, séptima, octava, novena, y décima páginas del índice.	Información relacionada con esquemas de operación formato de mensajes y protocolos de comunicación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
2	1, 2	Información relacionada con especificaciones técnicas y esquemas de operación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
3	4, 5	Información relacionada con el procesamiento de órdenes de transferencia y traspasos	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
4	5	Información relacionada con el procesamiento de órdenes de transferencia y traspasos así como horarios de operación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
5	6, 7	Información relacionada con órdenes de transferencia y traspasos.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
6	7 a la 13	Información relacionada con la funcionalidad general, formatos de	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país

		mensajes y protocolos de comunicación.		y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
7	14	Información relacionada con la funcionalidad general, formatos de mensajes, protocolos de comunicación, órdenes de transferencia y traspasos.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
8	15 a la 17	Información relacionada con la funcionalidad general, formatos de mensajes y protocolos de comunicación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
9	18, 19	Información relacionada con procedimientos continuidad operativa y de contingencia, y protocolos de comunicación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
10	19,20,22	Información relacionada con la funcionalidad general y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
11	23 al 26	Información relacionada con especificaciones técnicas y funcionalidad general.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
12	27	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a

				proveer el buen funcionamiento de los sistemas de pagos.
13	28 a la 33	Información relacionada con la funcionalidad general, especificaciones técnicas, protocolos de comunicación y formatos de mensajes.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
14	36 a la 125	Información relacionada con protocolos de comunicación y formato de mensajes.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
15	132 a la 164 y de 167 a la 194	Información relacionada con la funcionalidad general, especificaciones técnicas, protocolos de comunicación, órdenes de transferencia y esquemas de operación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
16	194	Información relacionada con procedimientos continuidad operativa y de contingencia.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
17	195 a la 200	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
18	201 a la 206	Información relacionada con la funcionalidad general, especificaciones técnicas, protocolos de comunicación, órdenes de transferencia y esquemas de operación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.

19	207 a la 209	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
20	210 a la 215	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
21	216	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
22	217,218	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
23	221	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
24	223 a la 265, 267	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
25	270,271 y de 278 a la 283	Información relacionada con especificaciones	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero,

		técnicas y seguridad informática.		económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
26	284,285	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
27	286 a la 288	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
28	289 a la 297	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
29	299 a la 307	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
30	308	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
31	309 a la 313	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a

				proveer el buen funcionamiento de los sistemas de pagos.
32	314,315	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
33	316, 317	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
34	318	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
35	319 a la 330	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.

PRUEBA DE DAÑO

INFORMACIÓN RELACIONADA CON HORARIOS DE OPERACIÓN, PROCESAMIENTO DE ÓRDENES DE TRANSFERENCIA Y TRASPASOS, FUNCIONALIDAD ESPECIFICA, ESPECIFICACIONES TÉCNICAS, PROTOCOLOS DE COMUNICACIÓN, FORMATOS DE MENSAJES, ESQUEMAS DE OPERACIÓN, PROCEDIMIENTOS DE CONTINUIDAD OPERATIVA Y DE CONTINGENCIA ASÍ COMO CUALQUIER OTRA INFORMACIÓN RELACIONADA CON LA SEGURIDAD INFORMÁTICA QUE SOPORTA EL FUNCIONAMIENTO DE LOS SISTEMAS DE PAGOS.

En términos de lo dispuesto por 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; así como, Vigésimo segundo, fracciones I, II, III y IV, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, debe clasificarse como información reservada, entre otra:

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

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

- Aquélla que otorgue una ventaja indebida o que genere distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pago; y

- Aquélla que 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.

Al respecto, revelar al público la información relativa a los horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de los sistemas de pagos, crearía distorsiones en los sistemas de pagos, comprometería las acciones encaminadas a propiciar el buen funcionamiento de los sistemas de pagos y podría generar el incumplimiento de obligaciones de un participante en los sistemas de pagos.

En particular, esto se debe a que esta información, en caso de divulgarse podría ser analizada y utilizada por una persona o grupo de personas malintencionadas para **perpetrar ataques cibernéticos dirigidos** específicamente a los sistemas de pagos, lo cual posibilitaría la creación de mecanismos que faciliten el acceso indebido al propio sistema, la substracción de información relativa a sus usuarios y las operaciones que realizan, **la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios de pagos electrónicos interbancarios** y, en consecuencia, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de los sistemas de pagos, crearía distorsiones en estos sistemas, comprometería las acciones encaminadas a propiciar el buen funcionamiento de los sistemas de pagos y podría generar el incumplimiento de obligaciones de un participante en los sistemas de pagos.

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

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

Al respecto, está documentado en la literatura especializada en la materia[1] que los principales elementos de información que requiere conocer un cibercriminal son: la arquitectura de los sistemas, sus especificaciones técnicas, horarios de operación, funcionalidad general, protocolos de comunicación, aspectos de seguridad informática instrumentados, entre otros, para descubrir y aprovechar los puntos débiles que pudieran existir en estos elementos y atacar a los sistemas.

Dentro de los elementos mencionados en el párrafo anterior, la información materia de la presente prueba de daño contienen **aspectos de seguridad informática**, tales como horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, por lo cual su divulgación podría habilitar un ataque al mismo.

Demostrable. Está documentado en diversos medios de comunicación, 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, lo cual es un hecho público y notorio. Las investigaciones realizadas señalan que estos ataques han sido orquestados por organizaciones criminales internacionales con herramientas y técnicas sofisticadas que, además

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

de dañar la reputación de las instituciones afectadas, han generado cuantiosas pérdidas económicas. Tal es el caso 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[2]. 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 financieros[3]. Entre otros ataques relevantes se encuentran: 1) el ataque de tipo "Whatering hole" en Polonia, que permitió utilizar un servidor de la Autoridad de Supervisión Financiera para distribuir código malicioso a más de 20 bancos polacos[4], el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada[5]; 2) el ataque del ransomware de WannaCry, cuyo código se propagó por los ordenadores de una red 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 afectó a diversos bancos en Rusia[6] y 3) 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[7]. En relación con lo anterior, es importante señalar que México ocupa el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica[8] y que tan sólo en México, el costo causado por el cibercrimen ascendió a $5,500 millones de dólares y afectó alrededor de 22.4 millones de personas, mientras que a nivel mundial, el costo ascendió a $125,900 millones de dólares y afectó a 689.4 millones de personas[9].

En este sentido, la divulgación de la información materia de la presente prueba de daño, potencializaría que hechos como los mencionados en el párrafo anterior ocurran respecto de los sistemas informáticos que opera el Banco de México, particularmente los sistemas de pagos, puesto que los cibercriminales contarían con los elementos necesarios para perpetrar un ataque a la información de este Instituto Central.

---

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

3 Antony Peyton. "Symantec reveals more hack attempts on Swift network". Banking Technology. 11 oct 2016

4 Badcyber, Author. "Several Polish Banks Hacked, Information Stolen by Unknown Attackers." BadCyber, 9 feb 2017, http://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/ consultado el 18 oct 2017.

5 Hernández, Aura. "CNBV y Nueve Bancos Han Sido Hackeados." Excélsior, Excélsior, 17 feb 2017, http://www.excelsior.com.mx/hacker/2017/02/17/1146899 consultado el 18 oct 2017.

6 Winning, Alexander, and Jack Stubbs. "WannaCry Cyber Attack Compromised Some Russian Banks: Central Bank." Reuters, Thomson Reuters, 19 may 2017, http://www.reuters.com/article/us-cyber-attack-russia-cenbank/wannacry-cyber-attack-compromised-some-russian-banks-central-bank-idUSKCN18F16V consultado el 18 oct 2017.

7 Palazuelos, Félix. "Petya, un virus más peligroso y sofisticado que WannaCry" El País, elpais.com, 29 jun 2017, https://elpais.com/tecnologia/2017/06/28/actualidad/1498639459_556568.html consultado el 18 oct 2017.

8 Arreola Javier. "Ciberseguridad (casi) a prueba del enemigo 'invisible'". Forbes México. http://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/ consultado el 18 de oct de 2016.

9 Informe Norton sobre Ciberseguridad 2016 - Comparaciones Globales https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf consultado el 9 de oct de 2017.

Identificable. Independientemente del origen o finalidad de un ataque contra los sistemas de pagos, las tecnologías de la información, comunicaciones o infraestructura tecnológica bajo la cual operan los sistemas de pagos, podrían resultar afectadas las órdenes de transferencia en las cuentas bancarias de los distintos participantes y usuarios de los sistemas 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 personas morales.

Adicionalmente, una disrupción en los servicios provistos por los sistemas de pagos como el Sistema de Pagos Electrónicos Interbancarios (SPEI) o el Sistema de Pagos Interbancarios en Dólares (SPID), producto de un ataque contra éstos 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, los usuarios que utilizan estos medios de pago, verían afectadas su capacidad para realizar o cumplir con el pago de bienes y servicios, y las instituciones financieras participantes en los sistemas de pagos como el SPEI o el SPID, que además de hacer uso de estos sistemas para su operación propia obtienen ingresos del cobro de comisiones por la prestación de los servicio de pagos que ofrecen estos sistemas, también resultarían gravemente perjudicadas, lo cual provocaría una seria afectación al sistema financiero.

Por lo anterior, un ataque informático a los sistema de pagos, ocasionado por dar a conocer la información relacionada con esta prueba de daño, representa un perjuicio significativo para el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias, pues de acuerdo con la información del Banco de México, en agosto 2017, se realizaron en el SPEI aproximadamente 42 millones de pagos electrónicos interbancarios por un monto de 22 mil millones de pesos[10]; lo anterior equivale a más de 6 mil operaciones por un monto de 3 mil millones de pesos por hora. Para el caso del SPID, en agosto de 2017 se realizaron aproximadamente 155 mil operaciones interbancarias en dólares entre personas morales, con un monto total transferido de aproximadamente 12 mil millones de dólares. Con base en estas cifras, es evidente que un ataque cibernético que vulnere la operación del SPEI, del SPID o sus tecnologías de la información y de comunicaciones, sin importar la duración de la disrupción, puede llegar a tener efectos cuantiosos sobre la actividad económica del país e incluso en actividad económica que forma parte de cadenas productivas globales, así como 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.

---

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

En consecuencia, proporcionar la información reservada motivo de esta prueba de daño, no aporta un beneficio al particular que sea comparable con el perjuicio que implicaría el hecho de divulgar información que en un momento dado, permita planear y perpetrar ataques cibernéticos dirigidos específicamente al SPEI, al SPID o a cualquier otro sistema de pagos administrado por este Instituto Central así como a la infraestructura relacionada con éstos, los cuales tengan como resultado la creación de mecanismos que faciliten el acceso indebido, la substracción de información 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 estos sistema de pagos. En este sentido, el riesgo de perjuicio antes señalado supera claramente el interés particular del solicitante, incluso el general de que se difunda la información solicitada.

