BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró , con fundamento en los artículos 3, fracción XXI, 70, 100, 106, fracción III, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 68, 97, 98, fracción III, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, fracción III, Quincuagésimo sexto, Sexagésimo segundo, inciso b) y Sexagésimo tercero de los "*Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas*", emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Lineamientos).

VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Subgerencia de Gestión de Obligaciones de Transparencia y Solicitudes de Información y Subgerencia de Análisis Jurídico y Promoción de Transparencia
II. La identificación de los documentos del que se elaboran las versiones públicas.	Acta de la sesión extraordinaria 07/2018 del Comité de Transparencia del Banco de México.
III. Firma del titular del área y de quien clasifica.	**ELIZABETH CASILLAS TREJO** Subgerente de Gestión de Obligaciones de Transparencia y Solicitudes de Información **SERGIO ZAMBRANO HERRERA** Subgerente de Análisis Jurídico y Promoción de Transparencia
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia "Especial", número 23/2018 celebrada el 12 de Julio de 2018. Secretaría del Comité de Transparencia Rodolfo Salvador Luna De La Torre, Gerente de Análisis y Promoción de Transparencia, y Secretario del Comité de Transparencia del Banco de México. Firma:

BANCO DE MÉXICO

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

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Referencia	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
1	21, 46-49	Información sobre los sistemas en los que se almacenan o tratan datos personales en el Banco de México y las acciones que se adoptarán como parte del plan de trabajo para la protección de dichos datos, descritos en el Documento de Seguridad	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

FOLIO 1

BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN EXTRAORDINARIA 07/2018
DEL 28 DE JUNIO DE 2018

En la Ciudad de México, a las once horas con treinta minutos del veintiocho de junio de dos mil dieciocho, en el edificio ubicado en avenida Cinco de Mayo, número seis, colonia Centro, delegación Cuauhtémoc, se reunieron Claudia Álvarez Toca, Directora de la Unidad de Transparencia; Humberto Enrique Ruiz Torres, Director Jurídico, y José Ramón Rodríguez Mancilla, Gerente de Organización de la Información, suplente del Director de Coordinación de la Información, todos integrantes del Comité de Transparencia de este Instituto Central, así como Rodolfo Salvador Luna de la Torre, Gerente de Análisis y Promoción de Transparencia, en su carácter de Secretario de dicho órgano colegiado. También estuvieron presentes, como invitados de este Comité, en términos de los artículos 4o. y 31, fracción XIII, del Reglamento Interior del Banco de México, así como la Tercera, párrafos primero y segundo, de las Reglas de Operación del Comité de Transparencia del Banco de México, publicadas en el Diario Oficial de la Federación el dos de junio de dos mil dieciséis, las personas que se indican en la lista de asistencia que se adjunta a la presente como **ANEXO "A"**, quienes también son servidores públicos del Banco de México.----------

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

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

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

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

---

BANCO DE MÉXICO

ÚNICO. PRESENTACIÓN DE LA PRIMERA VERSIÓN DEL DOCUMENTO DE SEGURIDAD, PREVISTO EN LOS ARTÍCULOS 3, FRACCIÓN XIV y 35 DE LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS (LGPDPPSO).----------

En desahogo de este punto del orden del día, Claudia Álvarez Toca, Directora de la Unidad de Transparencia y Presidenta de este órgano colegiado, manifestó que el veinticuatro de mayo del año en curso, en sesión extraordinaria 05/2018, este Comité aprobó el *Acuerdo por el que se determinan los criterios para establecer y mantener el Sistema de Gestión de Seguridad de Datos Personales, la política interna de gestión y tratamiento de datos personales, y otras políticas y programas de protección de datos personales*. Al respecto, destacó que en el punto SEGUNDO del referido Acuerdo quedó establecido que la elaboración y actualización periódica del Documento de Seguridad previsto en el artículo 35 de la LGPDPPSO estará a cargo, de manera coordinada, de la Unidad de Transparencia, las Direcciones de Coordinación de la Información, de Administración de Riesgos y de Control Interno, con la participación de las unidades administrativas del Banco. Por otra parte, en términos de artículo SEGUNDO transitorio del propio acuerdo, quedó establecido que la Unidad de Transparencia debería presentar a este Comité de Transparencia la primera versión del Documento de Seguridad, en el que se dé cuenta de la información existente al momento, y en el que deberá incluirse el programa de trabajo respectivo, dentro de un plazo de treinta días hábiles bancarios, contados a partir del día siguiente a la entrada en vigor del mencionado acuerdo.--------

Acto seguido, la Presidenta de este órgano colegiado solicitó se conceda el uso de la palabra Carlos Eduardo Cicero Lebrija, Gerente de Gestión de Transparencia, quien se encuentra presente en este acto, a efecto de que presente a los integrantes de este Comité la primera versión del documento de seguridad referido.----------

En uso de la voz, el referido funcionario manifestó que en atención a las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Unidad de Transparencia, en coordinación con las Direcciones de Coordinación de la Información, de Administración de Riesgos y de Control Interno, elaboraron el documento que ahora se presenta, y que es la primera versión del Documento de Seguridad del Banco de México. Acto seguido, explicó de manera detallada el contenido de dicho instrumento, que se puso a la vista de los presentes, e hizo énfasis en que el mismo será actualizado de manera periódica como resultado del proceso de mejora continua, y derivado del monitoreo y revisión que se haga del sistema de gestión, o cuando ocurra alguno otro de los eventos previstos en el artículo 36 del mencionado ordenamiento.---------

---

Al respecto, después de un amplio intercambio de opiniones, se acordó lo siguiente: ----------

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes presentes, con fundamento en los artículos 83 y 84, fracciones I, IV y V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como 4o. y 31, fracciones II, V, XVI y XX, del Reglamento Interior del Banco de México, aprueba la primera versión del Documento de Seguridad que ha sido presentado por la Unidad de Transparencia en este acto, mismo que se agrega a la presente acta como **ANEXO "C"**. Asimismo, instruye que dicho instrumento sea resguardado por la Unidad de Transparencia.----------

BANCO DE MÉXICO

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

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

RODOLFO SALVADOR LUNA DE LA TORRE
Secretario

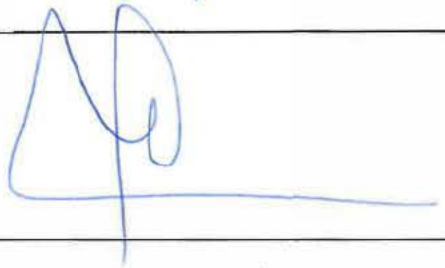
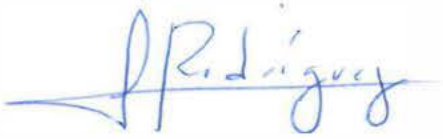
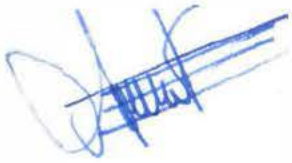
BANCO DE MÉXICO

LISTA DE ASISTENCIA

SESIÓN EXTRAORDINARIA 07/2018

28 DE JUNIO DE 2018

COMITÉ DE TRANSPARENCIA

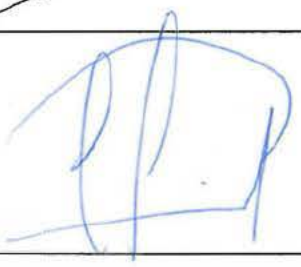
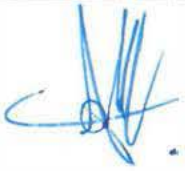
CLAUDIA ÁLVAREZ TOCA Directora de la Unidad de Transparencia Integrante	
HUMBERTO ENRIQUE RUIZ TORRES Director Jurídico Integrante	
JOSÉ RAMÓN RODRÍGUEZ MANCILLA Gerente de Organización de la Información Integrante suplente	
RODOLFO SALVADOR LUNA DE LA TORRE Secretario del Comité de Transparencia	

INVITADOS PERMANENTES

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

INVITADOS

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

MARÍA DEL CARMEN REY CABARCOS Gerente de Riesgos No Financieros	
RODRIGO MÉNDEZ PRECIADO Gerente de Enlace Institucional y Relaciones Públicas	
MARGARITA LISSETE PONCE GUARNEROS Subgerente de Identificación y Evaluación de Riesgos Operativos	
JOSÉ LUIS PÉREZ ARREDONDO Director de Control Interno	
RODRIGO VILLA COLLINS Gerente de Control Normativo	
JORGE FERNANDO GUTIÉRREZ HERNÁNDEZ Gerente de Evaluación y Seguimiento de Control	
MIRNA ESPERANZA CORTÉS CAMPOS Directora de Administración de Emisión	

APOLINAR PARRA AROCHE Director de Seguridad	
OCTAVIO BERGÉS BASTIDA Director General de Tecnologías de la Información	
JUAN FELIPE CALDERÓN MONTELONGO Titular de la Unidad de Auditoría	
MARTÍN ALFONSO CORTÉS PINEDA Gerente de Auditorías de Tecnología de Información y Especiales	
MARÍA DE LOURDES RAMÍREZ SALINAS Subgerente de Seguimiento de Auditorías y Proyectos Institucionales	
SERGIO ZAMBRANO HERRERA Subgerente de Análisis Jurídico y Promoción de Transparencia	
HÉCTOR GARCÍA MONDRAGÓN Jefe de la Oficina de Análisis Jurídico y Promoción de Transparencia	

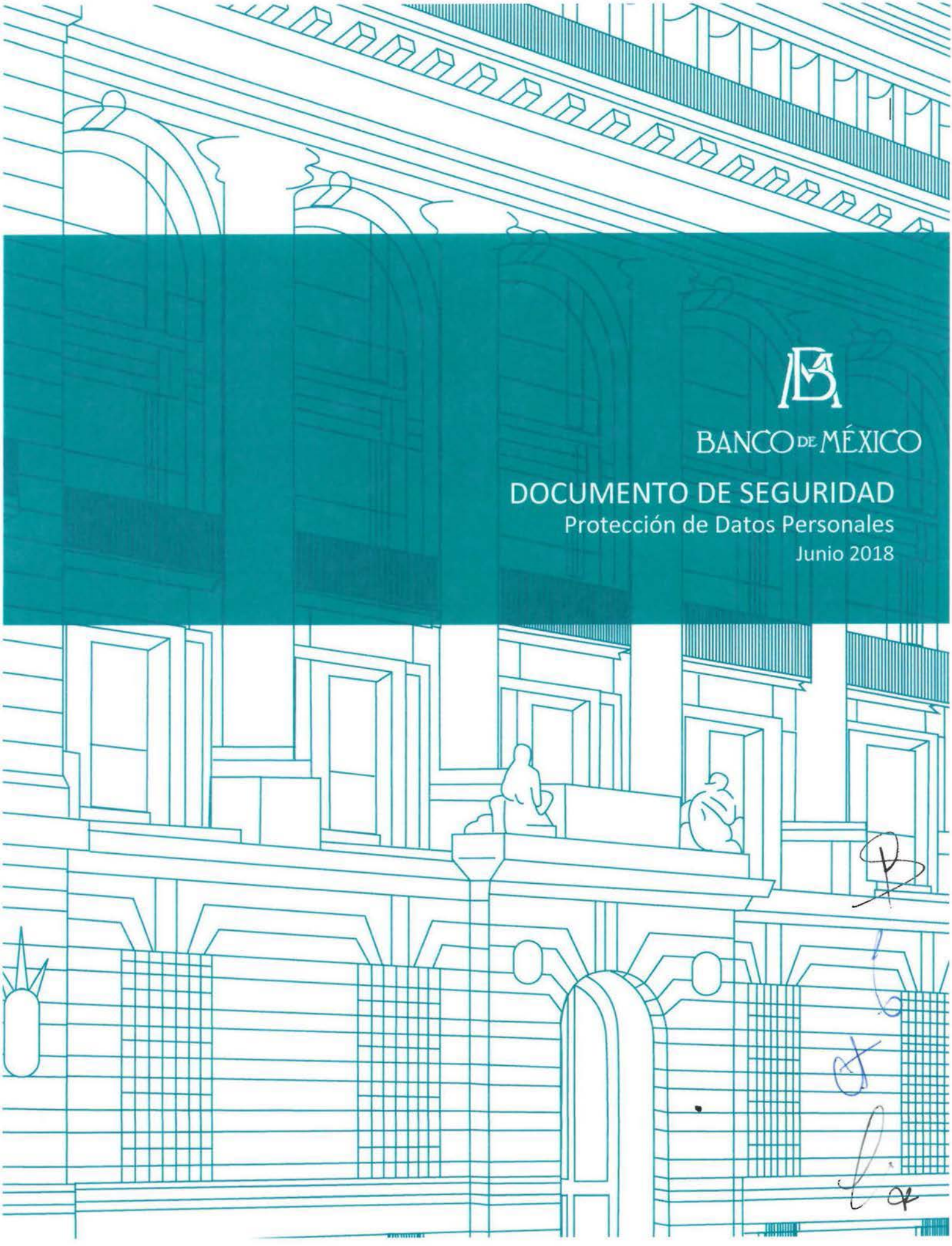
Mónica Alejandra Salcedo Tapia	

BANCO DE MÉXICO

Comité de Transparencia

ORDEN DEL DÍA
Sesión Extraordinaria 07/2018
28 de junio de 2018

ÚNICO. PRESENTACIÓN DE LA PRIMERA VERSIÓN DEL DOCUMENTO DE SEGURIDAD, PREVISTO EN LOS ARTÍCULOS 3, FRACCIÓN XIV y 35 DE LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS (LGPDPPSO).