Por otra parte, la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, toda vez que en todo momento debe prevalecer el interés público sobre el interés particular, y como se ha dicho, la reserva de la información en comento evitará poner en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, así como también podría prevenir un daño en el buen funcionamiento de los sistemas de pagos, la creación de distorsiones en los sistemas de pagos, que se comprometan las acciones encaminadas a propiciar el buen funcionamiento del sistema de pagos, al igual que podría evitar la generación del incumplimiento de obligaciones de un participante en los sistemas de pagos.

Dicha determinación es además proporcional considerando que, como se ha explicado, dar a conocer la información reservada materia de esta prueba de daño generaría un riesgo o daño de perjuicio significativo, el cual sería claramente mayor al beneficio particular que pudiera existir al dar a conocer dicha información.

En este orden de ideas, la reserva de la información referente a horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, resulta el medio menos restrictivo disponible para evitar el perjuicio señalado anteriormente. Por ello, se considera que dicha reserva deberá mantenerse por un plazo de cinco años, a partir de la fecha de clasificación, en razón de que la operación de los sistemas de pagos no tiene una fecha establecida de conclusión.

La referida reserva, evitaría, como se ha explicado, poner en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, así como también podría prevenir un daño en el buen funcionamiento de los sistemas de pagos, la creación de distorsiones en estos sistemas de pagos, que se comprometan las acciones encaminadas a propiciar el buen funcionamiento de éstos sistema de pagos, al igual que podría evitar la generación del incumplimiento de obligaciones de un participante en los sistemas de pagos.

Por lo expuesto, 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; 100, 103, 104, 105, 106, fracción I, 108, último párrafo, 109, 113, fracción IV, y 114 de la Ley General de Transparencia y Acceso a la Información Pública; 97, 98, fracción I, 100, 103, 104, 105, último párrafo, 106, 110, fracción IV, y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública; 1o., 2o. y 3o., fracción I, de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, 20, fracciones II, IV, V, VI, IX y XVI, del Reglamento Interior del Banco de México; Segundo, fracción VIII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, así como, Primero, Segundo, fracción XIII, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I, II, III y IV de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, se ha determinado clasificar como información reservada la relacionada con horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, materia de esta prueba de daño, en virtud de que su divulgación pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, y comprometería las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.

Dr. Othón Martino Moreno González
Gerente de Política y Vigilancia de los Sistemas de Pagos
De conformidad con el Art. 66 del Reglamento Interior del Banco de México

United States Government Accountability Office

GAO

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

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

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

David A. Powner, Director
Information Technology Management Issues

GAO-10-230T

REFERENCIA 2

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

by **Michael Riley** and **Alan Katz**
2016 MDS 26 08:36 GMT-5
Updated on 2016 MDS 26 15:21GMT-5

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

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.

FireEye <https://www.bloomberg.com/quote/FEYE:US>, the security firm hired by the Bangladesh bank, has been contacted by the other banks, most of which are in Southeast Asia, because of signs that hackers may have breached their networks, the person said. They include banks in the Philippines and New Zealand but not in Western Europe or the United States. There is no indication of whether money was taken.

The expansion of the investigation four months after the discovery of the Bangladesh attack, the biggest known cyber-heist in history, suggests a broad and serious campaign to breach the international financial system.

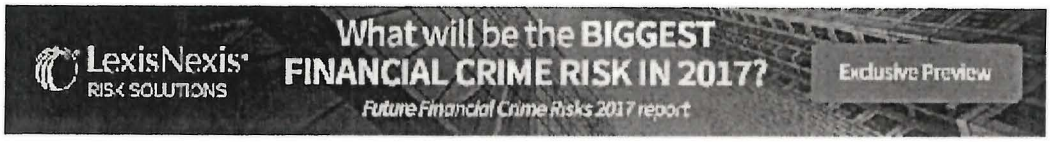
FireEye declined to comment on the report.

"The emergence of new possible instances of compromise is not entirely surprising given that banks should now be undertaking rigorous reviews of their environments," Swift said in a written statement. "Many may turn out to be false positives and or have nothing to do with Swift messages, but it is key that these reviews take place and banks' environments are secured."

For details on how Swift member banks have responded to the breaches, click here.
<http://www.bloomberg.com/news/articles/2016-05-17/global-lenders-on-edge-as-hacks-embroil-growing-list-of-banks>

The Brussels-based interbank cooperative, whose full name is the Society for Worldwide Interbank Financial Telecommunication, has warned that there may have been more breaches than the three already publicly

REFERENCIA 3



banking technology

18 May, 2017

39



tec reveals more hack attempts on Swift network

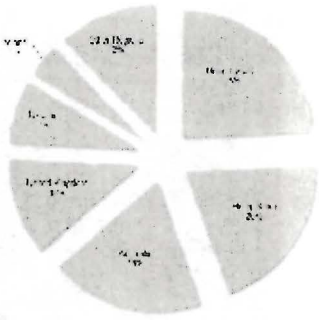
banking, 2016 Written by Antony Peyton
techno

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

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

Symantec says these Odinaff attacks are an example of another group believed to be involved in this kind of activity, following the Bangladesh central bank heist linked to the Lazarus group.

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



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

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

This is bad news for Swift but its fight back against these attacks has been extensive and ongoing. It has spoken strongly on the subject and recently unveiled SwiftSmart modules to help its customers operate their Swift environment "securely and in-line with best practice". This move is also a "critical part" of its Customer Security Programme launched in May 2016. That five-part plan was a result of various hacking incidents.

It's not just Swift

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

REFERENCIA 4

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 5

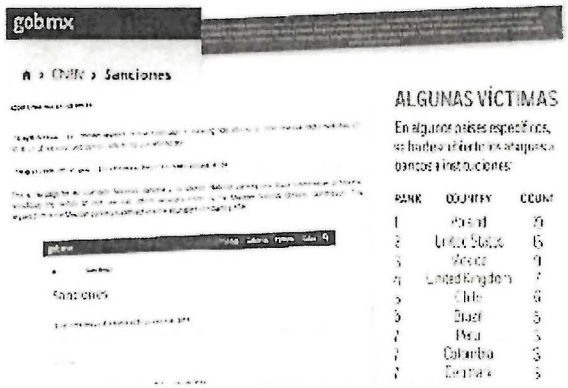


CNBV y nueve bancos han sido hackeados

Criminales han vulnerado la seguridad de instituciones financieras en México

17/02/2017 09:40 **AURA HERNÁNDEZ Y PAUL LARA**

COMPARTIR SÍGUENOS



REFERENCIA 6

REUTERS

#TECHNOLOGY NEWS
MAY 19, 2017 / 6:09 AM / 5 MONTHS AGO

WannaCry cyber attack compromised some Russian banks: central bank

Alexander Winning, Jack Stubbs

MOSCOW (Reuters) - The WannaCry ransomware attack compromised the systems of Russian banks in some isolated cases, the Russian central bank said on Friday in the first official acknowledgement by Moscow that the virus had an impact on the country's banking system.

REFERENCIA 7

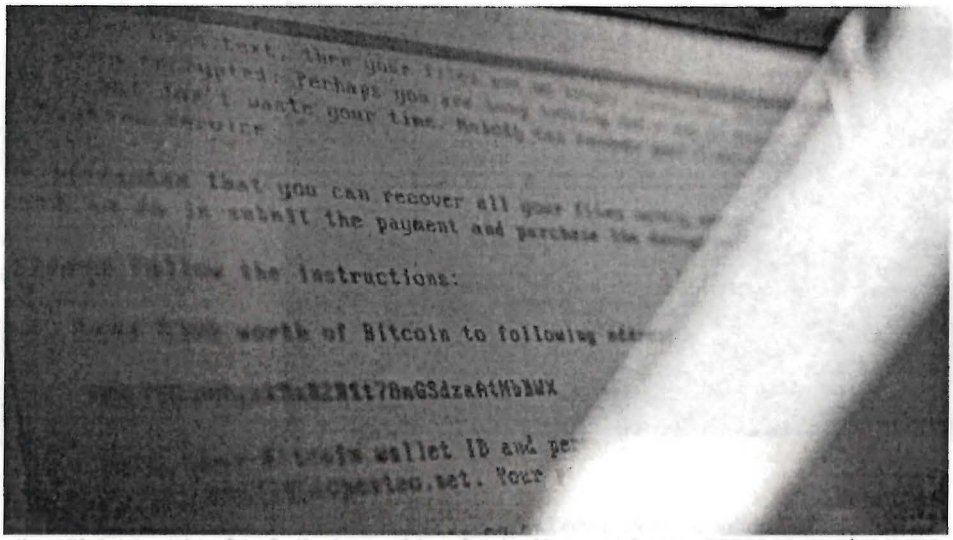
CIBERATAQUES ›

Petya, un virus más peligroso y sofisticado que WannaCry

Los expertos muestran su sorpresa por estos últimos ataques que no intentan robar y vender información pasando inadvertidos

FÉLIX PALAZUELOS

29 JUN 2017 - 09:32 CEST



Un portátil infectado con el virus Petya. En vídeo, dos especialistas analizan el posible origen del ciberataque. ROB ENGELAAR (AFP) / VÍDEO: REUTERS QUALITY

El virus Petya, que ayer afectó a grandes empresas de todo el mundo es más peligroso y sofisticado que WannaCry, aunque se base en el mismo principio de propagación masiva a través de las redes locales. "Pese a que todavía no sepamos con certeza cuál es el primer equipo infectado y cómo se infectó, sabemos que este nuevo *malware* usa la vulnerabilidad EternalBlue junto a lo que llamamos en ciberseguridad movimientos laterales", dice Sergio de los Santos, director de innovación y laboratorio en Eleven Paths, unidad especializada en ciberseguridad de Telefónica, a EL PAÍS. "Ahora no sólo busca equipos vulnerables, también emplea herramientas de administración para infectar a todos los equipos de una red si, por suerte, encuentra previamente una máquina con dichos privilegios".

No hemos aprendido pese al tirón de orejas

"Nos habíamos olvidado ya de los gusanos y los ataques informáticos siempre han estado enfocados a atacar a alguien de forma sigilosa a través de infecciones por *email* en los últimos años" señala De los Santos. "Pero no hemos aprendido pese al tirón de orejas".

REFERENCIA 8

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 @ 2:04 pm

Ciberseguridad (casi) a prueba del enemigo 'invisible'

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



Share Tweet +

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

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

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

MÁS COBERTURA



Scotiabank se une a aceleradora para impulsar su banca digital en AL (https://www.forbes.com.mx/scoti se-une-a-aceleradora-para-impulsar-su-banca-digital-en-al/)



Avianca iniciará proceso disciplinario contra pilotos en huelga (https://www.forbes.com.mx/aviar iniciara-proceso-disciplinario-contra-pilotos-en-huelga/)



Twitter endurece sus políticas contra el acoso y abuso sexual (https://www.forbes.com.mx/4012 2/)

Últimas Noticias

Tiroteo en Maryland deja 3 muerto: policía busca a sospechoso (https://www.forbes.com.mx/tirote en-maryland-deja-3-muertos-polici busca-a-sospechoso/)
OCTUBRE 18, 2017

Iberia tendrá tres vuelos semanales a Nicaragua para 2018 (https://www.forbes.com.mx/iberi tendra-tres-vuelos-semanales-a-nicaragua-para-2018/)
OCTUBRE 18, 2017

Resultados de IBM provocan apertu récord de Dow Jones (https://www.forbes.com.mx/resul de-ibm-provocan-apertura-record-dow-jones/)
OCTUBRE 18, 2017

REFERENCIA 9

Informe Norton sobre Ciberseguridad 2016

Comparaciones Globales

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

© 2016 Symantec Corporation. Todos los derechos reservados. Symantec, el logotipo de Checkmark, Norton y Norton by Symantec son marcas comerciales o registradas por Symantec Corporation o de sus filiales en los Estados Unidos y otros países. Otros nombres pueden ser marcas comerciales de sus respectivos dueños. 10/16

Norton

REFERENCIA 10

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real.

Fecha de consulta: 18/05/2017 08:51:11

Título	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios. SPEI, Número de operaciones	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios. SPEI, Importe
Periodo disponible	Ene 1992 - Abr 2017	Ene 1992 - Abr 2017
Periodicidad	Mensual	Mensual
Cifra	Volumen	Flujos
Unidad	Operaciones	Millones de Pesos
Base		
Aviso		
Tipo de información	Niveles	Niveles
Fecha	SF46188	SF46189
Ene 2017	35,016,703	23,877,271
Feb 2017	34,817,472	21,505,024
Mar 2017	40,016,546	26,180,217
Abr 2017	35,954,794	20,494,020

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

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

Versión Pública		
I.	Área titular que clasifica la información	Dirección de Sistemas de Pagos
II.	La identificación del documento del que se elabora la versión pública.	Manual de Operación del SPID® versión 3.1
III.	Firma del titular del área y de quien clasifica.	**Dr. Othón Martino Moreno González** Gerente de Política y Vigilancia de los Sistemas de Pagos En conformidad con lo establecido en el Art. 66 del Reglamento Interior del Banco de México
IV.	Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia "Ordinaria", número 29/2017, celebrada el 26 de octubre de 2017. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: cinco años				
Ref.	**Pág.**	**Información testada**	**Fundamento Legal**	**Motivación**
1	Tercera, cuarta y sexta página del índice.	Información relacionada con formato de mensajes y protocolos de comunicación.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
2	1,2	Información relacionada con especificaciones técnicas y esquemas de operación.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
3	4	Información relacionada con el procesamiento de órdenes de transferencia y traspasos	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
4	5	Información relacionada con el procesamiento de órdenes de transferencia y traspasos así como horarios de operación.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
5	6, 7	Información relacionada con órdenes de transferencia y traspasos.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
6	7 a la 15	Información relacionada con la funcionalidad general, formatos de mensajes y protocolos de comunicación.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a

				proveer el buen funcionamiento de los sistemas de pagos.
7	17	Información relacionada con la funcionalidad general, formatos de mensajes, protocolos de comunicación, órdenes de transferencia y traspasos.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
8	18,19	Información relacionada con la funcionalidad general, formatos de mensajes y protocolos de comunicación.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
9	19	Información relacionada con procedimientos continuidad operativa y de contingencia.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
10	21	Información relacionada con la funcionalidad general y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
11	22 a la 25	Información relacionada con especificaciones técnicas y funcionalidad general.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
12	25,26	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.

13	26	Información relacionada con la funcionalidad general, especificaciones técnicas, protocolos de comunicación y formatos de mensajes.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
14	26 a la 28	Información relacionada con protocolos de comunicación y formato de mensajes.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
15	28	Información relacionada con la funcionalidad general, especificaciones técnicas, protocolos de comunicación, órdenes de transferencia y esquemas de operación.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
16	29,30	Información relacionada con procedimientos continuidad operativa y de contingencia.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
17	30	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
18	30,31	Información relacionada con la funcionalidad general, especificaciones técnicas, protocolos de comunicación, órdenes de transferencia y esquemas de operación.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
19	34 a la 69	Información relacionada con especificaciones	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero,

		técnicas y seguridad informática.		económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
20	70 a la 94	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
21	95 a la 100	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
22	103 a la 110	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
23	111	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
25	118 a la 126	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
26	128,130 y 137 a la 175	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a

				proveer el buen funcionamiento de los sistemas de pagos.
27	179	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
28	181	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
29	182	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
30	183,184	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
31	185 a la 187	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
32	188 a la 193	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.

33	194,195	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
34	199 a la 234	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
35	236	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño.	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.

ANEXO "D"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: CTC-BM-20783

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

RESULTANDO

PRIMERO. El dieciocho de septiembre de dos mil diecisiete, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **CTC-BM-20783**, que se transcribe a continuación:

> *"Por medio del presente solicito por favor sea enviado o permita el acceso a los manuales: spei y spid última versión.*
> *Gracias"*

SEGUNDO. El mismo dieciocho de septiembre de dos mil diecisiete, la Unidad de Transparencia de este Instituto Central remitió a la Dirección de Sistemas de Pagos del Banco de México, para su atención, 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. Mediante oficio con referencia D01 C299/2017, del dos de octubre del presente año, la Dirección de Sistemas de Pagos del Banco de México, solicitó a este órgano colegiado la confirmación de la ampliación del plazo de respuesta a la solicitud que nos ocupa.

CUARTO. Por resolución del once de octubre del presente año, este Comité de Transparencia confirmó la determinación de ampliación del plazo de respuesta referida en el resultando anterior, misma que fue notificada al solicitante dentro del plazo de veinte días, contados a partir del siguiente a la presentación de su solicitud.

QUINTO. El Gerente de Política y Vigilancia de los Sistemas de Pagos, en suplencia por ausencia del Director de Sistemas de Pagos, mediante oficio con referencia D10/214/2017, del veinte de octubre de dos mil diecisiete, informó a este Comité de Transparencia que ha determinado clasificar diversa información contenida en los documentos señalados en el referido oficio, respecto del cual generó las versiones públicas respectivas, adjuntó la correspondiente prueba de daño, y solicitó a este Comité confirmar tal clasificación y aprobar las citadas versiones públicas.

CONSIDERANDOS

PRIMERO. Este Comité de Transparencia es competente para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas del

Banco de México, de conformidad con lo previsto en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México, así como para aprobar las versiones públicas que las unidades administrativas del referido Instituto Central sometan a su consideración, en términos del Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes.

SEGUNDO. Enseguida se analiza la clasificación realizada por la Gerencia de Política y Vigilancia de los Sistemas de Pagos, adscrita a la Dirección de Sistemas de Pagos del Banco de México, a través de las versiones publicas señalas en el referido oficio y de la prueba de daño que exhibió en el mismo.

Al respecto, este órgano colegiado advierte que se trata de información reservada los datos testados en las dos versiones públicas de los documentos identificados en el oficio señalado en el resultando Quinto de la presente resolución, los cuales se detallan, fundamentan y motivan en el cuadro identificado con la leyenda "PARTES O SECCIONES CLASIFICADAS COMO RESERVADA", en cada una de las referidas versiones públicas, y en particular en sus correspondientes carátulas y pruebas de daño.

En este sentido, a cada una de las versiones públicas aplica la prueba de daño en la que se fundamenta y motiva dicha clasificación, así como las razones, motivos y circunstancias especiales con las que se concluye que en el caso particular se ajusta al supuesto previsto por la norma legal invocada como fundamento. Se transcribe a continuación la prueba de daño citada.

"PRUEBA DE DAÑO

INFORMACIÓN RELACIONADA CON HORARIOS DE OPERACIÓN, PROCESAMIENTO DE ÓRDENES DE TRANSFERENCIA Y TRASPASOS, FUNCIONALIDAD ESPECIFICA, ESPECIFICACIONES TÉCNICAS, PROTOCOLOS DE COMUNICACIÓN, FORMATOS DE MENSAJES, ESQUEMAS DE OPERACIÓN, PROCEDIMIENTOS DE CONTINUIDAD OPERATIVA Y DE CONTINGENCIA ASÍ COMO CUALQUIER OTRA INFORMACIÓN RELACIONADA CON LA SEGURIDAD INFORMÁTICA QUE SOPORTA EL FUNCIONAMIENTO DE LOS SISTEMAS DE PAGOS.

En términos de lo dispuesto por 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; así como, Vigésimo segundo, fracciones I, II, III y IV, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, debe clasificarse como información reservada, entre otra:

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

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

- *Aquélla que otorgue una ventaja indebida o que genere distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pago; y*

- *Aquélla que 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.*

Al respecto, revelar al público la información relativa a los horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de los sistemas de pagos, crearía distorsiones en los sistemas de pagos, comprometería las acciones encaminadas a propiciar el buen funcionamiento de los sistemas de pagos y podría generar el incumplimiento de obligaciones de un participante en los sistemas de pagos.

En particular, esto se debe a que esta información, en caso de divulgarse podría ser analizada y utilizada por una persona o grupo de personas malintencionadas para ***perpetrar ataques cibernéticos dirigidos*** *específicamente a los sistemas de pagos, lo cual posibilitaría la creación de mecanismos que faciliten el acceso indebido al propio sistema, la substracción de información relativa a sus usuarios y las operaciones que realizan,* ***la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios de pagos electrónicos interbancarios*** *y, en consecuencia, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de los sistemas de pagos, crearía distorsiones en estos sistemas, comprometería las acciones encaminadas a propiciar el buen funcionamiento de los sistemas de pagos y podría generar el incumplimiento de obligaciones de un participante en los sistemas de pagos.*

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

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

Al respecto, está documentado en la literatura especializada en la materia[1] *que los principales elementos de información que requiere conocer un cibercriminal son: la arquitectura de los sistemas, sus especificaciones técnicas, horarios de operación, funcionalidad general, protocolos de comunicación, aspectos de seguridad informática instrumentados, entre otros, para descubrir y aprovechar los puntos débiles que pudieran existir en estos elementos y atacar a los sistemas.*

Dentro de los elementos mencionados en el párrafo anterior, la información materia de la presente prueba de daño contienen ***aspectos de seguridad informática****, tales como*

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

horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, por lo cual su divulgación podría habilitar un ataque al mismo.