BANCO DE MÉXICO

DOCUMENTO DE SEGURIDAD

Protección de Datos Personales

Junio 2018

UNIDADES ADMINISTRATIVAS QUE ELABORARON ESTE DOCUMENTO

Dirección General de Contraloría y Administración de Riesgos
Dirección General de Tecnologías de la Información
Unidad de Auditoría
Unidad de Transparencia

PRESENTACIÓN

La protección de la vida privada y los datos personales es un derecho humano, reconocido en los artículos 6o, Base A, fracciones II y III, y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), y en diversos tratados internacionales de los que el Estado mexicano es parte. En ese contexto, el 26 de enero de 2017, fue publicada en el Diario Oficial de la Federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), la cual entró en vigor al día siguiente.

De conformidad con el artículo 16 de la LGPDPPSO, los sujetos obligados deben observar en el tratamiento de los datos personales, entre otros, el principio de responsabilidad. El referido principio implica, de manera general, la implementación de acciones como: medidas de seguridad para la protección de datos personales (administrativas, técnicas y físicas); la rendición de cuentas sobre el tratamiento de datos personales; el establecimiento de esquemas de autorregulación, incluidos programas y políticas; sistemas de administración de riesgos; programas de capacitación y actualización del personal; el establecimiento de un sistema de supervisión y vigilancia, y la revisión periódica de las políticas y programas establecidos.

Las mencionadas acciones integran el denominado Sistema de Gestión de Seguridad de Datos Personales (Sistema de Gestión), el cual es entendido como un conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

En el contexto del referido Sistema de Gestión, el artículo 35 de la LGPDPPSO establece el deber de los responsables de elaborar el denominado **Documento de Seguridad**, en el cual los sujetos obligados han de dejar constancia de la parte medular del propio sistema, incluido el plan de trabajo que permitirá fortalecer, en el corto y mediano plazo, la seguridad en el tratamiento de los datos personales.

Por su naturaleza, el Documento de Seguridad, al igual que el Sistema de Gestión en su conjunto, es dinámico, ya que debe ser actualizado permanentemente como resultado del proceso de mejora continua, el cual es, a su vez, consecuencia del monitoreo y revisión periódica del propio sistema. En este sentido, el Documento de Seguridad da cuenta de las políticas, objetivos, riesgos, planes, procesos y procedimientos existentes, y prevé la evaluación y medición.

Además, el referido instrumento debe ser actualizado cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo; como parte de un proceso de mejora para mitigar el impacto de una vulneración, o para la implementación de acciones correctivas y preventivas.

En el marco anterior, el Banco de México, a través de su Unidad de Transparencia, la Dirección General de Tecnologías de la Información, y la Dirección General de Contraloría y Administración de Riesgos, ha elaborado el presente Documento de Seguridad, el cual fue presentado a la consideración del Comité de Transparencia de dicho Instituto Central, como máxima autoridad de la materia, en sesión extraordinaria 07/2018 de fecha 28 de junio de 2018.

Conforme al aludido carácter dinámico, el presente Documento de Seguridad será actualizado como producto de la mejora continua del Sistema de Gestión, y la ejecución del Plan de Trabajo que forma parte del mismo.

CONTENIDO

INTRODUCCIÓN

En los últimos años, el creciente avance de la tecnología ha propiciado cambios fundamentales en los procesos y modelos de negocio al interior de las organizaciones financieras, de distintos tamaños y en diferentes latitudes. Estos avances, sin duda, han contribuido a introducir eficiencias operativas y ahorros de costos. Banco de México no es la excepción, al igual que otros bancos centrales, está cada vez mejor interconectado, y utiliza sistemas de tecnologías de información más complejos. Sin embargo, el uso de dichas tecnologías también conlleva mayores riesgos.

En un entorno digital cada vez más interconectado, las brechas de seguridad en las Tecnologías de la Información y la Comunicación (TIC) pueden producir consecuencias no deseadas en la operación y, por ende, en la reputación del Banco de México y el sistema financiero del país. Las amenazas que pueden ocasionar la interrupción de la operación de las instituciones son cada día más evidentes y sofisticadas, independientemente de las acciones preventivas en materia de seguridad de la información y de las TIC, tanto la evidencia histórica[1,2,3,4], como las recientes intrusiones cibernéticas a nivel internacional sugieren que prácticamente todas las industrias, y particularmente los servicios financieros, son susceptibles a posibles eventos de pérdida.

Ante la responsabilidad de gestionar el riesgo no financiero[5], Banco de México ha instrumentado de forma proactiva un programa de fortalecimiento de la seguridad de la información, y datos personales, el cual comprende: inventario de activos de información[6] y datos personales; análisis de riesgos; arquitectura de seguridad, y la capacitación y concientización que habiliten al personal del Banco a ser vigilantes en el manejo seguro de la información.

Las acciones de protección definidas reducirán el riesgo para los sistemas, datos e información; sin obstaculizar la innovación y la colaboración en el manejo de los mismos.

---

[1] India's City Union Bank CEO says suffered cyber hack via SWIFT system - http://reut.rs/2F7r21F
[2] SWIFT to Advise Banks on Security as Bangladesh's central bank Hack Details Emerge - http://bit.ly/2FgZYAv
[3] Central banks seek better security on inter-bank payments - http://reut.rs/2F3gkxo
[4] Mexican authorities probe hack of export bank: official - http://reut.rs/2F1KiSt
[5] Por riesgo no financiero se entiende a la afectación en la ejecución de los procesos, la información y otros recursos a cargo del Banco de México, ocasionada por factores humanos, organizacionales, de equipamiento y tecnologías de información, o externos al Banco; entre otros incluye el riesgo operativo, riesgo de seguridad de la información y el riesgo de seguridad física.
[6] Activo de Información: Información necesaria para el ejercicio de las atribuciones y/o facultades del Banco, así como para el cumplimiento de sus obligaciones.

ANTECEDENTES

La información es un recurso fundamental para la toma de decisiones y el ejercicio de las atribuciones del Banco de México. Por ello se considera un activo institucional, y el Banco lleva a cabo actividades para su protección, a partir de la identificación de los riesgos asociados al mismo. Los factores que representan un reto para la realización de esfuerzos en materia de gestión de riesgo no financiero asociado a la protección de información del Banco de México incluyen los siguientes factores:

- Complejidad operacional,
- Uso generalizado de la tecnología,
- Dependencia incremental en activos intangibles, tales como información digital y software, y
- Cumplimiento regulatorio y requerimientos legales.

Para atender dichos factores, el Banco ha instrumentado distintas iniciativas de aplicabilidad transversal que fortalecen los esfuerzos encaminados a proteger la información y los datos personales.

Gestión por procesos y Arquitectura Empresarial en Banco de México

La identificación de procesos constituye la base a partir de la cual, las Unidades Administrativas encargadas de su ejecución, gestionan los riesgos no financieros a los que están expuestas. El objetivo es contar con un Catálogo Institucional de Procesos que incluya todos los procesos que se llevan a cabo en el Banco, que sirva de guía para definir los programas de trabajo no sólo para la identificación y documentación normativa basada en procesos, sino también para la administración de riesgos, el seguimiento de los puntos de control a nivel institucional y la mejora normativa.

En la identificación del proceso se presentan de manera simple y ordenada los subprocesos y actividades que los conforman, de manera que se delimiten los responsables de su ejecución, y se identifiquen sus interrelaciones con otros procesos. En adición, se identifican las Actividades de Control Relevante (ACR), las cuales ayudan a mitigar un riesgo, toda vez que definen un procedimiento claro de ejecución, y aseguran la segregación de funciones, y la generación y resguardo de la evidencia o registro documental de su ejecución. Conforme a este sistema de gestión se establecen y documentan los roles y responsabilidades de las personas participantes en los procesos y la cadena de rendición de cuentas para efectos de cada uno de los procesos.

El entendimiento de los procesos facilita la identificación y evaluación de los riesgos no financieros a los que están expuestos y que, de materializarse, podrían afectar la entrega o provisión de los productos o servicios intermedios y finales que de éstos se generen.

El Catálogo Institucional de Procesos busca determinar todos los macro procesos y procesos por medio de los cuales cada Unidad Administrativa da cumplimiento a sus atribuciones. Dentro del citado Catálogo se han establecido definiciones para homogeneizar y estandarizar criterios al momento de identificar y clasificar los mencionados macro procesos. De esta forma, un macro

proceso se define como la agrupación de varios procesos que contribuyen a una función común. Al día de hoy, el Banco cuenta con un Catálogo Institucional de Procesos compuesto por 26 macro procesos y 98 procesos.

Asimismo, es importante señalar que los procesos en el Banco están documentados en una ficha de soporte, que contiene la información más relevante respecto a lo siguiente:

- Nombre: Nombre con el que se identifica al macro proceso.
- Propósito: Objetivo primordial que persigue la institución con la ejecución del proceso.
- Ejes Rectores y Objetivos Institucionales: Nombre de los ejes rectores y objetivos institucionales en los cuales participa el macro proceso.
- Unidades Administrativas Participantes: Las Unidades Administrativas que son responsables del proceso y las áreas involucradas en su ejecución. Puede ser desde nivel dirección general hasta oficinas.
- Marco Jurídico y Normatividad Asociada: Describe la normativa asociada al proceso, incluyendo: CPEUM; Ley del Banco de México; leyes federales o locales que pudieran serles aplicables; Reglamento Interior del Banco de México; Normas administrativas internas, Manuales generales de macroprocesos, Manuales de procedimientos de operación, etc.
- Soluciones de tecnologías de información (TI): Describe las soluciones de TI de uso específico y las transversales.
- Procesos vinculados: Describe los procesos de aplicación específica y los transversales que se relacionan con el macro proceso que se está identificando.
- Productos o servicios intermedios: Describe los productos o servicios intermedios que se generan al ejecutar los procesos del macro proceso.
- Productos o servicios finales: Describe las salidas de la ficha de flujo general del macro proceso.
- Entradas: Describe las entradas de la ficha de flujo general del macro proceso.
- Organismos Externos Relacionados: Entidades externas que participan directamente en el proceso.

Protección de Información

Banco de México continuamente fortalece su programa de seguridad de la información, con el fin de implementar un modelo más proactivo y amplio de seguridad de la información y protección de datos personales. Asimismo, estableceremos un sistema de vanguardia que sea referente para otras autoridades y participantes en el sistema financiero. El programa contempla que el Banco desarrolle capacidades para identificar vulnerabilidades potenciales, mitigar aquellas que sea factible, y reaccionar ágilmente en caso de ataques, dentro y fuera de la Institución, con una perspectiva de protección de la información. La cultura de seguridad del Banco evolucionará de un enfoque reactivo diseñado para protegerse y defenderse de ataques, a uno preventivo, que de manera activa y supervisada identifique las amenazas.