Demostrable. *Está documentado en diversos medios de comunicación, 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, lo cual es un hecho público y notorio. 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. Tal es el caso 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[2]. 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 financieros[3]. Entre otros ataques relevantes se encuentran: 1) el ataque de tipo "Whatering hole" en Polonia, que permitió utilizar un servidor de la Autoridad de Supervisión Financiera para distribuir código malicioso a más de 20 bancos polacos[4], el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada[5]; 2) el ataque del ransomware de WannaCry, cuyo código se propagó por los ordenadores de una red 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 afectó a diversos bancos en Rusia[6] y 3) 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[7]. En relación con lo anterior, es importante señalar que México ocupa el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica[8] y que tan sólo en México, el costo causado por el cibercrimen ascendió a $5,500 millones de dólares y afectó alrededor de 22.4 millones de personas, mientras que a nivel mundial, el costo ascendió a $125,900 millones de dólares y afectó a 689.4 millones de personas[9].*

---

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

3 Antony Peyton. "Symantec reveals more hack attempts on Swift network". Banking Technology. 11 oct 2016

4 Badcyber, Author. "Several Polish Banks Hacked, Information Stolen by Unknown Attackers." BadCyber, 9 feb 2017, http://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/ consultado el 18 oct 2017.

5 Hernández, Aura. "CNBV y Nueve Bancos Han Sido Hackeados." Excélsior, Excélsior, 17 feb 2017, http://www.excelsior.com.mx/hacker/2017/02/17/1146899 consultado el 18 oct 2017.

6 Winning, Alexander, and Jack Stubbs. "WannaCry Cyber Attack Compromised Some Russian Banks: Central Bank." Reuters, Thomson Reuters, 19 may 2017, http://www.reuters.com/article/us-cyber-attack-russia-cenbank/wannacry-cyber-attack-compromised-some-russian-banks-central-bank-idUSKCN18F16V consultado el 18 oct 2017.

7 Palazuelos, Félix. "Petya, un virus más peligroso y sofisticado que WannaCry" El País, elpais.com, 29 jun 2017, https://elpais.com/tecnologia/2017/06/28/actualidad/1498639459_556568.html consultado el 18 oct 2017.

8 Arreola Javier. "Ciberseguridad (casi) a prueba del enemigo 'invisible'". Forbes México. http://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/ consultado el 18 de oct de 2016.

9 Informe Norton sobre Ciberseguridad 2016 - Comparaciones Globales https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf consultado el 9 de oct de 2017.

En este sentido, la divulgación de la información materia de la presente prueba de daño, potencializaría que hechos como los mencionados en el párrafo anterior ocurran respecto de los sistemas informáticos que opera el Banco de México, particularmente los sistemas de pagos, puesto que los cibercriminales contarían con los elementos necesarios para perpetrar un ataque a la información de este Instituto Central.

Identificable. *Independientemente del origen o finalidad de un ataque contra los sistemas de pagos, las tecnologías de la información, comunicaciones o infraestructura tecnológica bajo la cual operan los sistemas de pagos, podrían resultar afectadas las órdenes de transferencia en las cuentas bancarias de los distintos participantes y usuarios de los sistemas 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 personas morales.*

Adicionalmente, una disrupción en los servicios provistos por los sistemas de pagos como el Sistema de Pagos Electrónicos Interbancarios (SPEI) o el Sistema de Pagos Interbancarios en Dólares (SPID), producto de un ataque contra éstos 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, los usuarios que utilizan estos medios de pago, verían afectadas su capacidad para realizar o cumplir con el pago de bienes y servicios, y las instituciones financieras participantes en los sistemas de pagos como el SPEI o el SPID, que además de hacer uso de estos sistemas para su operación propia obtienen ingresos del cobro de comisiones por la prestación de los servicio de pagos que ofrecen estos sistemas, también resultarían gravemente perjudicadas, lo cual provocaría una seria afectación al sistema financiero.

Por lo anterior, un ataque informático a los sistema de pagos, ocasionado por dar a conocer la información relacionada con esta prueba de daño, representa un perjuicio significativo para el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias, pues de acuerdo con la información del Banco de México, en agosto 2017, se realizaron en el SPEI aproximadamente 42 millones de pagos electrónicos interbancarios por un monto de 22 mil millones de pesos[10]; lo anterior equivale a más de 6 mil operaciones por un monto de 3 mil millones de pesos por hora. Para el cáso del SPID, en agosto de 2017 se realizaron aproximadamente 155 mil operaciones interbancarias en dólares entre personas morales, con un monto total transferido de aproximadamente 12 mil millones de dólares. Con base en estas cifras, es evidente que un ataque cibernético que vulnere la operación del SPEI, del SPID o sus tecnologías de la información y de comunicaciones, sin importar la duración de la disrupción, puede llegar a tener efectos cuantiosos sobre la actividad económica del país e incluso en actividad económica que forma parte de cadenas productivas globales, así como 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.

---

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

En consecuencia, proporcionar la información reservada motivo de esta prueba de daño, no aporta un beneficio al particular que sea comparable con el perjuicio que implicaría el hecho de divulgar información que en un momento dado, permita planear y perpetrar ataques cibernéticos dirigidos específicamente al SPEI, al SPID o a cualquier otro sistema de pagos administrado por este Instituto Central así como a la infraestructura relacionada con éstos, los cuales tengan como resultado la creación de mecanismos que faciliten el acceso indebido, la substracción de información 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 estos sistema de pagos. En este sentido, el riesgo de perjuicio antes señalado supera claramente el interés particular del solicitante, incluso el general de que se difunda la información solicitada.

Por otra parte, la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, *toda vez que en todo momento debe prevalecer el interés público sobre el interés particular, y como se ha dicho, la reserva de la información en comento evitará poner en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, así como también podría prevenir un daño en el buen funcionamiento de los sistemas de pagos, la creación de distorsiones en los sistemas de pagos, que se comprometan las acciones encaminadas a propiciar el buen funcionamiento del sistema de pagos, al igual que podría evitar la generación del incumplimiento de obligaciones de un participante en los sistemas de pagos.*

Dicha determinación es además proporcional considerando que, como se ha explicado, dar a conocer la información reservada materia de esta prueba de daño generaría un riesgo o daño de perjuicio significativo, el cual sería claramente mayor al beneficio particular que pudiera existir al dar a conocer dicha información.

En este orden de ideas, la reserva de la información referente a horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, resulta el medio menos restrictivo disponible para evitar el perjuicio señalado anteriormente. Por ello, se considera que dicha reserva deberá mantenerse por un plazo de cinco años, a partir de la fecha de clasificación, en razón de que la operación de los sistemas de pagos no tiene una fecha establecida de conclusión.

La referida reserva, evitaría, como se ha explicado, poner en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, así como también podría prevenir un daño en el buen funcionamiento de los sistemas de pagos, la creación de distorsiones en estos sistemas de pagos, que se comprometan las acciones encaminadas a propiciar el buen funcionamiento de éstos sistema de pagos, al igual que podría evitar la generación del incumplimiento de obligaciones de un participante en los sistemas de pagos.

Por lo expuesto, 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; 100, 103, 104, 105, 106, fracción I, 108, último párrafo, 109, 113, fracción IV, y 114 de la Ley General de Transparencia y Acceso a la Información Pública; 97, 98, fracción I, 100, 103, 104, 105, último párrafo, 106, 110, fracción IV, y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública; 1o., 2o. y 3o.,

fracción I, de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, 20, fracciones II, IV, V, VI, IX y XVI, del Reglamento Interior del Banco de México; Segundo, fracción VIII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, así como, Primero, Segundo, fracción XIII, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I, II, III y IV de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, se ha determinado clasificar como información reservada la relacionada con horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, materia de esta prueba de daño, en virtud de que su divulgación pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, y comprometería las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos."

Con base en lo anterior, este órgano colegiado estima que la citada prueba de daño es idónea para clasificar como reservada la Información relacionada con horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad específica, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soporta el funcionamiento de los sistemas de pagos.

Lo anterior, en razón de que divulgar la información materia de la presente clasificación, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto y podría generar el incumplimiento de obligaciones de uno o más participantes en los sistemas de pagos. De igual forma, la misma podría ser analizada y utilizada por una persona o grupo de personas malintencionadas para perpetrar ataques cibernéticos dirigidos específicamente a los sistemas de pagos, lo cual posibilitaría la creación de mecanismos que faciliten el acceso indebido al propio sistema, la substracción de información relativa a sus usuarios y las operaciones que realizan, la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios de pagos electrónicos interbancarios y, en consecuencia, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto y podría generar el incumplimiento de obligaciones de un participante en los sistemas de pagos.

Adicionalmente, se debe destacar que en todo momento debe prevalecer el interés público sobre el interés particular, y como se ha dicho, la reserva de la información en comento evitará poner en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, al igual que podría evitar la generación del incumplimiento de obligaciones de un participante en los sistemas de pagos.

En consecuencia, con fundamento en los artículos 44, fracción II, 103, 105, 106, fracción I, 108, último párrafo, 109, 113, fracción IV, 114, y 137, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 98, fracción I, 100, 103, 105, último párrafo, 106, 110, fracción IV, y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, 20, fracciones II, IV, V, VI, IX y XVI, 31, fracción II, del Reglamento Interior del Banco de México; así como Primero, Segundo, fracción XIII, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero,

Vigésimo segundo, fracciones I y IV, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, este Comité de Transparencia **confirma la clasificación de la información realizada por la Gerencia de Política y Vigilancia de los Sistemas de Pagos, adscrita a la Dirección de Sistemas de Pagos del Banco de México**, identificada, fundada y motivada en las versiones públicas y prueba de daño referidas en el presente considerando, toda vez que se trata de información reservada, en virtud de que su divulgación pone en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, y podría generar el incumplimiento de obligaciones de uno o más participantes en los sistemas de pagos.

Por lo expuesto, con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, y 111, de la Ley General de Transparencia y Acceso a la Información Pública, 64, párrafos primero, segundo, tercero, y quinto, 65 fracciones II y IX, y 31, fracciones II y XIV, del Reglamento Interior del Banco de México, Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", emitidos por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, vigentes, y Quinta, inciso e), de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

ÚNICO. Se confirma la clasificación de información realizada por la Gerencia de Política y Vigilancia de los Sistemas de Pagos, adscrita a la Dirección de Sistemas de Pagos del Banco de México, misma que se detalla, fundamenta y motiva en las carátulas y prueba de daño, de las correspondientes versiones públicas señaladas en el oficio con referencia D10/214/2017, y también este órgano colegiado aprueban las versiones públicas respectivas, en términos del considerando Segundo de la presente resolución.

Así lo resolvió, por unanimidad de los integrantes presentes de este Comité de Transparencia del Banco de México, en sesión ordinaria celebrada el veintiséis de octubre de dos mil diecisiete. ------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

ABDÓN SÁNCHEZ ARROYO
Integrante

ANEXO "E"

BANCO DE MÉXICO

"Año del Centenario de la Promulgación de la Constitución Política de los Estados Unidos Mexicanos"

REF.: D10/215/2017

Ciudad de México, a 20 de octubre de 2017

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
PRESENTE

Me refiero a la solicitud de acceso a la información identificada con el número de folio CTC-BM-20852, que nos turnó la Unidad de Transparencia el veintidós de septiembre del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, que se transcribe a continuación:

> *"Por medio del presente, Solicito de su apoyo en que nos puedan proporcionar donde podrémos encontrar el Manual de Operación de SPEI, esto con el fin de comprender por completos los Requisitos de Seguridad Informática descritos en la circula 14/2017.Agradecemos de apoyo."*

Sobre el particular, con fundamento en los artículos 100, 106, fracción I y 111, de la Ley General de Transparencia y Acceso a la Información Pública; 97, 98, fracción I y 108, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como el Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" (Lineamientos), vigentes, me permito informarles que esta unidad administrativa ha determinado clasificar diversa información contenida en el documento que se indican más adelante.

En consecuencia, esta área ha generado la versión pública respectiva, junto con la carátula que la distingue e indica los datos concretos que han sido clasificados, al igual que los motivos y fundamentos respectivos. Asimismo, se ha elaborado la correspondiente prueba de daño, que se adjunta al presente. Dichos documentos se encuentran disponibles a partir de esta fecha en la carpeta compartida ubicada en la red interna del Banco de México, a la que se puede acceder a través de la siguiente liga:

I:\A13 Dir Unidad de Transparencia\Comité de Transparencia Compartida\2017\Sesiones Ordinarias 2017\Asuntos para sesión

Para facilitar su identificación, en el siguiente cuadro encontrarán el detalle del título del documento clasificado, el cual coinciden con el que aparece en la carátula que debidamente firmada se acompaña al presente. Asimismo, en dicho cuadro encontrarán las ligas respectivas al repositorio institucional en el que reside la versión digitalizada del documento original respecto del cual se elaboró la versión pública.

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXO	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)
Manual de Operación del SPEI® versión 5.0	1	2	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Sistemas%20de%20pagos/Web%20Externo/Manuales/SPEI-MANUAL_Ver-5_0.pdf

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 II, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, de los Lineamientos, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de la información realizada por esta unidad administrativa, y aprobar la versión pública señalada en el cuadro precedente.

Asimismo, de conformidad con el Décimo de los señalados Lineamientos, informo que el personal que por la naturaleza de sus atribuciones tiene acceso al referido documento clasificado es el adscrito a la Dirección de Sistemas de Pagos.

BANCO DE MÉXICO
RECIBIDO
20 OCT 2017
Comité de Transparencia
Por: 715383 Hora: 13:40

ATENTAMENTE,

DR. OTHÓN MARTINO MORENO GONZÁLEZ
GERENTE DE POLÍTICA Y VIGILANCIA DE LOS SISTEMAS DE PAGOS
En conformidad con lo establecido en el Art. 66 del Reglamento Interior del Banco de México

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

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

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

Versión Pública		
I.	Área titular que clasifica la información	Dirección de Sistemas de Pagos
II.	La identificación del documento del que se elabora la versión pública.	Manual de Operación del SPEI® versión 5.0
III.	Firma del titular del área y de quien clasifica.	**Dr. Othón Martino Moreno González** Gerente de Política y Vigilancia de los Sistemas de Pagos En conformidad con lo establecido en el Art. 66 del Reglamento Interior del Banco de México
IV.	Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: **cinco años**				
Ref.	**Pág.**	**Información testada**	**Fundamento Legal**	**Motivación**
1	Primera y segunda páginas del histórico de revisiones Tercera, cuarta, sexta, séptima, octava, novena, y décima páginas del índice.	Información relacionada con esquemas de operación formato de mensajes y protocolos de comunicación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
2	1, 2	Información relacionada con especificaciones técnicas y esquemas de operación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
3	4, 5	Información relacionada con el procesamiento de órdenes de transferencia y traspasos	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
4	5	Información relacionada con el procesamiento de órdenes de transferencia y traspasos así como horarios de operación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
5	6, 7	Información relacionada con órdenes de transferencia y traspasos.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
6	7 a la 13	Información relacionada con la funcionalidad general, formatos de	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país

		mensajes y protocolos de comunicación.		y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
7	14	Información relacionada con la funcionalidad general, formatos de mensajes, protocolos de comunicación, órdenes de transferencia y traspasos.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
8	15 a la 17	Información relacionada con la funcionalidad general, formatos de mensajes y protocolos de comunicación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
9	18, 19	Información relacionada con procedimientos continuidad operativa y de contingencia, y protocolos de comunicación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
10	19,20,22	Información relacionada con la funcionalidad general y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
11	23 al 26	Información relacionada con especificaciones técnicas y funcionalidad general.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
12	27	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a

				proveer el buen funcionamiento de los sistemas de pagos.
13	28 a la 33	Información relacionada con la funcionalidad general, especificaciones técnicas, protocolos de comunicación y formatos de mensajes.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
14	36 a la 125	Información relacionada con protocolos de comunicación y formato de mensajes.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
15	132 a la 164 y de 167 a la 194	Información relacionada con la funcionalidad general, especificaciones técnicas, protocolos de comunicación, órdenes de transferencia y esquemas de operación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
16	194	Información relacionada con procedimientos continuidad operativa y de contingencia.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
17	195 a la 200	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
18	201 a la 206	Información relacionada con la funcionalidad general, especificaciones técnicas, protocolos de comunicación, órdenes de transferencia y esquemas de operación.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.

19	207 a la 209	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
20	210 a la 215	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
21	216	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
22	217,218	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
23	221	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
24	223 a la 265, 267	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
25	270,271 y de 278 a la 283	Información relacionada con especificaciones	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero,

		técnicas y seguridad informática.		económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
26	284,285	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
27	286 a la 288	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
28	289 a la 297	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
29	299 a la 307	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
30	308	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
31	309 a la 313	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a

				proveer el buen funcionamiento de los sistemas de pagos.
32	314,315	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
33	316, 317	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
34	318	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.
35	319 a la 330	Información relacionada con especificaciones técnicas y seguridad informática.	De conformidad a la prueba de daño	Contiene información clasificada como reservada cuya divulgación compromete el funcionamiento de los sistemas financiero, económico, cambiario o monetario del país y de la economía nacional en su conjunto, así como las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.

PRUEBA DE DAÑO

INFORMACIÓN RELACIONADA CON HORARIOS DE OPERACIÓN, PROCESAMIENTO DE ÓRDENES DE TRANSFERENCIA Y TRASPASOS, FUNCIONALIDAD ESPECIFICA, ESPECIFICACIONES TÉCNICAS, PROTOCOLOS DE COMUNICACIÓN, FORMATOS DE MENSAJES, ESQUEMAS DE OPERACIÓN, PROCEDIMIENTOS DE CONTINUIDAD OPERATIVA Y DE CONTINGENCIA ASÍ COMO CUALQUIER OTRA INFORMACIÓN RELACIONADA CON LA SEGURIDAD INFORMÁTICA QUE SOPORTA EL FUNCIONAMIENTO DE LOS SISTEMAS DE PAGOS.

En términos de lo dispuesto por 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; así como, Vigésimo segundo, fracciones I, II, III y IV, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, debe clasificarse como información reservada, entre otra:

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

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

- Aquélla que otorgue una ventaja indebida o que genere distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pago; y

- Aquélla que 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.

Al respecto, revelar al público la información relativa a los horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de los sistemas de pagos, crearía distorsiones en los sistemas de pagos, comprometería las acciones encaminadas a propiciar el buen funcionamiento de los sistemas de pagos y podría generar el incumplimiento de obligaciones de un participante en los sistemas de pagos.

En particular, esto se debe a que esta información, en caso de divulgarse podría ser analizada y utilizada por una persona o grupo de personas malintencionadas para **perpetrar ataques cibernéticos dirigidos** específicamente a los sistemas de pagos, lo cual posibilitaría la creación de mecanismos que faciliten el acceso indebido al propio sistema, la substracción de información relativa a sus usuarios y las operaciones que realizan, **la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios de pagos electrónicos interbancarios** y, en consecuencia, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de los sistemas de pagos, crearía distorsiones en estos sistemas, comprometería las acciones encaminadas a propiciar el buen funcionamiento de los sistemas de pagos y podría generar el incumplimiento de obligaciones de un participante en los sistemas de pagos.

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

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

Al respecto, está documentado en la literatura especializada en la materia[1] que los principales elementos de información que requiere conocer un cibercriminal son: la arquitectura de los sistemas, sus especificaciones técnicas, horarios de operación, funcionalidad general, protocolos de comunicación, aspectos de seguridad informática instrumentados, entre otros, para descubrir y aprovechar los puntos débiles que pudieran existir en estos elementos y atacar a los sistemas.

Dentro de los elementos mencionados en el párrafo anterior, la información materia de la presente prueba de daño contienen **aspectos de seguridad informática**, tales como horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, por lo cual su divulgación podría habilitar un ataque al mismo.

Demostrable. Está documentado en diversos medios de comunicación, 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, lo cual es un hecho público y notorio. Las investigaciones realizadas señalan que estos ataques han sido orquestados por organizaciones criminales internacionales con herramientas y técnicas sofisticadas que, además

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

de dañar la reputación de las instituciones afectadas, han generado cuantiosas pérdidas económicas. Tal es el caso 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[2]. 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 financieros[3]. Entre otros ataques relevantes se encuentran: 1) el ataque de tipo "Whatering hole" en Polonia, que permitió utilizar un servidor de la Autoridad de Supervisión Financiera para distribuir código malicioso a más de 20 bancos polacos[4], el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada[5]; 2) el ataque del ransomware de WannaCry, cuyo código se propagó por los ordenadores de una red 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 afectó a diversos bancos en Rusia[6] y 3) 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[7]. En relación con lo anterior, es importante señalar que México ocupa el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica[8] y que tan sólo en México, el costo causado por el cibercrimen ascendió a $5,500 millones de dólares y afectó alrededor de 22.4 millones de personas, mientras que a nivel mundial, el costo ascendió a $125,900 millones de dólares y afectó a 689.4 millones de personas[9].

En este sentido, la divulgación de la información materia de la presente prueba de daño, potencializaría que hechos como los mencionados en el párrafo anterior ocurran respecto de los sistemas informáticos que opera el Banco de México, particularmente los sistemas de pagos, puesto que los cibercriminales contarían con los elementos necesarios para perpetrar un ataque a la información de este Instituto Central.

---

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

3 Antony Peyton. "Symantec reveals more hack attempts on Swift network". Banking Technology. 11 oct 2016

4 Badcyber, Author. "Several Polish Banks Hacked, Information Stolen by Unknown Attackers." BadCyber, 9 feb 2017, http://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/ consultado el 18 oct 2017.

5 Hernández, Aura. "CNBV y Nueve Bancos Han Sido Hackeados." Excélsior, Excélsior, 17 feb 2017, http://www.excelsior.com.mx/hacker/2017/02/17/1146899 consultado el 18 oct 2017.

6 Winning, Alexander, and Jack Stubbs. "WannaCry Cyber Attack Compromised Some Russian Banks: Central Bank." Reuters, Thomson Reuters, 19 may 2017, http://www.reuters.com/article/us-cyber-attack-russia-cenbank/wannacry-cyber-attack-compromised-some-russian-banks-central-bank-idUSKCN18F16V consultado el 18 oct 2017.