Protección de Datos Personales

A partir de la publicación del Decreto por el que se expidió la LGPDPPSO, el 26 de enero de 2017, durante el primer trimestre de 2017 se instrumentaron medidas al interior del Banco para obtener información de las Unidades Administrativas del Banco que tratan datos personales[7].

Este esfuerzo consistió en identificar en conjunto con las Unidades Administrativas del Banco los datos personales en su posesión y aspectos relevantes tales como los siguientes:

- Nombre del sistema o archivo físico de almacenamiento que contiene datos personales;
- Tipo de dato personal que se posee por ejemplo: nombre, edad, domicilio, correo electrónico, RFC, CURP, estado de salud, etc;
- Fuente de la que se obtienen los datos;
- Procedimiento empleado para el tratamiento, y
- Formato en que se contienen los datos.

El referido inventario de datos personales contribuirá a los análisis para determinar las medidas que, en su caso, el Banco adoptará para garantizar la integridad y seguridad de los datos personales que son objeto de tratamiento por parte de sus Unidades Administrativas en el ejercicio de sus facultades y atribuciones.

Los datos personales son tratados por diversas Unidades Administrativas del Banco y son almacenados en distintos tipos de repositorios, tales como archivos físicos, sistemas y aplicaciones del Banco, archivos electrónicos, etc. [redacted]

[redacted]

De igual manera, a través de la implementación del "*Acuerdo del Comité de Transparencia: por el que se establecen los formatos de avisos de privacidad del Banco de México*", así como la generación

[7] El tratamiento de acuerdo con la LGPDPPSO se define como: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados, aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

de los respectivos Avisos de Privacidad,[8] se cuenta con la información respecto de los medios a través de los cuales se obtienen los datos personales, la finalidades de su tratamiento, el catálogo de tipos de datos (identificando si son sensibles o no), las unidades administrativas que llevan a cabo el tratamiento, así como, en su caso, las transferencias de los mismos.

a) Medidas de seguridad

El artículo Séptimo transitorio de la LGPDPPSO establece que *"Los sujetos obligados correspondientes deberán tramitar, expedir o modificar su normatividad interna a más tardar dentro de los dieciocho meses siguientes a la entrada en vigor de esta Ley."*. En ese sentido, el Banco ha estado realizando las gestiones correspondientes para tramitar, expedir y modificar la normatividad interna necesaria para establecer el Sistema de Gestión previsto en los artículos 12, fracción IV, y 34 de la LGPDPPSO, en el cual deben estar contenidos los elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, y mejorar el tratamiento y seguridad de los datos personales.

A continuación, se destacan las medidas de seguridad existentes, la mayoría de las cuales fueron implementadas con anterioridad a la entrada en vigor de la LGPDPPSO.

a. Medidas administrativas[9]:

1. La normatividad interna del Banco de México (en particular, "Provisión de Servicios de Tecnologías de la Información"[10] y "Tecnologías de Información para Usuarios"[11]) considera medidas de seguridad aplicables a la información que se trata en la institución, tanto en los sistemas de cómputo y telecomunicaciones, como en los desarrollos de aplicativos adquiridos o de manufactura interna. Estas medidas de seguridad administrativa aplican a la provisión y el uso de servicios de Tecnologías de la Información (TI). Otras políticas relacionadas con el tratamiento de datos personales se encuentran en los "Lineamientos para Borrar Datos en las ETB" y el "Manual de Procedimientos de Operación Centros de Cómputo".

2. Asimismo, el Banco cuenta con una norma administrativa interna denominada "Organización y gestión de los documentos de archivo del Banco de México"[12] emitida para identificar, catalogar y resguardar, por el plazo de conservación que le corresponda, la documentación que da evidencia del ejercicio de sus funciones. Además, regula la gestión de los documentos durante su ciclo de vida, desde su generación hasta la aplicación de su

[8] Disponibles en el sitio de internet oficial del Banco de México, a través del enlace siguiente: http://www.banxico.org.mx/ley-de-transparencia/aviso-privacidad.html

[9] Se incluyen las ligas a la normatividad vigente a la fecha de la elaboración del presente *"Documento de Seguridad"*. En caso de que dicha normatividad sufra cambios en el futuro, la normatividad vigente del Banco de México podrá consultarse a través del Portal de Obligaciones de Transparencia, en el apartado "Marco Normativo".

[10] http://transparencia.banxico.org.mx/documentos/{F9B5A0B2-78BD-733F-452E-F502F012E7E0}.pdf

[11] http://www.banxico.org.mx/documentos/%7B54524F82-F9A1-472F-80C0-63F98C81719F%7D.pdf

[12] http://transparencia.banxico.org.mx/documentos/%7B698F7CB3-6CCA-DC9E-8572-9A6365F0EEE3%7D.pdf

destino final, eliminación o conservación permanente, así como la forma en que se otorgarán derechos de consulta a documentos de archivo. En razón de que esta norma establece procedimientos respecto de documentos, a través de la misma se gestiona el ciclo de vida de los datos personales tratados por el Banco de México.

3. Otras normas que contienen políticas relacionadas con la gestión, soporte y revisión de la seguridad de la información a nivel organizacional; la identificación, clasificación y borrado seguro de la información, son las siguientes:

NORMA	MATERIA	VÍNCULO
Norma Administrativa Interna: *"Normas bajo las cuales los servidores públicos del Banco de México deberán presentar declaraciones de situación patrimonial y de datos curriculares"*	Establece los términos en que se deberá presentar la declaración de situación patrimonial por parte de las personas obligadas. Al respecto, en su norma TERCERA prevé: "El sistema 'DEPTEL' deberá garantizar, bajo cualquier circunstancia, la confidencialidad e integridad de la información contenida en él, misma que deberá mantenerse debidamente respaldada."	NAI: Normas bajo las cuales los servidores públicos del Banco de México deberán presentar declaraciones de situación patrimonial y de datos curriculares
Norma Administrativa Interna: *"Operación en situaciones de alerta"*	Prevé (en la disposición Octava, segundo párrafo) que se deberá garantizar la confidencialidad de los datos personales incluidos en el directorio de datos de contacto: "El 'Responsable de continuidad operativa' deberá contar con un directorio con los datos de contacto que permita la localización de los 'Trabajadores' que participan en la ejecución de los 'Procesos' de la 'Unidad administrativa' a cargo del 'Funcionario facultado'. Para estos efectos, deberá tomar las medidas necesarias para tener acceso a dicho directorio, mantenerlo actualizado, así como garantizar la confidencialidad de los datos personales ahí incluidos"	NAI: Operación en situaciones de alerta
Norma Administrativa Interna: *"Auditoría Interna "*	Establece la obligación del personal de auditoría de señalar en sus papeles de trabajo cuando la información del área auditada haya sido reportada como reservada o confidencial. "TRIGÉSIMA SEGUNDA. Papeles de trabajo Durante la ejecución de las auditorías, se deberán elaborar los correspondientes papeles de trabajo, los cuales deberán contar con las marcas de auditoría, índices y cruces respectivos. Dichos papeles de trabajo serán supervisados por el 'Personal de Auditoría' designado responsable del grupo de auditores. Cuando los papeles de trabajo contengan información que la 'Unidad Administrativa' auditada haya reportado como reservada o confidencial, deberá indicarse expresamente y de forma	NAI: Auditoría Interna

	llamativa en dichos papeles en su parte superior o inferior."	
Manual General de Macroproceso: *"Información y Transparencia".*	Se regula la administración y publicación de la Información institucional, la administración de los archivos de concentración e histórico del Banco, así como la atención de solicitudes de información. En este sentido el manual prevé medidas de seguridad para el manejo de la información de la Institución, dentro de la que se encuentran datos personales.	MGM: Información y Transparencia
Manual General de Macroproceso: *"Registro y control normativo"*	Prevé el registro y resguardo de la información de los servidores públicos que presentan en sus declaraciones patrimoniales.	MGM: Registro y control normativo
Manual de Procedimientos de Operación: *"Administración de antivirus para servidores y computadoras personales".*	Regula los procesos relativos al aseguramiento de la calidad, instalación, actualización y monitoreo del producto antivirus dentro de las computadoras personales y servidores con sistema operativo Microsoft Windows propiedad del Banco de México, algunos de estos equipos de cómputo almacenan, entre otros, datos personales.	MPO: Administración de antivirus para servidores y computadoras personales
Manual de Procedimientos de Operación: *"Servidor de base de datos Oracle y componentes del ERP".*	Regula, entre otros aspectos, el manejo de la información de algunas bases de datos que contienen datos personales.	MPO: Servidor de base de datos Oracle y ERP
Manual de Procedimientos de Operación: *"Detección y manejo de vulnerabilidades".*	Establece procedimientos de operación para la detección y manejo de vulnerabilidades informáticas de software en equipos en telecomunicaciones y cómputo, a través de los cuales pueden ser tratados datos personales.	MPO: Detección y manejo de vulnerabilidades
Manual de Procedimientos de Operación: *"Control de bienes informáticos".*	Regula la recepción, administración, distribución y control de los bienes informáticos del Banco de México, lo que permite revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware de los equipos que contengan datos personales.	MPO: Control de bienes informáticos
Manual de Procedimientos de Operación: *"Centros de cómputo".*	Regula el acceso a los sitios de alta seguridad con control de acceso restringido, administrado por la Dirección de Sistemas en donde se encuentran operando algunos equipos de cómputo que almacenan, entre otros, datos personales. Asimismo, regula el uso, operación y administración de los centros de cómputo.	MPO: Centros de cómputo
Manual de Procedimientos de Operación: *"Administración de usuarios y computadoras de dominio".*	Regula el uso y administración del Directorio Institucional en donde se registran las cuentas de Usuarios, grupos de control de acceso a los recursos de información y los propios recursos informáticos, el cual permite asegurar la identidad de los usuarios y definir los mecanismos formales para mantener actualizados	MPO: Administración de usuarios y computadoras de dominio

	los grupos a través de los cuales se da acceso a la información y sistemas en el Banco de México.	
Manual de Procedimientos de Operación: *"Evaluación de riesgos operativos"*.	El manual regula la metodología mediante la cual la Dirección de Administración de Riesgos realiza la evaluación de riesgos operativos en la Institución.	MPO: Evaluación de riesgos operativos
Manual de Procedimientos de Operación: *"Registro de servidores públicos"*.	Regula el registro de servidores públicos obligados a presentar declaraciones de situación patrimonial y curricular, así como los sistemas y depósitos institucionales en donde se resguarda la información de sus declaraciones entre las que se encuentran datos personales.	MPO: Registro de servidores públicos
Manual de Procedimientos de Operación: *"Administración de datos del personal"*	Regula, entre otros aspectos, la captura, consulta y registro de datos a través de los sistemas internos, y la administración del Expediente Único de Personal y del Expediente de Crédito Hipotecario.	MPO: Administración de datos personal
Manual de Procedimientos de Operación: *"Control del archivo de concentración"*.	Regula las actividades del archivo de concentración relativas a la custodia temporal, consulta de documentos de archivo, devolución de documentos de archivo en custodia y destino final de documentos de archivo.	MPO: Control del archivo de concentración
Manual de Procedimientos de Operación: *"Atención de solicitudes de acceso a la información"*.	Se regulan las actividades para dar atención a las solicitudes de acceso a la información.	MPO: Atención de solicitudes de acceso a la información
Acuerdo del Comité de Transparencia: por el que se establecen los formatos de avisos de privacidad del Banco de México[13]	Estandarizar el formato de los avisos de privacidad que lleguen a elaborar y utilizar las diferentes unidades administrativas del Banco en el ejercicio de sus funciones y procurar que estos se apeguen a la ley.	Acuerdo de establecimiento de formatos de avisos de privacidad

b. Medidas físicas:

El Banco de México tiene instalada la capacidad tecnológica necesaria para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. Al respecto, cuenta con un "Macroproceso de Seguridad Física"[14] debidamente documentado, el cual tiene como propósito coordinar y ejecutar las actividades correspondientes para salvaguardar los valores, al personal y las instalaciones de Banco de México, el cual es de observancia general. Asimismo, el Banco de México cuenta con una Norma Administrativa Interna que regula la entrada, permanencia y salida de las instalaciones, tanto de trabajadores como de terceros (Norma Administrativa Interna: *"Entrada*

[13] Esta medida de seguridad fue implementada posterior a la promulgación de la LGPDPPSO. El Acuerdo del CT se emitió el 11 de octubre de 2017.

[14] http://transparencia.banxico.org.mx/documentos/%7B073AD0C5-82F1-5BFE-5DFB-A1774D5967E6%7D.pdf

permanencia y salida a los inmuebles que ocupe el Banco de México, así como el control de sus bienes muebles"[15]).

Entre las medidas físicas, destacan las siguientes:

1. Sistemas de control de acceso automatizados los cuales sólo permiten a empleados del Banco de México realizar solicitudes de acceso. Para tal efecto, deben utilizar una clave de usuario y una contraseña, de tal manera que ninguna persona ajena al Banco puede autorizar el acceso a los inmuebles del Banco de México. Además, dichos accesos son autorizados con nivel mínimo de Jefe de Oficina.

2. Las personas que ingresan a las instalaciones del Banco Central son debidamente identificadas, y se les asigna una credencial que sólo permite el acceso a las áreas autorizadas, lo cual es controlado con barreras físicas y lectoras. (Al respecto, se encuentra establecida la Norma Administrativa Interna: *"Medidas de seguridad para el control de acceso de los proveedores y contratistas, así como del personal a su cargo, a los inmuebles que ocupe el Banco de México"*[16])

3. Se previene el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.

4. Se protegen los recursos móviles portátiles y cualquier soporte físico o electrónico que pueda salir de la organización.

5. Se encuentran instaladas barreras físicas en los puntos de ingreso peatonal y vehicular que permiten evitar el ingreso forzoso o no autorizado como son:

    a. Puertas de nivel medio y nivel alto de seguridad, liberadas por medio de la credencial de empleado o visitante cuando está autorizado.

    b. Barreras físicas (pilonas).

    c. Plumas de acceso, las cuales son liberadas por medio de la credencial del trabajador, cuando está autorizado, o de manera manual por personal de seguridad de servicio en los puntos de acceso a los inmuebles.

    d. Detección de intrusión en los diferentes inmuebles que permiten de manera amplia y segura poder detectar a tiempo cuando exista un posible intento de intrusión.

    e. Cámaras que conforman el circuito cerrado de televisión para la evaluación de las diferentes situaciones con grabación las 24 horas del día.

[15] http://transparencia.banxico.org.mx/documentos/%7B13CDA36C-1F35-BF0A-44C8-1F322996A66F%7D.pdf
[16] http://transparencia.banxico.org.mx/documentos/%7B5C1A0144-AD39-EC4F-BDE2-8BC98179D93C%7D.pdf

f. Detección de incendio y sistema de voceo, los cuales permiten reaccionar a tiempo ante cualquier evento de emergencia por incendio y/o sismo y mantener informado al personal del seguimiento del evento.

g. Los sistemas mencionados anteriormente, envían señal a los Centros de Coordinación y Control instalados en los inmuebles del Banco que operan con personal propio para la detección temprana para cualquier emergencia que se presente. Cabe hacer mención que estas herramientas son empleadas por personal del propio Instituto Central debidamente capacitado para la atención de los diferentes temas que atañen a la seguridad institucional, así como para el uso y operación de los sistemas mencionados.

h. Requerimiento de autorización de acceso y control dual para actividades específicas.

i. Uso de celdas para el resguardo de determinada información con controles de acceso y vigilancia a través de circuito cerrado de televisión.

c. Medidas tecnológicas:

Banco de México cuenta con tecnología para proteger el entorno digital de la información que se gestiona en sus procesos, incluyendo los datos personales y los recursos involucrados en su tratamiento, entre éstos destacan los siguientes:

1. Acceso a equipo de cómputo personal exclusivamente con cuentas individualizadas y sus respectivas contraseñas.

2. Acceso a las bases de datos o a la información, así como a los recursos, los cuales deben ser por usuarios identificados y autorizados.

3. Esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.

4. Activación automática del protector de pantalla, protegido con la contraseña de servicios.

5. Distribución automática de actualizaciones de software.

6. Antivirus y Firewall personal.

7. Restricción de uso de software no certificado.

8. Configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.

9. Se provee a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, al igual que a los equipos que no los contienen, procurando que se asegure su disponibilidad e integridad.

10. Control de acceso en la navegación a internet, o desde éste.

11. Cifrado y encriptación en comunicaciones institucionales.

12. Protección contra código malicioso en los servicios de tecnologías de la información.

13. Borrado seguro de los datos contenidos en los discos duros, tanto de los equipos de cómputo personal, como de los servidores del Banco de México.

14. Gestión de las comunicaciones, operaciones y medios de almacenamiento de la información.

15. Autenticación mediante certificados digitales y cifrado asimétrico de información mediante llaves públicas y privadas.

16. Bitácoras de consulta de información en los sistemas.

17. De manera particular, tratándose de los sistemas de pagos administrados por el Banco de México, la protección de los datos personales se lleva a cabo a través de la implementación de mecanismos y procedimientos de seguridad robustos, basados en lineamientos y estándares internacionales. Por ejemplo, en el caso concreto del Sistema de Pagos Electrónicos Interbancarios (SPEI®), que es el sistema de pagos más importante de nuestro país, se siguen políticas de seguridad a nivel institucional, las cuales están armonizadas con normas internacionales, particularmente el ISO/IEC 27001[17] (estándar que determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información). Adicionalmente, el SPEI utiliza mecanismos de firma digital para proteger las transacciones que procesa el sistema. Estos mecanismos están basados en estándares de seguridad internacionales para la autenticación, firmado y cifrado de información, entre las cuales se puede mencionar:

    a. Formato de certificados basados en el estándar X.509v3 (RFC 3280[18]).
    b. Claves privadas tipo RSA basadas en el estándar1 PKCS #1 (RFC 2313[19]).
    c. Generación de firmas digitales y su verificación de acuerdo con el estándar PKCS #1.

b) Mecanismos de monitoreo

En lo que respecta a los mecanismos de monitoreo, debe destacarse que la Unidad de Auditoría, de acuerdo con el Reglamento Interior del Banco de México, cuenta con atribuciones que le permiten monitorear la gestión del Banco en materia de datos personales. Puntualmente, el art. 29 Bis 1 Fr. IV, señala:

[17] https://www.iso.org/isoiec-27001-information-security.html
[18] https://www.ietf.org/rfc/rfc3280.txt
[19] https://www.ietf.org/rfc/rfc2313.txt

"IV. Verificar a través de auditorías, la aplicación de los criterios para el manejo, mantenimiento, seguridad y protección de los datos personales que estén en posesión de las Unidades Administrativas del Banco, así como de la información en general;"

Adicionalmente, durante 2017 la Dirección de Control Interno instrumentó la evaluación bienal del Sistema de Control Interno institucional, en la que se incorporaron métricas para estimar el estado del control relativo al conocimiento de la LGPDPPSO y a las acciones que, en su caso, han identificado e implementado las Unidades Administrativas del Banco de México que participaron en dicha evaluación, para atender las nuevas obligaciones en esa materia. El nivel de conocimiento y aplicación del Sistema de Control Interno en la Institución es alto (dentro de una escala de cinco posibles estados de control: incipiente, medio, adecuado, alto y avanzado).

c) Capacitación

De conformidad con lo dispuesto en el artículo 3, fracción XXI, de la LGPDPPSO, la capacitación del personal en materia de protección de datos personales forma parte de las medidas de seguridad administrativas que deben adoptar los responsables, en cumplimiento al principio de responsabilidad.

Al respecto, de manera concreta, el referido ordenamiento prevé que se deberá poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales (art. 30, fracción III, LGPDPPSO), y diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades y funciones respecto del tratamiento de los datos personales (art. 33, fracción VIII, LGPDPPSO).

En relación con lo anterior, respecto de la capacitación a corto y mediano plazo, debe destacarse que el Programa de Capacitación[20, 21] para el ejercicio 2017 fue aprobado por el Comité de Transparencia del Banco de México, en sesión 09/2017, de 19 de abril de 2017, y remitido en esa misma fecha a la Dirección General de Capacitación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

El programa de capacitación referido comprendió expresamente la materia de Protección de Datos Personales, y particularmente la LGPDPPSO.

En términos del programa mencionado, los días 9, 10 y 11 de octubre de 2017, el Banco de México participó como institución sede del curso Introducción a la Ley General de Protección de Datos

---

[20] En la siguiente liga puede consultarse, entre otra información, el acta de dicha sesión y la documentación correspondiente al mencionado programa. http://www.banxico.org.mx/documentos/%7BE7D8B46C-AA2D-12F0-CF23-CA325DB60D93%7D.pdf

[21] El referido programa de capacitación fue objeto de diversos ajustes, tal como se desprende del acta de la sesión extraordinaria 08/2017, de 30 de noviembre de 2017, la cual se encuentra visible en la siguiente liga: http://transparencia.banxico.org.mx/documentos/%7BF138C85A-9954-B305-9795-70965E6257AB%7D.pdf

Personales en Posesión de Sujetos Obligados, organizado por el INAI y la Universidad Iberoamericana, A.C.

En total en el referido ejercicio fueron capacitados 192 servidores públicos de este Banco Central en la ley mencionada, quienes recibieron la constancia oficial respectiva. Cabe señalar que, para la convocatoria al curso referido, fueron considerados los roles de las áreas participantes respecto al tratamiento de datos personales.

Por lo que se refiere al ejercicio 2018, el 7 de junio de 2018, el Comité de Transparencia, en sesión extraordinaria 06/2018, aprobó el programa de capacitación correspondiente, el cual fue enviado al INAI en esa misma fecha, en la forma y términos establecidos por dicho Instituto Nacional. Al respecto, debe destacarse que en ese programa se contempla la capacitación de 633 servidores públicos en el curso de introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 14 servidores públicos en el curso de capacitación especializada en Protección de Datos Personales (Documento de Seguridad).

Por otra parte, en el mismo rubro de capacitación, debe destacarse que como parte de las acciones para garantizar el derecho a la protección de los datos personales en este Banco Central, el Comité de Transparencia, como máxima autoridad en la materia, emitió el "Acuerdo por el que se establece la obligación de los servidores públicos del Banco de México de participar en los cursos de capacitación en materia de Transparencia, Acceso a la Información, Protección de Datos de Personales y temas relacionados, conforme al programa de capacitación que establezca este órgano colegiado, o a través de la Unidad de Transparencia para el año correspondiente".

PROGRAMA DE FORTALECIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES EN BANCO DE MÉXICO

Banco de México ha instrumentado un programa transversal al interior de la Institución con el objetivo de reforzar la seguridad de la información y protección de datos personales, que en conjunto con las medidas de seguridad señaladas, opere como Sistema de Gestión de la información. Como parte de dicho programa, se pretende fortalecer la cultura organizacional en la materia a fin de que cada trabajador esté consciente y asuma su correspondiente responsabilidad.

Alcance

Los procesos definidos al interior son un recurso importante que Banco de México utiliza como herramienta para cumplir su finalidad y objetivos. Cada proceso tiene un propósito cuyo cumplimiento respalda el logro de los objetivos institucionales que, a su vez, están alineados a los ejes rectores del Banco. El propósito de este programa es fortalecer la seguridad de los activos de información de los procesos en función de su valor y considerando el perfil de riesgo de Banco de México.

Particularmente, el programa persigue las siguientes metas:

- Identificar y proteger los activos de información y los datos personales,
- Proporcionar elementos para fortalecer la toma de decisiones para la protección de los activos de información, en función del riesgo a la seguridad de la información y a los datos personales, y
- Promover un comportamiento vigilante y proactivo que contribuya a reforzar una cultura en materia de seguridad de la información.

Este programa será implementado por fases a lo largo de todos los procesos del Banco, involucrando a todas las unidades administrativas a lo largo de su instrumentación.

Normatividad

Banco de México ha desarrollado una propuesta de norma administrativa interna que asigna responsabilidades a los trabajadores en materia de seguridad de la información y protección de datos personales, la identificación de esta información a través de categorías de seguridad, así como los lineamientos de manejo seguro de esta información.