7 Palazuelos, Félix. "Petya, un virus más peligroso y sofisticado que WannaCry" El País, elpais.com, 29 jun 2017, https://elpais.com/tecnologia/2017/06/28/actualidad/1498639459_556568.html consultado el 18 oct 2017.

8 Arreola Javier. "Ciberseguridad (casi) a prueba del enemigo 'invisible'". Forbes México. http://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/ consultado el 18 de oct de 2016.

9 Informe Norton sobre Ciberseguridad 2016 - Comparaciones Globales https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf consultado el 9 de oct de 2017.

Identificable. Independientemente del origen o finalidad de un ataque contra los sistemas de pagos, las tecnologías de la información, comunicaciones o infraestructura tecnológica bajo la cual operan los sistemas de pagos, podrían resultar afectadas las órdenes de transferencia en las cuentas bancarias de los distintos participantes y usuarios de los sistemas 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 personas morales.

Adicionalmente, una disrupción en los servicios provistos por los sistemas de pagos como el Sistema de Pagos Electrónicos Interbancarios (SPEI) o el Sistema de Pagos Interbancarios en Dólares (SPID), producto de un ataque contra éstos 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, los usuarios que utilizan estos medios de pago, verían afectadas su capacidad para realizar o cumplir con el pago de bienes y servicios, y las instituciones financieras participantes en los sistemas de pagos como el SPEI o el SPID, que además de hacer uso de estos sistemas para su operación propia obtienen ingresos del cobro de comisiones por la prestación de los servicio de pagos que ofrecen estos sistemas, también resultarían gravemente perjudicadas, lo cual provocaría una seria afectación al sistema financiero.

Por lo anterior, un ataque informático a los sistema de pagos, ocasionado por dar a conocer la información relacionada con esta prueba de daño, representa un perjuicio significativo para el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias, pues de acuerdo con la información del Banco de México, en agosto 2017, se realizaron en el SPEI aproximadamente 42 millones de pagos electrónicos interbancarios por un monto de 22 mil millones de pesos[10]; lo anterior equivale a más de 6 mil operaciones por un monto de 3 mil millones de pesos por hora. Para el caso del SPID, en agosto de 2017 se realizaron aproximadamente 155 mil operaciones interbancarias en dólares entre personas morales, con un monto total transferido de aproximadamente 12 mil millones de dólares. Con base en estas cifras, es evidente que un ataque cibernético que vulnere la operación del SPEI, del SPID o sus tecnologías de la información y de comunicaciones, sin importar la duración de la disrupción, puede llegar a tener efectos cuantiosos sobre la actividad económica del país e incluso en actividad económica que forma parte de cadenas productivas globales, así como 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.

---

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

En consecuencia, proporcionar la información reservada motivo de esta prueba de daño, no aporta un beneficio al particular que sea comparable con el perjuicio que implicaría el hecho de divulgar información que en un momento dado, permita planear y perpetrar ataques cibernéticos dirigidos específicamente al SPEI, al SPID o a cualquier otro sistema de pagos administrado por este Instituto Central así como a la infraestructura relacionada con éstos, los cuales tengan como resultado la creación de mecanismos que faciliten el acceso indebido, la substracción de información 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 estos sistema de pagos. En este sentido, el riesgo de perjuicio antes señalado supera claramente el interés particular del solicitante, incluso el general de que se difunda la información solicitada.

Por otra parte, la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, toda vez que en todo momento debe prevalecer el interés público sobre el interés particular, y como se ha dicho, la reserva de la información en comento evitará poner en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, así como también podría prevenir un daño en el buen funcionamiento de los sistemas de pagos, la creación de distorsiones en los sistemas de pagos, que se comprometan las acciones encaminadas a propiciar el buen funcionamiento del sistema de pagos, al igual que podría evitar la generación del incumplimiento de obligaciones de un participante en los sistemas de pagos.

Dicha determinación es además proporcional considerando que, como se ha explicado, dar a conocer la información reservada materia de esta prueba de daño generaría un riesgo o daño de perjuicio significativo, el cual sería claramente mayor al beneficio particular que pudiera existir al dar a conocer dicha información.

En este orden de ideas, la reserva de la información referente a horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, resulta el medio menos restrictivo disponible para evitar el perjuicio señalado anteriormente. Por ello, se considera que dicha reserva deberá mantenerse por un plazo de cinco años, a partir de la fecha de clasificación, en razón de que la operación de los sistemas de pagos no tiene una fecha establecida de conclusión.

La referida reserva, evitaría, como se ha explicado, poner en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, así como también podría prevenir un daño en el buen funcionamiento de los sistemas de pagos, la creación de distorsiones en estos sistemas de pagos, que se comprometan las acciones encaminadas a propiciar el buen funcionamiento de éstos sistema de pagos, al igual que podría evitar la generación del incumplimiento de obligaciones de un participante en los sistemas de pagos.

Por lo expuesto, 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; 100, 103, 104, 105, 106, fracción I, 108, último párrafo, 109, 113, fracción IV, y 114 de la Ley General de Transparencia y Acceso a la Información Pública; 97, 98, fracción I, 100, 103, 104, 105, último párrafo, 106, 110, fracción IV, y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública; 1o., 2o. y 3o., fracción I, de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, 20, fracciones II, IV, V, VI, IX y XVI, del Reglamento Interior del Banco de México; Segundo, fracción VIII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, así como, Primero, Segundo, fracción XIII, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I, II, III y IV de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, se ha determinado clasificar como información reservada la relacionada con horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, materia de esta prueba de daño, en virtud de que su divulgación pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, y comprometería las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos.

Dr. Othón Martino Moreno González
Gerente de Política y Vigilancia de los Sistemas de Pagos
De conformidad con el Art. 66 del Reglamento Interior del Banco de México

REFERENCIA 1

United States Government Accountability Office

GAO

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

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

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

David A. Powner, Director
Information Technology Management Issues

GAO-10-230T

REFERENCIA 2

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

by **Michael Riley** and **Alan Katz**
2016 MDS 26 08:36 GMT-5
Updated on 2016 MDS 26 15:21 GMT-5

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

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.

FireEye <https://www.bloomberg.com/quote/FEYE:US>, the security firm hired by the Bangladesh bank, has been contacted by the other banks, most of which are in Southeast Asia, because of signs that hackers may have breached their networks, the person said. They include banks in the Philippines and New Zealand but not in Western Europe or the United States. There is no indication of whether money was taken.

The expansion of the investigation four months after the discovery of the Bangladesh attack, the biggest known cyber-heist in history, suggests a broad and serious campaign to breach the international financial system.

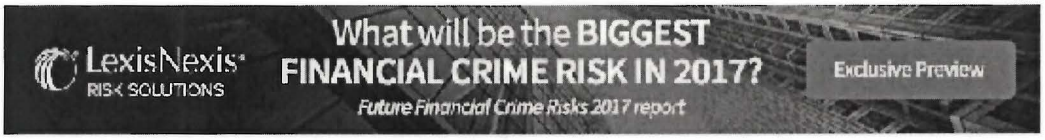
FireEye declined to comment on the report.

"The emergence of new possible instances of compromise is not entirely surprising given that banks should now be undertaking rigorous reviews of their environments," Swift said in a written statement. "Many may turn out to be false positives and or have nothing to do with Swift messages, but it is key that these reviews take place and banks' environments are secured."

For details on how Swift member banks have responded to the breaches, click here. <http://www.bloomberg.com/news/articles/2016-05-17/global-lenders-on-edge-as-hacks-embroil-growing-list-of-banks>

The Brussels-based interbank cooperative, whose full name is the Society for Worldwide Interbank Financial Telecommunication, has warned that there may have been more breaches than the three already publicly

REFERENCIA 3



18 May, 2017

banking technology

Tweet
39
Share

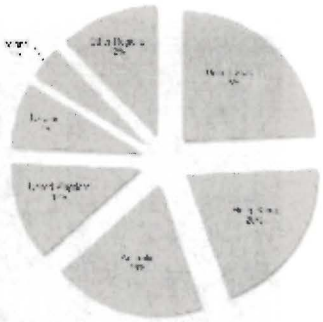

tec reveals more hack attempts on Swift network

Follow @banking techno; 2016 Written by Antony Peyton

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

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

Symantec says these Odinaff attacks are an example of another group believed to be involved in this kind of activity, following the Bangladesh central bank heist linked to the Lazarus group.



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

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 on the subject and recently unveiled SwiftSmart modules to help its customers operate their Swift environment "securely and in-line with best practice". This move is also a "critical part" of its Customer Security Programme launched in May 2016. That five-part plan was a result of various hacking incidents.

It's not just Swift

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

REFERENCIA 4

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 5

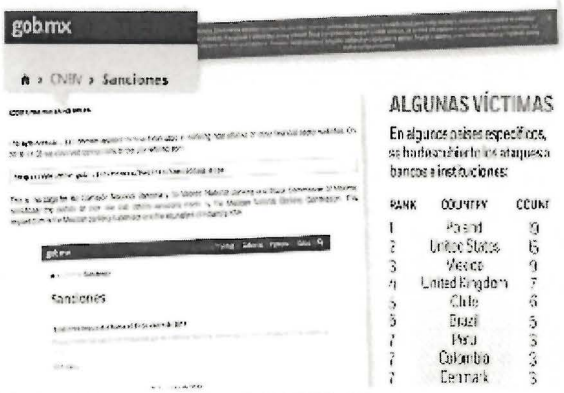


CNBV y nueve bancos han sido hackeados

Criminales han vulnerado la seguridad de instituciones financieras en México

17/02/2017 09:40 **AURA HERNÁNDEZ Y PAUL LARA**

COMPARTIR SÍGUENOS



REFERENCIA 6

REUTERS

#TECHNOLOGY NEWS
MAY 19, 2017 / 6:09 AM / 5 MONTHS AGO

WannaCry cyber attack compromised some Russian banks: central bank

Alexander Winning, Jack Stubbs

MOSCOW (Reuters) - The WannaCry ransomware attack compromised the systems of Russian banks in some isolated cases, the Russian central bank said on Friday in the first official acknowledgement by Moscow that the virus had an impact on the country's banking system.