Entre las responsabilidades en materia de seguridad de la información se prevén las siguientes:

- Identificación y categorización de seguridad de la información de los procesos,
- Identificación y categorización de datos personales tratados en los procesos,
- Identificación y categorización de seguridad de los sistemas de información,
- Identificación y categorización de seguridad los sistemas de tratamiento de datos personales,
- Consolidación y mantenimiento del inventario de activos de información e inventario de datos personales,
- Análisis de impacto y de los riesgos en el tratamiento de los datos personales acorde a las políticas establecidas por el Comité de Transparencia,
- Definición de las medidas de seguridad para la información, los datos personales, y los sistemas de información que los tratan, a partir de un análisis de brecha,
- La generación y actualización de un plan de seguridad por sistema de información que contenga:
    - Contexto del proceso,
    - Inventario de activos de información,
    - Inventario de datos personales que se tratan en el sistema de información,
    - Documentación técnica de los sistemas de información que soportan el proceso,
    - Medidas de seguridad para el sistema de información,
    - Listado de los controles administrativos, técnicos o físicos implementados,
    - Documentación de la brecha existente en la implementación de los controles, y
    - Plan para instrumentar controles faltantes.

Como política interna para la gestión y tratamiento de los datos personales, se han definido las siguientes responsabilidades:

1. En la gestión y el tratamiento de datos personales los servidores públicos del Banco de México deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, conforme a la LGPDPPSO, los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales), y demás disposiciones aplicables. Los servidores públicos que tengan personal a su cargo, además deberán supervisar el cumplimiento de dichos principios por parte de sus subordinados y adoptar las medidas necesarias para su aplicación.

2. La gestión y el tratamiento de datos personales que lleven a cabo las unidades administrativas del Banco de México deberá sujetarse a las facultades y atribuciones que a dicho Banco Central confieren la Ley del Banco de México, el Reglamento Interior del Banco de México y las demás disposiciones legales y reglamentarias que regulen su competencia.

3. Los datos personales se gestionarán y tratarán de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad. En su obtención, los servidores públicos del Banco de México deberán actuar con apego a los principios de legalidad, honradez y lealtad.

4. El tratamiento de datos personales deberá sujetarse al consentimiento del titular, salvo las excepciones previstas en la ley.

5. Deberá informarse a los titulares la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a través del correspondiente aviso de privacidad.

6. Los titulares de las unidades administrativas del Banco de México que recaben datos personales adoptarán las medidas necesarias para procurar que estos sean exactos, completos, correctos y actualizados, a fin de que no se altere su veracidad. Se presumirá que los datos tienen dichas características, cuando se recaben directamente de los titulares.

7. Únicamente deberán tratarse los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

8. Cuando los datos personales que se recaben hayan dejado de ser necesarios para las finalidades que motivaron su tratamiento, deberán ser suprimidos, previo bloqueo en su caso, conforme a los procedimientos previstos en la LGPDPPSO, los Lineamientos Generales y demás disposiciones aplicables. En todo caso, para determinar los plazos de conservación correspondientes, deberán atenderse las disposiciones aplicables y considerarse los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.

9. El tratamiento de los datos personales deberá limitarse al cumplimiento de las finalidades previstas en el correspondiente aviso de privacidad. Solo podrán tratarse datos personales para finalidades distintas, cuando dicho tratamiento sea conforme a las atribuciones legales del Banco de México, y medie consentimiento del titular, conforme a la ley.

10. Los servidores públicos del Banco de México deberán implementar, cumplir y mantener las medidas de seguridad que determinen las instancias competentes del propio Banco para la protección de los datos personales. Dichas medidas deberán ser establecidas, actualizadas, monitoreadas y revisadas, con base en la metodología que determinen las áreas competentes del Banco y los análisis de riesgos respectivos.

11. Los servidores públicos del Banco de México deberán guardar la confidencialidad de los datos personales a los que tengan acceso. Lo anterior, sin perjuicio del cumplimiento de las disposiciones en materia de transparencia y acceso a la información pública.[22]

12. En aquellos casos en que sea necesario clasificar los datos personales, como puede ser para la atención de solicitudes de acceso a la información o para la publicación de la información a través de la Plataforma Nacional de Transparencia, los titulares de las unidades administrativas deberán clasificar como confidenciales aquellos datos personales que así lo requieran, según lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como las disposiciones derivadas de tales ordenamientos.

13. Los derechos de los titulares en relación con sus datos personales deberán ser respetados por los servidores públicos del Banco de México. El procedimiento para la atención de los derechos de acceso, rectificación, cancelación y oposición (ARCO), deberá llevarse de conformidad con lo dispuesto en la LGPDPPSO y los Lineamientos Generales.

14. La Unidad de Transparencia establecerá procedimientos para recibir y responder dudas y quejas de los titulares de datos personales que sean de fácil acceso y con la mayor cobertura posible.

15. El incumplimiento de los principios y deberes establecidos en la LGPDPPSO serán sancionados de conformidad con lo establecido en dicho ordenamiento. Lo anterior, sin perjuicio de las sanciones del orden civil, penal o de cualquier otro tipo que pudieran derivarse de los mismos hechos.

16. La gestión y el tratamiento de datos personales en el Banco de México estará alineada al marco institucional de gestión y seguridad de la información.

Respecto al manejo seguro de la información y datos personales, se prevé el manejo de la información durante las siguientes fases:

- Elaboración,
- Etiquetado,

[22] El cumplimiento de esta obligación se respalda además por el Compromiso de Confidencialidad suscrito por los servidores públicos del Banco de México.

- Resguardo,
- Acceso,
- Compartición,
- Reproducción,
- Disposición.

Roles y Responsabilidades

Banco de México ha constituido un equipo multidisciplinario que instrumentará el programa de fortalecimiento de la seguridad de la información y datos personales. El equipo está compuesto por integrantes de diferentes áreas del Banco, y tendrá como tarea el levantamiento y mantenimiento de información de los activos y datos personales, el análisis de riesgos y la definición de medidas de seguridad o controles que se deriven de las acciones de mitigación. Una meta fundamental del equipo es propiciar que los aspectos de seguridad de la información y protección de datos personales sean considerados y, en la medida de lo posible, atendidos cuando se realicen planes para actualizar cualquier proceso o sistema.

Estos son los diferentes roles que contribuyen a metas del equipo:

Rol	Responsabilidad
Responsable del proceso	Identificar los tipos de información que recibe, procesa, almacena y/o produce en el proceso y en los sistemas de información relacionados con el mismo. Categorizar la seguridad de la información e identificar los datos personales tratados en el proceso.
Responsable de los servicios de TI	Proveer información técnica sobre los sistemas de información que soportan los procesos. Categorizar la seguridad de los sistemas de información en función de la información que usan, procesan o transmiten dicho servicio. Mantener actualizado el plan de seguridad del sistema de información.
Especialista de seguridad de la información	Evaluar las metodologías para la categorización de seguridad de la información y sistema de información. Definir las medidas de seguridad que mitiguen los riesgos de seguridad de la información y a los datos personales.
Especialista de seguridad en Tecnologías de Información	Proporcionar las guías de implementación de las medidas de seguridad en los componentes de TI que soportan el sistema de información.
Unidad de Transparencia	Documentar el inventario de datos personales y sus respectivos sistemas de tratamiento. Promover las prácticas de protección de datos personales en el Banco.
Especialistas en control en procesos y en TI	Dar seguimiento al monitoreo del control y estimar su estado, así como a la atención de las acciones de mitigación de los riesgos.
Especialista en gestión de la información	Mantener el inventario de activos de información y datos personales, procurando la oportuna actualización ante la modificación de los procesos y sistemas de tratamiento. Capacitar al personal del Banco en aspectos de gestión y seguridad de la información, así como en la normatividad interna aplicable.

Inventario de activos de información

Como parte del programa, los activos de información del Banco de México son identificados, categorizados y registrados en un inventario. Los procesos están soportados por dichos activos y constituyen sus elementos fundamentales para operar.

Un proceso no puede cumplir su propósito a menos que cuente con:

- **Personas para operar y monitorear el proceso.** Las necesarias para la operación y el rendimiento esperado del proceso. Ejecutan el proceso y lo supervisan para asegurarse de que está cumpliendo su propósito, y hacen correcciones al mismo cuando es necesario. Pueden ser trabajadores del Banco o personal externo, y pueden realizar algún tipo de tratamiento de datos personales.
- **Información y datos para alimentar el proceso y ser producidos por el mismo.** Cualquier información o datos, en cualquier medio, incluso en papel o en formato electrónico, necesarios para el funcionamiento previsto del proceso. Debido a la sensibilidad de la información y las obligaciones en materia de protección de datos personales, la seguridad de la información debe categorizarse en función del riesgo. La categorización de seguridad de la información proporciona otro nivel de descripción para un activo de información, y es de ayuda para definir las estrategias para protegerlo.
- **Tecnología para automatizar y apoyar el proceso.** Cualquier componente o activo de tecnología que admite o automatiza un proceso y facilita su capacidad para cumplir su propósito. Los datos personales son tratados por personas a través de la tecnología que soporta el proceso.
- **Instalaciones donde se realiza el proceso.** Son los lugares donde se ejecutan los procesos y suelen compartirse de forma que se ejecuta más de un proceso y depende de ellos.

Cada tipo de activo para un proceso específico es identificado y documentado. En el Banco, este proceso de identificación y priorización ayuda a la documentación del inventario de datos personales y los sistemas de tratamiento, los cuales contienen los siguientes elementos:

Elemento	Propósito
El catálogo de los medios físicos y electrónicos que forman parte del tratamiento de los datos personales.	Provee contexto y describe los medios a través de los cuales son tratados los datos personales.
Las finalidades de cada tratamiento de datos personales (en su caso, conforme al aviso de privacidad).	Establece el propósito para el que los datos son tratados
El responsable del sistema de tratamiento y los	Es un punto de contacto para cualquier información adicional que se requiera del sistema

servidores públicos que tienen acceso a éstos.	
Ubicación del sistema	Ubicación geográfica del sistema mediante el cual se tratan y a dónde y a quién se transmiten
El volumen de información en este sistema	Identificar cuántos datos residen en el sistema de tratamiento
El formato de almacenamiento de la información	Describe el formato de la información: • Físico • Digital Describe la estructura de la información: • Estructurado (Bases de datos, formularios, etc.) • No- estructurado (Archivos de texto, documentos sin formato, etc.)
El tratamiento de esta información	Describe el tipo de tratamiento que se realiza sobre la información en el sistema (acceso, manejo, aprovechamiento, monitoreo y procesamiento)
Roles con tratamiento de información	Describe los roles en el sistema de tratamiento y el tipo de tratamiento que realizan
Tipo de datos personales	Descripción del tipo de datos personales que son tratados
Sensibilidad de los datos	Describe si los datos son sensibles o no (y en su caso, si son especiales de acuerdo con la definición utilizada al interior del Banco)
Ubicación de los datos personales	Descripción general de los lugares donde se almacenan los datos.
Lugar de acceso	Desde qué ubicaciones se tiene acceso a esta información
Remisiones y Transferencias	Describe el flujo de información entre entidades
Encargados	Identificación de los encargados y el instrumento jurídico que formaliza la prestación de sus servicios.
Conclusión del tratamiento	Bloqueo, cancelación, supresión o destrucción de los datos personales.

La priorización de los activos de información del Banco es el instrumento que ayuda a garantizar que se dirijan correctamente los recursos de protección a los activos de información que impactan y contribuyen más directamente a los procesos que respaldan la misión del Banco.

Procesos para la protección de información y datos personales

A lo largo de la instrumentación del programa, se interrelacionan diferentes procesos al interior del Banco que persiguen, desde diferentes perspectivas, proteger sus activos de información. Estos procesos son los siguientes:

Proceso	Función
Administración de activos de información	Identificar, documentar y gestionar activos de información del Banco durante su ciclo de vida
Administración de riesgos	Identificar, analizar, prevenir y controlar los riesgos a que están sometidos los activos de información del Banco que podrían representar un impacto operacional, financiero o reputacional para el mismo (y, en su caso, para el titular de los datos personales).
Administración de controles	Establecer, monitorear y administrar el control que en su caso se requiera para dar seguridad razonable de la efectividad de las operaciones del Banco y de la seguridad de los activos de información que los soportan.
Administración de la continuidad operativa	Garantizar la continuidad de las operaciones esenciales de los procesos y sus activos de información asociados si ocurre una interrupción como resultado de un incidente, desastre, u otro evento disruptivo.
Administración de vulnerabilidades	Identificar, analizar y administrar vulnerabilidades en el entorno operativo del Banco.
Administración de incidentes	Establecer procesos para identificar y analizar eventos, detectar incidentes y determinar una respuesta organizacional apropiada.
Administración de medidas de seguridad	Identificar, documentar y analizar las medidas de seguridad de la información y de protección de datos personales en los procesos y activos de información relacionados, así como identificar inconsistencias entre estos requisitos y las actividades que el Banco realiza para cumplir con dichos requerimientos.
Administración de Seguridad de la información	Establecer y administrar un nivel apropiado de controles para respaldar la sensibilidad, integridad y disponibilidad de la información del Banco, datos personales y propiedad intelectual.
Administración de tecnología	Establecer y administrar un nivel apropiado de controles relacionados con la integridad y la disponibilidad de los activos de TI para respaldar los procesos del Banco.
Seguridad física	Establecer y administrar un nivel apropiado de controles físicos, ambientales y geográficos para respaldar la operación continua de los procesos en las instalaciones del Banco.
Concientización y formación	Promover la conciencia en el personal y desarrollar habilidades y conocimiento en apoyo de sus roles para alcanzar y sostener la seguridad de la información y de los datos personales.

Análisis de impacto a la información y a los datos personales

Banco de México cuenta con una Metodología de Análisis de Impacto a la Información, la cual tiene como objetivo categorizar la seguridad de la información.

La Metodología toma como insumo la información del Banco previamente identificada y catalogada con base en su contenido. En el caso de datos personales, se consideran los siguientes:

- Datos personales en nivel estándar[23]
- Datos personales en nivel estándar en volumen[24]
- Datos personales en nivel especial[25]
- Datos personales en nivel especial en volumen[26]

Una vez identificada la información, se evalúan los impactos que la información tiene, con base en las dimensiones siguientes: Operativo, Monetario, Reputacional y al Titular (cuando se trata de la evaluación de impacto a datos personales). Los impactos mencionados se evalúan bajo la perspectiva de cada uno de los siguientes atributos de seguridad: Sensibilidad, Integridad y Disponibilidad. Para el caso de los datos personales, los atributos de seguridad mencionados guardan la siguiente correspondencia con el art. 38 de la LGPDPPSO:

- Sensibilidad: Fr. II El robo, extravío o copia no autorizada y Fr. III, Uso, acceso o tratamiento no autorizado.
- Integridad: Fr. IV El daño, la alteración o modificación no autorizada.
- Disponibilidad: Fr. I Pérdida o destrucción no autorizada.

Análisis de riesgos y brechas

Se cuenta con una Metodología de Evaluación de Riesgos no Financieros, la cual tiene como finalidad identificar los riesgos no financieros a los que se está expuesto en el desarrollo de las actividades y analizar los distintos factores (humanos, organizacionales, de equipamiento y de tecnologías de información, o en su caso de origen externo) que pueden provocarlos, con la finalidad de definir las estrategias que permitan administrarlos y, por lo tanto, tener una seguridad razonable sobre el logro de los objetivos institucionales. Lo anterior incluye lo relativo a seguridad de la información y la información generada que derive de este análisis se utilizará para la actualización y mejora de las referidas medidas de seguridad.

---

[23] Se refieren a información concerniente a una persona identificada o identificable, que por haber sido desasociada, por existir en fuentes de acceso público, o por cualquier otra razón, se considera que el riesgo de que se causara un daño directo a los titulares en caso de que fuera conocida por terceros es nulo o muy bajo.

[24] Los criterios para considerar el tipo de información como "en volumen" pueden ser dos:
1) Bases que contengan datos personales de más de 3,000 titulares (500 para los datos en nivel especial) y/o
2) Bases que contengan datos personales que combinados o asociados entre sí puedan causar daño directo a los titulares (por ejemplo, Nombre, en combinación con cualquier otro dato relacionado, como teléfono, RFC, etc.), con independencia del número de titulares.

[25] Los datos personales en nivel especial se dividen en "Sensibles de acuerdo a la LGPDPPSO" y "No Sensibles de acuerdo con la definición de la LGPDPPSO".

[26] Son aquellos datos personales que cumplen con las características tanto de "nivel especial" como "en volumen".

La Metodología está conformada de las etapas siguientes:

1. Identificación del riesgo: Identificar aquellos eventos que de materializarse pueden afectar al personal o bienes del Banco, la entrega o provisión de los productos o servicios intermedios o finales que genera el proceso, el funcionamiento adecuado de los servicios de TI, y la protección de la información y datos personales en su posesión.

2. Evaluación del riesgo: Estimar la probabilidad o frecuencia con la que pueden materializarse los riesgos y el impacto que tendrían.

3. Respuesta al riesgo: Determinar la estrategia de respuesta a cada riesgo identificado, la cual puede ser cualquiera de las siguientes: Reducir, Transferir, Evitar o Aceptar. Se incluyen también las acciones específicas de mitigación del riesgo y el plan de trabajo para implementarlas.

4. Seguimiento al riesgo: Dar seguimiento a las acciones de mitigación establecidas en la etapa de Respuesta, así como medir la eficiencia del plan implementado.

5. Comunicación y supervisión de los riesgos: Dar a conocer a todos los involucrados el informe sobre la exposición a riesgos no financieros del Banco.

Como parte de la evaluación de riesgos no financieros, se identifica el riesgo inherente asociado al proceso y a sus activos de información, para posteriormente analizar los controles establecidos que gestionan dichos riesgos y determinan el riesgo residual. Posteriormente se determina la estrategia de respuesta al riesgo y, se identifican las posibles acciones a implementar seleccionando aquellas que mitiguen el riesgo de manera más eficiente. Una vez seleccionadas las acciones de mitigación, las Unidades Administrativas encargadas de los procesos elaboran el plan de implementación, el cual contiene las acciones específicas, fechas compromiso y responsables de su ejecución. La Dirección de Control Interno lleva a cabo el seguimiento a la atención de las acciones de mitigación en intervalos definidos y comunica los resultados correspondientes a la Dirección de Administración de Riesgos.

Para llevar a cabo la evaluación de riesgos de seguridad de la información (incluidos los datos personales) se desarrolló un esquema de revisión de riesgos potenciales con base en la serie ISO 27000[27], el cual incluye un estándar de referencia para los Sistemas de Gestión de Seguridad de la Información. El esquema de revisión se divide en dominios o aspectos relacionados con la seguridad de la información y pretende determinar aquellos aspectos en los que existe un riesgo potencial que vulnere los atributos de seguridad: Sensibilidad, Integridad y Disponibilidad.

Mediante un ejercicio de autoevaluación de controles, se determinará la capacidad de protección de los datos personales actual, que soporte las medidas de seguridad identificadas como parte de las acciones de mitigación de riesgos. Durante esta fase, el Responsable Tecnológico de Información revisa las capacidades actuales de los sistemas de información, los sistemas operativos, el hardware,

[27] https://www.iso.org/isoiec-27001-information-security.html

las herramientas de administración, la infraestructura física entre otros factores, para determinar el grado de progreso en el cumplimiento de las medidas de seguridad para mitigar el riesgo.

Si bien el referido sistema implicará el análisis de los riesgos para toda la información del Banco de México, para el caso particular de los datos personales tomará en cuenta lo siguiente:

1. Considerará las amenazas y vulnerabilidades[28] existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.
2. Los requerimientos regulatorios, códigos de conducta y ética o mejores prácticas del sector en que opera el Banco Central.
3. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.
4. El valor y exposición de los activos involucrados en el tratamiento de los datos personales.
5. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.
6. El riesgo inherente a los datos personales tratados.
7. La sensibilidad de los datos personales tratados.
8. El desarrollo tecnológico.
9. Las transferencias de datos personales que se realicen
10. El número de titulares
11. Las vulneraciones previas ocurridas en los sistemas de tratamiento
12. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

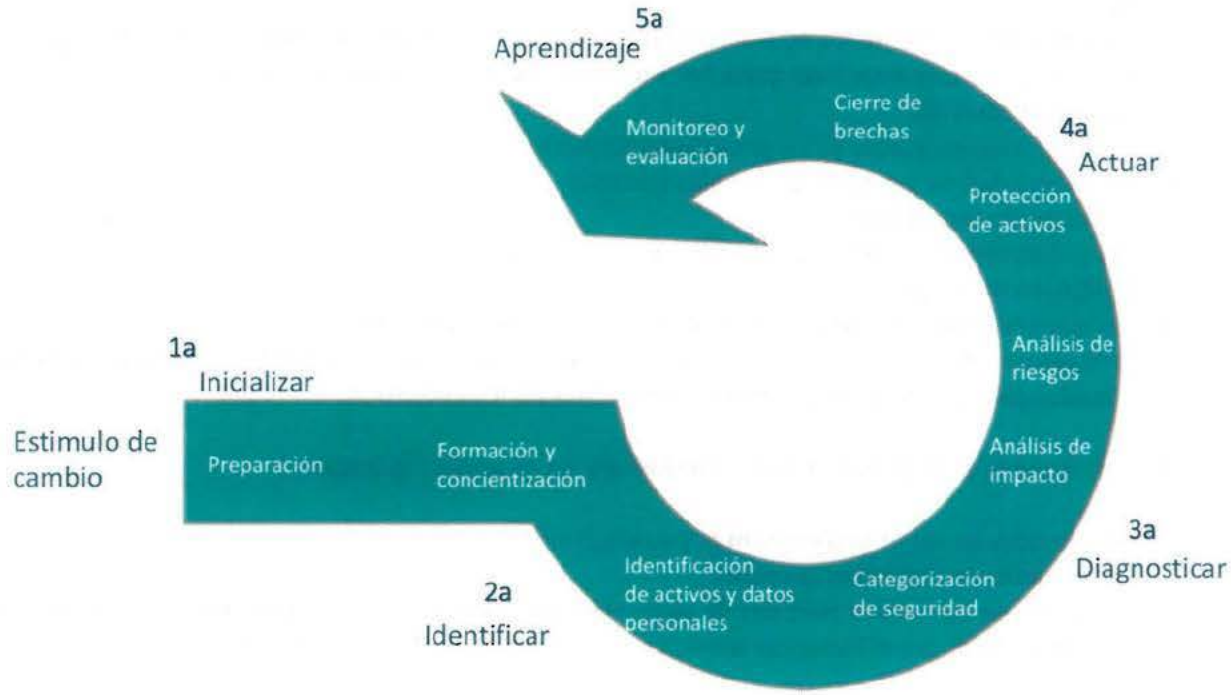
De igual manera, el análisis de brecha considerará los aspectos siguientes:

1. Las medidas de seguridad existentes y su efectividad.
2. Las medidas de seguridad faltantes.
3. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados por el Banco de México al momento de la realización del análisis.

[28] De conformidad con el punto SEXTO del *ACUERDO por el que se determinan los criterios para establecer y mantener el Sistema de Gestión de Seguridad de Datos Personales, la política interna de gestión y tratamiento s de datos personales, y otras políticas y programas de protección de datos personales*, emitido por el Comité de Transparencia el 24 de mayo de 2018, en caso de que se presente una vulneración a la seguridad de los datos personales, el titular de la unidad administrativa involucrada deberá dar aviso inmediato a la Dirección de Administración de Riesgos para que ésta lleve a cabo el correspondiente registro en la bitácora de vulneraciones. Asimismo, deberá dar aviso a la Unidad de Transparencia y remitir un informe al Comité de Transparencia. En el referido Acuerdo se especifica el contenido mínimo de este informe, así como la forma en que se adoptarán las determinaciones internas correspondientes, y se coordinará la instrumentación de las acciones previstas en las disposiciones aplicables. De igual forma, se considerarán las Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales emitidas por el INAI.

Implementación y operación

El programa de fortalecimiento de la seguridad de la información y datos personales ha adoptado el ciclo de Deming[29] como método de adopción de los procesos de seguridad de los activos de información a lo largo del Banco. Esto ayuda a contar con un modelo de mejora que sirve como hoja de ruta para las acciones de inicialización, planeación e implementación.