WATCH LIVE
Sessions testifies on oversight of the Department of Justice

REFERENCIA 7

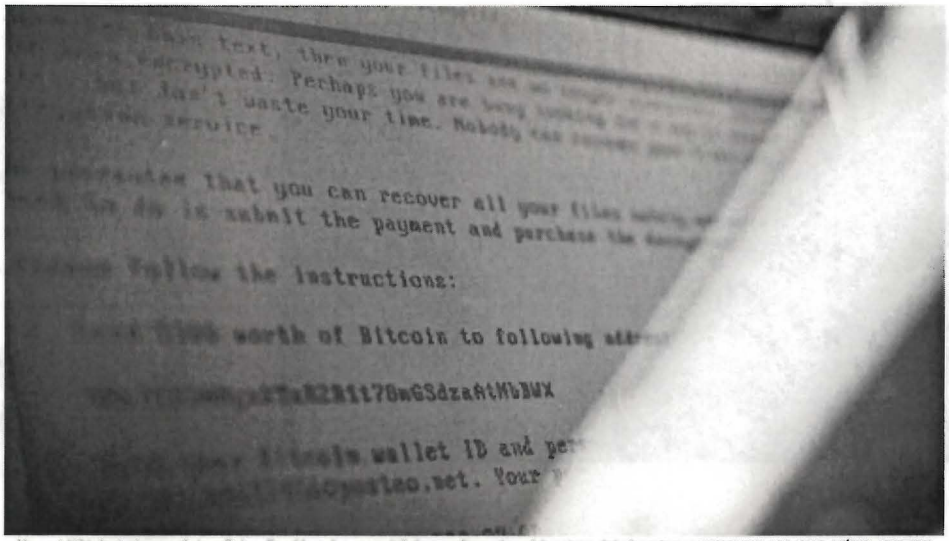
CIBERATAQUES ›

Petya, un virus más peligroso y sofisticado que WannaCry

Los expertos muestran su sorpresa por estos últimos ataques que no intentan robar y vender información pasando inadvertidos

FÉLIX PALAZUELOS

29 JUN 2017 - 09:32 CEST



Un portátil infectado con el virus Petya. En vídeo, dos especialistas analizan el posible origen del ciberataque. ROB ENGELAAR (AFP) / VÍDEO: REUTERS-QUALITY

El virus Petya, que ayer afectó a grandes empresas de todo el mundo es más peligroso y sofisticado que WannaCry, aunque se base en el mismo principio de propagación masiva a través de las redes locales. "Pese a que todavía no sepamos con certeza cuál es el primer equipo infectado y cómo se infectó, sabemos que este nuevo *malware* usa la vulnerabilidad EternalBlue junto a lo que llamamos en ciberseguridad movimientos laterales", dice Sergio de los Santos, director de innovación y laboratorio en Eleven Paths, unidad especializada en ciberseguridad de Telefónica, a EL PAÍS. "Ahora no sólo busca equipos vulnerables, también emplea herramientas de administración para infectar a todos los equipos de una red si, por suerte, encuentra previamente una máquina con dichos privilegios".

No hemos aprendido pese al tirón de orejas

"Nos habíamos olvidado ya de los gusanos y los ataques informáticos siempre han estado enfocados a atacar a alguien de forma sigilosa a través de infecciones por *email* en los últimos años" señala De los Santos. "Pero no hemos aprendido pese al tirón de orejas".

REFERENCIA 8

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.



Share Tweet +

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

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

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

EDU

MÁS COBERTURA



Scotiabank se une a aceleradora para impulsar su banca digital en AL (https://www.forbes.com.mx/scoti se-une-a-aceleradora-para-impulsar-su-banca-digital-en-al/)



Avianca iniciará proceso disciplinario contra pilotos en huelga (https://www.forbes.com.mx/aviar iniciara-proceso-disciplinario-contra-pilotos-en-huelga/)



Twitter endurece sus políticas contra el acoso y abuso sexual (https://www.forbes.com.mx/4012 2/)

Últimas Noticias

Tiroteo en Maryland deja 3 muertos policía busca a sospechoso (https://www.forbes.com.mx/tirote en-maryland-deja-3-muertos-polici busca-a-sospechoso/)
OCTUBRE 18, 2017

Iberia tendrá tres vuelos semanales a Nicaragua para 2018 (https://www.forbes.com.mx/iberi tendra-tres-vuelos-semanales-a-nicaragua-para-2018/)
OCTUBRE 18, 2017

Resultados de IBM provocan apertu récord de Dow Jones (https://www.forbes.com.mx/resul de-ibm-provocan-apertura-record-dow-jones/)
OCTUBRE 18, 2017

REFERENCIA 9

Informe Norton sobre Ciberseguridad 2016

Comparaciones Globales

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

© 2016 Symantec Corporation. Todos los derechos reservados. Symantec, el logotipo de Checkmark, Norton y Norton by Symantec son marcas comerciales o registradas por Symantec Corporation o de sus filiales en los Estados Unidos y otros países. Otros nombres pueden ser marcas comerciales de sus respectivos dueños. 10/16

Norton by Symantec

REFERENCIA 10

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real.

Fecha de consulta: 18/05/2017 06:51:11

Título	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios. SPEI, Número de operaciones	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios. SPEI, Importe
Periodo disponible	Ene 1992 - Abr 2017	Ene 1992 - Abr 2017
Periodicidad	Mensual	Mensual
Cifra	Volumen	Flujos
Unidad	Operaciones	Millones de Pesos
Base		
Aviso		
Tipo de información	Niveles	Niveles
Fecha	SF46188	SF46189
Ene 2017	35,016,703	23,877,271
Feb 2017	34,817,472	21,505,024
Mar 2017	40,016,546	26,180,217
Abr 2017	35,954,794	20,494,020

ANEXO "F"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: CTC-BM-20852

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

RESULTANDO

PRIMERO. El veintidós de septiembre de dos mil diecisiete, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **CTC-BM-20852**, que se transcribe a continuación:

> *"Por medio del presente,*
> *Solicito de su apoyo en que nos puedan proporcionar donde podrémos encontrar el Manual de Operación de SPEI, esto con el fin de comprender por completos los Requisitos de Seguridad Informática descritos en la circula 14/2017.*
> *Agradecemos de apoyo."*

SEGUNDO. El mismo veintidós de septiembre de dos mil diecisiete, la Unidad de Transparencia de este Instituto Central remitió a la Dirección de Sistemas de Pagos del Banco de México, para su atención, 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. Mediante oficio con referencia D01 C298/2017, del dos de octubre del presente año, la Dirección de Sistemas de Pagos del Banco de México, solicitó a este órgano colegiado la confirmación de la ampliación del plazo de respuesta a la solicitud que nos ocupa.

CUARTO. Por resolución del once de octubre del presente año, este Comité de Transparencia confirmó la determinación de ampliación del plazo de respuesta referida en el resultando anterior, misma que fue notificada al solicitante dentro del plazo de veinte días, contados a partir del siguiente a la presentación de su solicitud.

QUINTO. El Gerente de Política y Vigilancia de los Sistemas de Pagos, en suplencia por ausencia del Director de Sistemas de Pagos, mediante oficio con referencia D10/215/2017, del veinte de octubre de dos mil diecisiete, informó a este Comité de Transparencia que esa unidad administrativa estima que aún subsisten las causas que dieron origen a la clasificación del documento referido en el citado oficio, por lo que solicitó a este órgano colegiado confirmar la clasificación referida.

CONSIDERANDOS

PRIMERO. Este Comité de Transparencia es competente para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas del

Banco de México, de conformidad con lo previsto en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México, así como para aprobar las versiones públicas que las unidades administrativas del referido Instituto Central sometan a su consideración, en términos del Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes.

SEGUNDO. Enseguida se analiza la clasificación realizada por la Gerencia de Política y Vigilancia de los Sistemas de Pagos, adscrita a la Dirección de Sistemas de Pagos del Banco de México, a través de la versión pública señalada en el referido oficio y de la prueba de daño correspondiente.

Al respecto, este órgano colegiado advierte que se trata de información reservada los datos testados en la versión pública del documento identificado en el oficio señalado en el resultando Quinto de la presente resolución, los cuales se detallan, fundamentan y motivan en el cuadro identificado con la leyenda "PARTES O SECCIONES CLASIFICADAS COMO RESERVADA", en la referida versión pública, y en particular en su correspondiente carátula y prueba de daño.

En este sentido, la prueba de daño en la que se fundamenta y motiva dicha clasificación, así como las razones, motivos y circunstancias especiales con las que se concluye que en el caso particular se ajusta al supuesto previsto por la norma legal invocada como fundamento, se transcribe a continuación:

"PRUEBA DE DAÑO

INFORMACIÓN RELACIONADA CON HORARIOS DE OPERACIÓN, PROCESAMIENTO DE ÓRDENES DE TRANSFERENCIA Y TRASPASOS, FUNCIONALIDAD ESPECIFICA, ESPECIFICACIONES TÉCNICAS, PROTOCOLOS DE COMUNICACIÓN, FORMATOS DE MENSAJES, ESQUEMAS DE OPERACIÓN, PROCEDIMIENTOS DE CONTINUIDAD OPERATIVA Y DE CONTINGENCIA ASÍ COMO CUALQUIER OTRA INFORMACIÓN RELACIONADA CON LA SEGURIDAD INFORMÁTICA QUE SOPORTA EL FUNCIONAMIENTO DE LOS SISTEMAS DE PAGOS.

En términos de lo dispuesto por 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; así como, Vigésimo segundo, fracciones I, II, III y IV, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, debe clasificarse como información reservada, entre otra:

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

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

- *Aquélla que otorgue una ventaja indebida o que genere distorsiones en la estabilidad de los mercados, incluyendo los sistemas de pago; y*

- *Aquélla que 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.*

Al respecto, revelar al público la información relativa a los horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de los sistemas de pagos, crearía distorsiones en los sistemas de pagos, comprometería las acciones encaminadas a propiciar el buen funcionamiento de los sistemas de pagos y podría generar el incumplimiento de obligaciones de un participante en los sistemas de pagos.

En particular, esto se debe a que esta información, en caso de divulgarse podría ser analizada y utilizada por una persona o grupo de personas malintencionadas para ***perpetrar ataques cibernéticos dirigidos*** *específicamente a los sistemas de pagos, lo cual posibilitaría la creación de mecanismos que faciliten el acceso indebido al propio sistema, la substracción de información relativa a sus usuarios y las operaciones que realizan,* ***la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios de pagos electrónicos interbancarios*** *y, en consecuencia, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de los sistemas de pagos, crearía distorsiones en estos sistemas, comprometería las acciones encaminadas a propiciar el buen funcionamiento de los sistemas de pagos y podría generar el incumplimiento de obligaciones de un participante en los sistemas de pagos.*

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

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

Al respecto, está documentado en la literatura especializada en la materia[1] *que los principales elementos de información que requiere conocer un cibercriminal son: la arquitectura de los sistemas, sus especificaciones técnicas, horarios de operación, funcionalidad general, protocolos de comunicación, aspectos de seguridad informática instrumentados, entre otros, para descubrir y aprovechar los puntos débiles que pudieran existir en estos elementos y atacar a los sistemas.*

Dentro de los elementos mencionados en el párrafo anterior, la información materia de la presente prueba de daño contienen ***aspectos de seguridad informática****, tales como*

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

horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, por lo cual su divulgación podría habilitar un ataque al mismo.