Modelo de mejora continua del programa

Las razones del Banco para fortalecer la seguridad de la información y los datos personales son articulados de manera precisa durante la fase inicial. Este esfuerzo ayuda a tener una alineación con los objetivos institucionales y los ejes rectores de Banco de México. Se pretende asegurar el de los titulares de las unidades administrativas, que constituye un instrumento de habilitación de los recursos necesarios por el programa.

La fase de identificación (2a) permite tener un entendimiento integral del esfuerzo requerido. Durante esta fase, el personal involucrado en la instrumentación del programa es capacitado en los procesos y procedimientos a emplear durante su participación, los activos de información son

[29] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=20208

identificados, los datos personales y los sistemas de tratamiento son inventariados y priorizados de acuerdo con su nivel de sensibilidad, integridad y disponibilidad.

La fase de diagnóstico (3a) nos permite identificar y analizar los escenarios de riesgo que pueden tener un impacto operativo, financiero o reputacional en el Banco y, en su caso, en el titular de los datos personales; identificando las vulnerabilidades en el entorno del Banco y las brechas de controles. De igual forma, se habilita la toma de decisiones en función del riesgo identificado.

El propósito de la fase de actuación (4a) consiste en cerrar las brechas identificadas, mediante la implementación de medidas de seguridad administrativas, técnicas o físicas para lograr un nivel de riesgo aceptable para el Banco.

La fase de aprendizaje (5a) permite identificar desviaciones del estado deseado, documentar lecciones aprendidas y actuar ante las nuevas posibles brechas que surjan en el ambiente operativo, enriqueciendo el proceso en cada ciclo de ejecución. Además, durante esta fase se determina lo que se ha logrado, y si el esfuerzo alcanzó las metas planteadas.

El objetivo de este modelo es mejorar continuamente la habilidad del Banco de adoptar al cambio los esfuerzos de fortalecimiento de la seguridad de la información y datos personales.

Monitoreo y revisión

La gestión de riesgos no financieros en el Banco está basada en el modelo de tres líneas de defensa[30], el cual tiene por objetivo delimitar los roles y responsabilidades de las diferentes áreas involucradas.

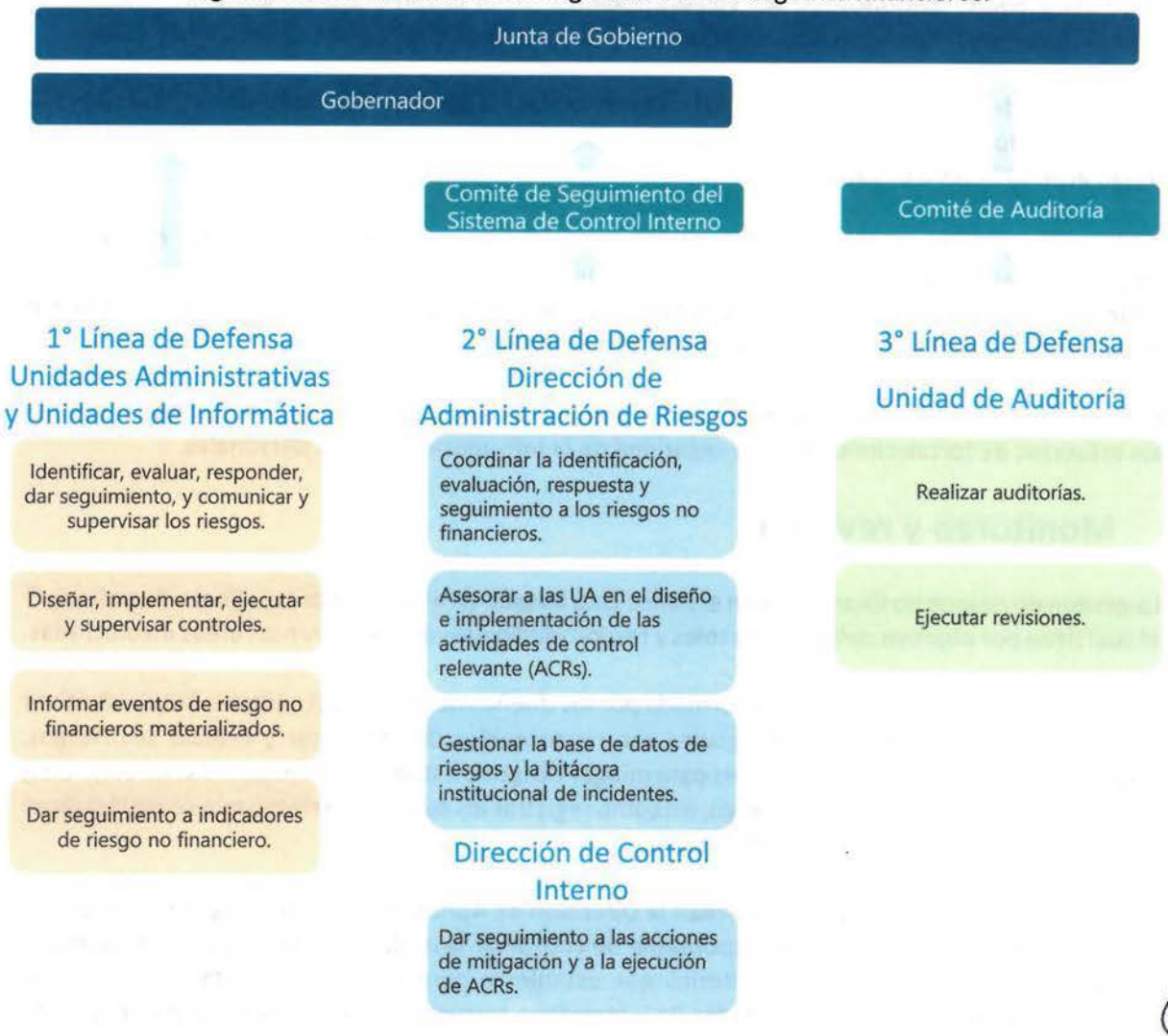
La primera línea de defensa está conformada por los dueños del proceso (Unidades Administrativas y las Unidades de Informática), las cuales son responsables de identificar y evaluar sus riesgos, implementar controles y otras acciones para mitigar riesgos o establecer mejoras a dichos controles, dar seguimiento a indicadores de riesgo, así como registrar los eventos de riesgo que se materialicen en la ejecución de sus procesos y actividades.

La segunda línea de defensa la conforman la Dirección de Administración de Riesgos y la Dirección de Control Interno. La primera es responsable de coordinar la evaluación de riesgos no financieros conforme a la metodología y los criterios que establezca para tal efecto; brindar asesoría a las Unidades Administrativas y las Unidades de Informática respecto a la implementación o mejora de controles y otras acciones para mitigar riesgos; gestionar la base de datos de riesgos y la bitácora institucional de incidentes; así como informar los resultados de las evaluaciones a los diferentes involucrados. La Dirección de Control Interno es responsable de dar seguimiento a la implementación de la acciones para mitigar riesgos, así como a que las Actividades de Control Relevante (ACRs) sean ejecutadas y supervisadas por las Unidades Administrativas, con la periodicidad establecida, dejando evidencia de su ejecución, minimizando así la materialización del riesgo por el incumplimiento de los controles.

[30] COSO (2015). *Leveraging across the three lines of defense* - http://aechile.cl/wp-content/uploads/2015/07/COSO-2015-3LOD-PDF-1.pdf

La tercera línea de defensa la conforma la Unidad de Auditoría y proporciona un aseguramiento razonable de que los riesgos estén correctamente identificados y evaluados por la primera y segunda líneas de defensa.

Figura 1. Líneas de defensa en la gestión de los riesgos no financieros.



Adicionalmente, Banco de México analiza información de inteligencia sobre amenazas para obtener indicadores de compromiso y firmas de detección. Una vez que analizan esta información, los especialistas del Banco pueden usarla para fortalecer las defensas de las TICs y mejorar las formas de anticipar, prevenir, detectar y responder a los posibles ataques cibernéticos.

De manera particular, para el caso de datos personales, se llevarán a cabo, a través de las medidas señaladas en el presente documento, un constante monitoreo y revisión de las medidas de seguridad implementadas, así como de las amenazas y vulneraciones a las que están sujetos los datos personales.

Mejora continua

En gran medida, la mejora continua versa sobre la gestión del cambio, ya sea que éste sea intencional o no intencional; inclusive considerando cambios causados por un evento disruptivo. Por su parte, la medición del desempeño es una parte fundamental de la mejora continua, y se describe como el proceso de formulación, selección y seguimiento de métricas para evaluar la implementación, eficiencia y/o eficacia; obtención de datos y producir información cuantitativa que describe el desempeño del programa de fortalecimiento de seguridad de la información y datos personales. Banco de México emplea este proceso como un método coherente para informar a las partes interesadas sobre cómo el Banco se está desempeñando en la protección de los activos de información y los datos personales, utilizando un sistema de medición que refleja los indicadores relevantes en la implementación del programa y que resulte práctico y fácil de entender.

Las métricas proveen un lenguaje común entre los tomadores de decisiones y quien está involucrado en la operación para discutir la información relevante relacionada con la evaluación del progreso del programa. Las métricas son descritas y utilizadas en un lenguaje claro y fácil de entender. Algunas de las métricas en materia de protección de datos personales que son desarrolladas para permitir la toma de decisiones son las siguientes:

- Avisos de privacidad publicados en la página de internet del Banco
- Encuestas de satisfacción sobre respuestas a solicitudes de derechos ARCO que incluyen:
    - Facilidad en el proceso de registro,
    - Calidad de la respuesta proporcionada,
    - Claridad en el lenguaje utilizado, y
    - Respeto a los derechos ARCO.
- Incidentes o vulneraciones.
- Capacitación del personal del Banco.
- Medición de conocimiento en materia de protección de datos personales con base en los resultados de la evaluación del Sistema de Control Interno 2017.
- Proporción de inconformidades (recursos de revisión) en relación con solicitudes atendidas.

El uso de estas métricas permite el análisis para determinar aspectos tales como:

- Tendencias,
- Eficacia en el proceso,
- Áreas de oportunidad,
- Cumplimiento de las obligaciones en la materia,
- Posición relativa en función de la situación de otros sujetos obligados, y
- Nivel de madurez del programa de protección de datos personales.

En todo caso, la revisión de las políticas y programas de seguridad y sistemas de supervisión y vigilancia implementados se revisarán, por lo menos, cada dos años.

De manera particular, para el caso de los datos personales, como resultado de la aplicación de las acciones descritas en el presente Documento de Seguridad y de la información obtenida de ello, se revisarán las medidas de seguridad implementadas por el Banco de México para que se incorporen aquellas cuestiones que requieran mejora derivadas del análisis de la información siguiente:

1. Riesgo inherente a los datos personales tratados.
2. Sensibilidad de los datos personales tratados.
3. Desarrollo tecnológico y técnicas existentes.
4. Las posibles consecuencias de una vulneración para los titulares.
5. Las transferencias de datos personales que se realicen.
6. El número de titulares de los datos personales tratados por el Banco de México.
7. Vulneraciones que, en su caso, ocurran en los sistemas de tratamiento.
8. Riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

PLAN DE TRABAJO

La instrumentación de este programa es esencial para la selección adecuada de las medidas de seguridad para garantizar la sensibilidad, integridad y disponibilidad de los datos personales y los sistemas de tratamiento. Representa un hito fundamental en la integración de la seguridad de la información en los procesos de Banco de México y establece las bases para la estandarización de seguridad entre los servicios de TI que los soportan.