Demostrable. *Está documentado en diversos medios de comunicación, 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, lo cual es un hecho público y notorio. 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. Tal es el caso 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[2]. 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 financieros[3]. Entre otros ataques relevantes se encuentran: 1) el ataque de tipo "Whatering hole" en Polonia, que permitió utilizar un servidor de la Autoridad de Supervisión Financiera para distribuir código malicioso a más de 20 bancos polacos[4], el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada[5]; 2) el ataque del ransomware de WannaCry, cuyo código se propagó por los ordenadores de una red 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 afectó a diversos bancos en Rusia[6] y 3) 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[7]. En relación con lo anterior, es importante señalar que México ocupa el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica[8] y que tan sólo en México, el costo causado por el cibercrimen ascendió a $5,500 millones de dólares y afectó alrededor de 22.4 millones de personas, mientras que a nivel mundial, el costo ascendió a $125,900 millones de dólares y afectó a 689.4 millones de personas[9].*

---

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

3 Antony Peyton. "Symantec reveals more hack attempts on Swift network". Banking Technology. 11 oct 2016

4 Badcyber, Author. "Several Polish Banks Hacked, Information Stolen by Unknown Attackers." BadCyber, 9 feb 2017, http://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/ consultado el 18 oct 2017.

5 Hernández, Aura. "CNBV y Nueve Bancos Han Sido Hackeados." Excélsior, Excélsior, 17 feb 2017, http://www.excelsior.com.mx/hacker/2017/02/17/1146899 consultado el 18 oct 2017.

6 Winning, Alexander, and Jack Stubbs. "WannaCry Cyber Attack Compromised Some Russian Banks: Central Bank." Reuters, Thomson Reuters, 19 may 2017, http://www.reuters.com/article/us-cyber-attack-russia-cenbank/wannacry-cyber-attack-compromised-some-russian-banks-central-bank-idUSKCN18F16V consultado el 18 oct 2017.

7 Palazuelos, Félix. "Petya, un virus más peligroso y sofisticado que WannaCry" El País, elpais.com, 29 jun 2017, https://elpais.com/tecnologia/2017/06/28/actualidad/1498639459_556568.html consultado el 18 oct 2017.

8 Arreola Javier. "Ciberseguridad (casi) a prueba del enemigo 'invisible'". Forbes México. http://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/ consultado el 18 de oct de 2016.

9 Informe Norton sobre Ciberseguridad 2016 - Comparaciones Globales https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf consultado el 9 de oct de 2017.

En este sentido, la divulgación de la información materia de la presente prueba de daño, potencializaría que hechos como los mencionados en el párrafo anterior ocurran respecto de los sistemas informáticos que opera el Banco de México, particularmente los sistemas de pagos, puesto que los cibercriminales contarían con los elementos necesarios para perpetrar un ataque a la información de este Instituto Central.

Identificable. *Independientemente del origen o finalidad de un ataque contra los sistemas de pagos, las tecnologías de la información, comunicaciones o infraestructura tecnológica bajo la cual operan los sistemas de pagos, podrían resultar afectadas las órdenes de transferencia en las cuentas bancarias de los distintos participantes y usuarios de los sistemas 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 personas morales.*

Adicionalmente, una disrupción en los servicios provistos por los sistemas de pagos como el Sistema de Pagos Electrónicos Interbancarios (SPEI) o el Sistema de Pagos Interbancarios en Dólares (SPID), producto de un ataque contra éstos 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, los usuarios que utilizan estos medios de pago, verían afectadas su capacidad para realizar o cumplir con el pago de bienes y servicios, y las instituciones financieras participantes en los sistemas de pagos como el SPEI o el SPID, que además de hacer uso de estos sistemas para su operación propia obtienen ingresos del cobro de comisiones por la prestación de los servicio de pagos que ofrecen estos sistemas, también resultarían gravemente perjudicadas, lo cual provocaría una seria afectación al sistema financiero.

Por lo anterior, un ataque informático a los sistema de pagos, ocasionado por dar a conocer la información relacionada con esta prueba de daño, representa un perjuicio significativo para el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias, pues de acuerdo con la información del Banco de México, en agosto 2017, se realizaron en el SPEI aproximadamente 42 millones de pagos electrónicos interbancarios por un monto de 22 mil millones de pesos[10]; lo anterior equivale a más de 6 mil operaciones por un monto de 3 mil millones de pesos por hora. Para el caso del SPID, en agosto de 2017 se realizaron aproximadamente 155 mil operaciones interbancarias en dólares entre personas morales, con un monto total transferido de aproximadamente 12 mil millones de dólares. Con base en estas cifras, es evidente que un ataque cibernético que vulnere la operación del SPEI, del SPID o sus tecnologías de la información y de comunicaciones, sin importar la duración de la disrupción, puede llegar a tener efectos cuantiosos sobre la actividad económica del país e incluso en actividad económica que forma parte de cadenas productivas globales, así como 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.

---

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

En consecuencia, proporcionar la información reservada motivo de esta prueba de daño, no aporta un beneficio al particular que sea comparable con el perjuicio que implicaría el hecho de divulgar información que en un momento dado, permita planear y perpetrar ataques cibernéticos dirigidos específicamente al SPEI, al SPID o a cualquier otro sistema de pagos administrado por este Instituto Central así como a la infraestructura relacionada con éstos, los cuales tengan como resultado la creación de mecanismos que faciliten el acceso indebido, la substracción de información 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 estos sistema de pagos. En este sentido, el riesgo de perjuicio antes señalado supera claramente el interés particular del solicitante, incluso el general de que se difunda la información solicitada.

Por otra parte, la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, *toda vez que en todo momento debe prevalecer el interés público sobre el interés particular, y como se ha dicho, la reserva de la información en comento evitará poner en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, así como también podría prevenir un daño en el buen funcionamiento de los sistemas de pagos, la creación de distorsiones en los sistemas de pagos, que se comprometan las acciones encaminadas a propiciar el buen funcionamiento del sistema de pagos, al igual que podría evitar la generación del incumplimiento de obligaciones de un participante en los sistemas de pagos.*

Dicha determinación es además proporcional considerando que, como se ha explicado, dar a conocer la información reservada materia de esta prueba de daño generaría un riesgo o daño de perjuicio significativo, el cual sería claramente mayor al beneficio particular que pudiera existir al dar a conocer dicha información.

En este orden de ideas, la reserva de la información referente a horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, resulta el medio menos restrictivo disponible para evitar el perjuicio señalado anteriormente. Por ello, se considera que dicha reserva deberá mantenerse por un plazo de cinco años, a partir de la fecha de clasificación, en razón de que la operación de los sistemas de pagos no tiene una fecha establecida de conclusión.

La referida reserva, evitaría, como se ha explicado, poner en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, así como también podría prevenir un daño en el buen funcionamiento de los sistemas de pagos, la creación de distorsiones en estos sistemas de pagos, que se comprometan las acciones encaminadas a propiciar el buen funcionamiento de éstos sistema de pagos, al igual que podría evitar la generación del incumplimiento de obligaciones de un participante en los sistemas de pagos.

Por lo expuesto, 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; 100, 103, 104, 105, 106, fracción I, 108, último párrafo, 109, 113, fracción IV, y 114 de la Ley General de Transparencia y Acceso a la Información Pública; 97, 98, fracción I, 100, 103, 104, 105, último párrafo, 106, 110, fracción IV, y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública; 1o., 2o. y 3o.,

fracción I, de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, 20, fracciones II, IV, V, VI, IX y XVI, del Reglamento Interior del Banco de México; Segundo, fracción VIII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, así como, Primero, Segundo, fracción XIII, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I, II, III y IV de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, se ha determinado clasificar como información reservada la relacionada con horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad general, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soportan el funcionamiento de los sistemas de pagos, materia de esta prueba de daño, en virtud de que su divulgación pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, y comprometería las acciones encaminadas a proveer el buen funcionamiento de los sistemas de pagos."

Con base en lo anterior, este órgano colegiado estima que la citada prueba de daño es idónea para clasificar como reservada la Información relacionada con horarios de operación, procesamiento de órdenes de transferencia y traspasos, funcionalidad específica, especificaciones técnicas, protocolos de comunicación, formatos de mensajes, esquemas de operación, procedimientos de continuidad operativa y de contingencia así como cualquier otra información relacionada con la seguridad informática que soporta el funcionamiento de los sistemas de pagos.

Lo anterior, en razón de que divulgar la información materia de la presente clasificación, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto y podría generar el incumplimiento de obligaciones de uno o más participantes en los sistemas de pagos. De igual forma, la misma podría ser analizada y utilizada por una persona o grupo de personas malintencionadas para perpetrar ataques cibernéticos dirigidos específicamente a los sistemas de pagos, lo cual posibilitaría la creación de mecanismos que faciliten el acceso indebido al propio sistema, la substracción de información relativa a sus usuarios y las operaciones que realizan, la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios de pagos electrónicos interbancarios y, en consecuencia, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto y podría generar el incumplimiento de obligaciones de un participante en los sistemas de pagos.

Adicionalmente, se debe destacar que en todo momento debe prevalecer el interés público sobre el interés particular, y como se ha dicho, la reserva de la información en comento evitará poner en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, al igual que podría evitar la generación del incumplimiento de obligaciones de uno o más participantes en los sistemas de pagos.

En consecuencia, con fundamento en los artículos 44, fracción II, 103, 105, 106, fracción I, 108, último párrafo, 109, 113, fracción IV, 114, y 137, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 98, fracción I, 100, 103, 105, último párrafo, 106, 110, fracción IV, y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, 20, fracciones II, IV, V, VI, IX y XVI, 31, fracción II, del Reglamento Interior del Banco de México; así como Primero, Segundo, fracción XIII, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero,

Vigésimo segundo, fracciones I y IV, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, este Comité de Transparencia **confirma la clasificación de la información realizada por la Gerencia de Política y Vigilancia de los Sistemas de Pagos, adscrita a la Dirección de Sistemas de Pagos del Banco de México**, identificada, fundada y motivada en la versión pública y prueba de daño referidas en el presente considerando, toda vez que se trata de información reservada, en virtud de que su divulgación pone en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, y podría generar el incumplimiento de obligaciones de uno o más participantes en los sistemas de pagos.

Por lo expuesto, con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, y 111, de la Ley General de Transparencia y Acceso a la Información Pública, 64, párrafos primero, segundo, tercero, y quinto, 65 fracciones II y IX, y 31, fracciones II y XIV, del Reglamento Interior del Banco de México, Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", emitidos por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, vigentes, y Quinta, inciso e), de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

ÚNICO. Se confirma la clasificación de información realizada por la Gerencia de Política y Vigilancia de los Sistemas de Pagos, adscrita a la Dirección de Sistemas de Pagos del Banco de México, misma que se detalla, fundamenta y motiva en la carátula y prueba de daño, de la correspondiente versión pública señalada en el oficio con referencia D10/215/2017, y también este órgano colegiado aprueba la versión pública respectiva, en términos del considerando Segundo de la presente resolución.

Así lo resolvió, por unanimidad de los integrantes presentes de este Comité de Transparencia del Banco de México, en sesión ordinaria celebrada el veintiséis de octubre de dos mil diecisiete. ------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

ABDÓN SÁNCHEZ ARROYO
Integrante