Banco de México ha definido un plan de trabajo como parte de la instrumentación del programa, enfocado a la implementación del mismo en todos los procesos a su cargo, siguiendo cada una de las fases del modelo de mejora continua. La implementación del plan implica la participación de todas las unidades administrativas del Banco, y particularmente, a efecto de coordinar los esfuerzos a nivel institucional, trabajando en conjunto con:

- Dirección de Administración de Riesgos
- Dirección de Ciberseguridad
- Dirección de Control Interno
- Dirección de Coordinación de la Información
- Dirección de Seguridad
- Dirección de Sistemas
- Unidad de Auditoría
- Unidad de Transparencia
- Gerencia de Seguridad de Tecnologías de la Información

A continuación, se listan los hitos en la implementación del programa a lo largo del tiempo, en donde la comuna "Dirigido por" indica el área responsable de coordinar la acción respectiva:

Acción	Programación	Entregable	Estado	Dirigido por
Preparación				
Evaluar el programa de ciberseguridad	Inicio: 2017	Líneas de acción para el fortalecimiento de la seguridad de la información	Terminado	Dirección de Sistemas Dirección de Ciberseguridad
1 [redacted]				
Formación y concientización				
Implementar el programa de capacitación en materia de datos personales 2017	2017	Formación a funcionarios en materia de protección de datos personales y la LGPDPPSO	Terminado	Unidad de Transparencia
Implementar el programa de capacitación en materia de datos personales 2018	2018	Formación a funcionarios en materia de protección de datos personales y la LGPDPPSO	En proceso	Unidad de Transparencia
Identificación de activos de información y datos personales				
1 [redacted]				

1 [redacted]

Categorización de seguridad

1 [redacted]

Análisis de impacto

1 [redacted]

Análisis de Riesgos

1 [redacted]

Protección de activos de información

1 [redacted]

Cierre de brechas

1 [redacted]

El resultado de este plan permite construir un fuerte vínculo entre los ejes rectores, los objetivos institucionales, los procesos, las actividades, la información, los datos personales y los servicios de TI con una gestión del riesgo no financiero rentable.

Las disposiciones que deriven de este plan, así como las medidas implementadas, serán hechas del conocimiento de los servidores públicos del Banco de México como parte del programa de capacitación a largo plazo.

ANEXO ÚNICO. SISTEMAS EN LOS QUE SE ALMACENAN DATOS PERSONALES

A continuación se enlistan los sistemas y aplicaciones del Banco que se han identificado como repositorios relevantes de datos personales. El siguiente listado se considera preliminar, ya que se prevé que durante la ejecución del plan de trabajo pueda ser ajustado.

El 28 de junio de 2018, en sesión extraordinaria 07/2018, el Comité de Transparencia del Banco de México, por unanimidad de sus integrantes presentes, aprobó la presente versión del Documento de Seguridad del Banco de México, con fundamento en los artículos 83 y 84, fracciones I, IV y V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como 4o. y 31, fracciones II, V, XVI y XX, del Reglamento Interior del Banco de México. Conste.----------
---

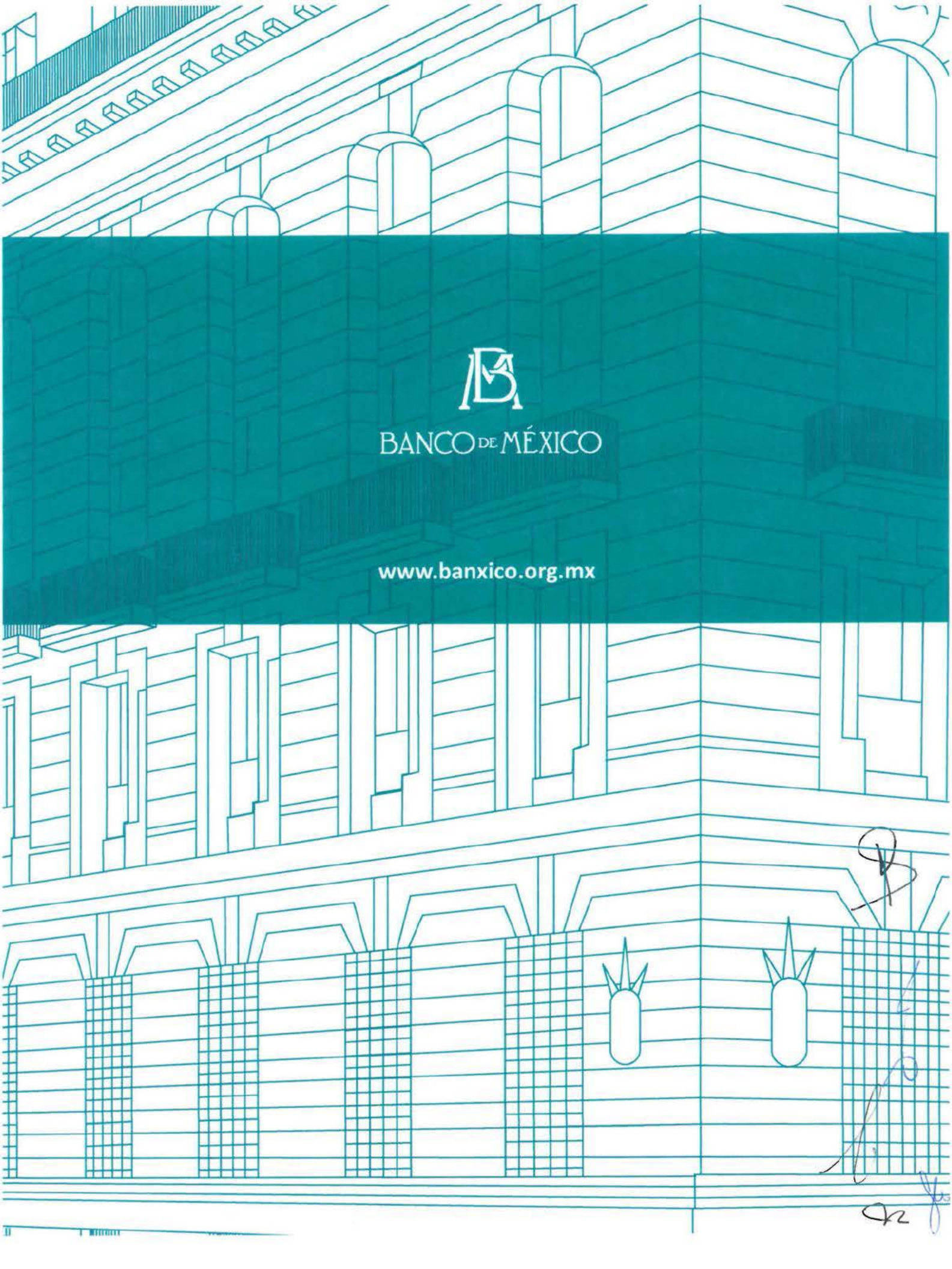
COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

RODOLFO SALVADOR LUNA DE LA TORRE
Secretario



BANCO DE MÉXICO

www.banxico.org.mx

BANCO DE MÉXICO

PRUEBA DE DAÑO

Información sobre los sistemas en los que se almacenan o tratan datos personales en el Banco de México y las acciones que se adoptarán como parte del plan de trabajo para la protección de dichos datos, descritos en el Documento de Seguridad

En términos de lo dispuesto en el artículo 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública 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 obstruya la prevención de los delitos, por lo que la **información sobre los sistemas en los que se almacenan o tratan datos personales en el Banco de México y las acciones que se adoptarán como parte del plan de trabajo para la protección de dichos datos, descritos en el Documento de Seguridad, es clasificada como reservada en virtud de lo siguiente:**

La divulgación de la citada información representa un riesgo de perjuicio significativo al interés público, en lo que respecta a la obstrucción en la prevención de los delitos, toda vez que dicho riesgo es:

1) Real, ya que revelar o divulgar información sobre los sistemas en los que se almacenan o tratan datos personales en el Banco de México y las acciones que se adoptarán como parte del plan de trabajo para la protección de dichos datos, descritos en el Documento de Seguridad, haría vulnerable la prevención de delitos como fraudes o robos de identidad, que podrían perpetrarse por personas o grupos delincuenciales.

2) Demostrable, ya que en los últimos años, el creciente avance de la tecnología ha propiciado cambios fundamentales en los procesos y modelos de negocio al interior de las organizaciones financieras. Estos avances, sin duda, han contribuido a introducir eficiencias operativas y ahorros de costos. Banco de México no es la excepción, al igual que otros bancos centrales, está cada vez mejor interconectado, y utiliza sistemas de tecnologías de información más complejos. Sin embargo, el uso de dichas tecnologías también conlleva mayores riesgos. Las vulneraciones de seguridad generan altos costos institucionales además de afectaciones en la esfera de otros derechos y libertades fundamentales de las personas.

En un entorno digital cada vez más interconectado, las brechas de seguridad en las Tecnologías de la Información y la Comunicación (TIC) pueden producir consecuencias no deseadas en la operación y, por ende, en la reputación del Banco de México y el sistema financiero del país. Las amenazas que pueden ocasionar la interrupción de la operación de las instituciones son cada día más evidentes y sofisticadas, independientemente de las acciones preventivas en materia de seguridad de la información y de las TIC, tanto la evidencia histórica como las recientes intrusiones cibernéticas a nivel internacional sugieren que prácticamente todas las industrias, y particularmente los servicios financieros, son susceptibles a posibles

eventos de pérdida o sustracción de información.

Con la finalidad de minimizar y evitar los riesgos de pérdida de datos personales, el Banco de México ha instrumentado de forma proactiva un programa de fortalecimiento de la seguridad de la información, el cual comprende un plan de trabajo con acciones concretas, que deben mantenerse reservadas, con la finalidad de que no pueda afectarse su efectividad y con ello, garantizar la continuidad de la operación de la institución.

Por otra parte, 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.

Adicionalmente, debe destacarse que de vulnerarse alguno de los sistemas en los que se almacenan datos personales, se afectaría la reputación del Banco Central del Estado mexicano.

3) Identificable, ya que difundir información de datos personales contenidos en los archivos electrónicos, sistemas o aplicaciones del Banco de México descritos en el Documento de Seguridad del Instituto Central 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 de archivo del Banco de México.

Cabe destacar que al hacer públicos los sistemas en los que se almacena o tratan datos personales, o bien información sobre las acciones que se implementarán para fortalecer la seguridad de dichos datos, ocasionaría un serio perjuicio a las actividades de prevención de los delitos que llevan a cabo las autoridades competentes, toda vez que facilitarían la vulneración de la integridad y confidencialidad de la información que éstos contienen.

El riesgo de perjuicio que supondría la divulgación, supera el interés público general de que se difunda, ya que no existe un beneficio social con la divulgación de los sistemas de almacenamiento y tratamiento de datos personales identificados en el Documento de Seguridad, o bien sobre las acciones que se tomarán como parte del plan de trabajo establecido. Por el contrario, difundir la citada

información podría poner en riesgo de vulneración los referidos sistemas y datos personales contenidos en los mismos.

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, en virtud de que al disminuir el riesgo de cualquier vulneración a los datos personales en posesión de este Banco Central, se contribuye a la prevención de los delitos.

El hecho de reservar esta información resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, ya que proporcionarla incrementaría el riesgo de obtener y utilizar de manera ilegal y sin autorización de su titular, datos personales para llevar a cabo conductas ilícitas como fraudes.

En razón de lo anterior, y vistas las consideraciones expuestas en el presente documento, la Unidad de Transparencia del Banco de México solicita la reserva de dicha información por un plazo de cinco años a partir de la fecha de la misma, ya que es indispensable proteger y evitar la divulgación de la información contenida en los archivos electrónicos, sistemas o aplicaciones del Banco de México descritos en el Documento de Seguridad del Instituto Central, con la intención de evitar conductas ilícitas.

Por lo 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, 106, fracción III, 108, último párrafo, 109, 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública; 98, fracción III, 100, 102, 106, 110, fracción VII, y 111, Ley Federal de Transparencia y Acceso a la Información Pública; 2o., y 4o. de la Ley del Banco de México; 4, párrafo primero, 8, párrafos primero y tercero, 10, párrafo primero, 31 Bis, fracciones, XXIV, XXVI y XXIX, del Reglamento Interior del Banco de México; Primero, párrafo primero, y Segundo, fracción XIII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Cuarto, Séptimo, fracción III, Octavo, párrafos primero, segundo y tercero, 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", la información contenida en los archivos electrónicos, sistemas o aplicaciones del Banco de México descritos en el Documento de Seguridad del Instituto Central, es reservada, toda vez que su divulgación dificultaría las labores, programas, políticas y lineamientos que la autoridad competente pueda tener en materia de prevención de los delitos.