BANCO DE MÉXICO®

Documento de Seguridad

Protección de Datos Personales

Septiembre 2025

UNIDADES ADMINISTRATIVAS QUE ELABORARON ESTE DOCUMENTO

Dirección General de Contraloría y Administración de Riesgos

Dirección General de Tecnologías de la Información

Dirección de Seguridad

Unidad de Auditoría

Unidad de Transparencia

Contenido

PRESENTACIÓN

La protección de la vida privada y los datos personales es un derecho humano, reconocido en los artículos 6o., párrafo cuarto, Apartado A, fracciones II, III, y VIII, y 16, párrafo segundo, 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 20 de marzo de 2025, fue publicado en el Diario Oficial de la Federación, el Decreto por el que se expiden, entre otras, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), la cual entró en vigor al día siguiente de su publicación.

De conformidad con el artículo 10 de la LGPDPPSO, los sujetos obligados deben observar en el tratamiento de los datos personales, entre otros, el principio de responsabilidad, de conformidad con los artículos 23 y 24 de la LGPDPPSO. 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.

Al efecto, conforme a lo dispuesto en el artículo 27 de la LGPDPPSO, los sujetos obligados debemos realizar, en términos generales, las acciones interrelacionadas para establecer y mantener las medidas de seguridad referidas, tales como las siguientes: crear políticas internas para la gestión y tratamiento de los datos personales que tomen en cuenta el contexto en el que ocurren los tratamientos, así como su ciclo de vida; definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales; elaborar un inventario de datos personales y de los sistemas de tratamiento; realizar un análisis de riesgo que considere las amenazas y vulnerabilidades a que se encuentran expuestos los elementos previamente inventariados; elaborar un análisis de brecha que permita identificar medidas de seguridad faltantes con base en los resultados obtenidos; elaborar un plan de trabajo para la incorporación de las medidas identificadas como faltantes; implementar acciones de monitoreo y revisión de las medidas para evaluar su funcionamiento y finalmente, diseñar y aplicar diferentes niveles de capacitación al personal relacionado con los tratamientos de datos personales, de acuerdo a sus roles y responsabilidades.

Las mencionadas acciones integran el denominado Sistema de Gestión de Seguridad de Datos Personales (Sistema de Gestión), el cual es entendido como el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, acorde a lo establecido en el artículo 28 de la LGPDPPSO.

En el contexto del referido Sistema de Gestión, el artículo 29 de la LGPDPPSO establece el deber de los responsables de elaborar el denominado **Documento de Seguridad**, mismo que deberá contener, al menos, lo siguiente:

- El inventario de datos personales y de los sistemas de tratamiento;
- Las funciones y obligaciones de las personas que traten datos personales;
- El análisis de riesgos;
- El análisis de brecha;
- El plan de trabajo;
- Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
- El programa general de capacitación.

Cabe mencionar que el Documento de Seguridad coadyuva al cumplimiento de las obligaciones, a cargo del Banco México, previstas en la LGPDPPSO, para la protección de datos personales, frente a las personas titulares de la información, así como frente a la Autoridad Garante, encargada de vigilar el cumplimiento de las disposiciones aplicables en la materia; además de contribuir a la madurez del Sistema de Gestión.

Al respecto, el Documento de Seguridad debe ser actualizado cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo; como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del Sistema de Gestión; como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y para la implementación de acciones correctivas y preventivas ante una vulneración de seguridad, conforme a lo previsto en el artículo 30 de la LGPDPPSO.

Bajo el marco normativo descrito, el Banco de México, a través de la Unidad de Transparencia, de la Dirección General de Contraloría y Administración de Riesgos, de la Dirección General de Tecnologías de la Información, de la Dirección de Seguridad y de la Unidad de Auditoría, con la colaboración de todas las Unidades Administrativas que participan de manera cotidiana en el tratamiento de datos personales y por ende, poseen información que alimenta las directrices y políticas que rigen el Sistema de Gestión, elaboró el presente Documento de Seguridad, el cual fue presentado a la consideración del Comité de Transparencia de dicho Instituto Central. Asimismo, de conformidad con lo previsto en los artículos 77, segundo párrafo, y 78, fracción V, de la LGPDPPSO, el Comité es la autoridad máxima en materia de protección de datos personales y responsable de supervisar, en coordinación con las Unidades Administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el citado documento.

Al respecto, las Unidades Administrativas del Banco de México son las principales encargadas de ejecutar las acciones que se describen en el Documento de Seguridad; no obstante, existen ciertas Unidades que participan directamente en su elaboración, las cuales, son las encargadas de coordinar los esfuerzos e información a nivel institucional, conforme a las atribuciones señaladas en el Reglamento Interior del Banco de México (RIBM), en los términos siguientes:

Unidad Administrativa	Especialidad
Dirección de Administración de Riesgos.	Identificar, evaluar y actualizar los riesgos de seguridad de la información, incluyendo datos personales.
Dirección de Ciberseguridad.	Evaluar y dar seguimiento a las actividades realizadas por las Unidades Administrativas del Banco en cumplimiento a la normatividad en materia de Ciberseguridad. Definir e instrumentar las acciones necesarias en las materias de ciberseguridad y ciberresiliencia, así como dar seguimiento a la corrección o mitigación de las vulnerabilidades informáticas que se identifiquen. Ambas acciones se encuentran relacionadas con la gestión de medidas de seguridad técnicas.
Dirección de Control Interno.	Proponer criterios, parámetros y métodos para la evaluación y seguimiento de los mecanismos de control que las Unidades Administrativas apliquen en la ejecución de los procesos del Banco, actividad que se encuentra relacionada con el monitoreo y revisión del Sistema de Gestión.
Dirección de Seguridad y Organización de la Información.	Establecer, para la adecuada gestión de la información del Banco, normas, lineamientos, prácticas, procedimientos, metodologías, indicadores, así como proponer herramientas informáticas especializadas para fortalecer la gestión y el análisis de su información y, por lo tanto, de sus datos personales.
Dirección de Seguridad.	Coordinar y ejecutar las actividades relacionadas con la seguridad interna y protección civil del Banco, tareas que se encuentran relacionadas con la gestión de medidas de seguridad físicas.
Unidad de Auditoría.	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.
Unidad de Transparencia.	Asesorar a las Unidades Administrativas del Banco en materia de protección de datos personales, y coordinar con estas las acciones que deban implementarse en el Banco para el cumplimiento de los principios y deberes previstos en la LGPDPPSO.

Introducción

En los últimos años, el creciente avance de la tecnología ha propiciado cambios fundamentales en los procesos y modelos de gestión al interior de todo tipo de organizaciones, 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 más 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 del 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 vulneraciones.

Ante la responsabilidad de gestionar los riesgos de seguridad de la información, Banco de México ha instrumentado de forma proactiva el Programa de Reforzamiento Continuo de Ciberseguridad que entre sus objetivos está mantener y mejorar la ciberseguridad de la Institución en todos sus procesos. El programa mencionado contempla medidas particulares de implementación y homologación de controles, para mantener la seguridad de la información y de los datos personales. Entre dichas medidas, destacan el seguimiento y verificación de acciones para: el levantamiento de un inventario de activos de información y datos personales; el etiquetado de dichos activos conforme a su categoría de información; la evaluación de riesgos de seguridad de la información; la corrección o mitigación de vulnerabilidades; la gestión de incidentes de ciberseguridad; así como la capacitación y concientización que habiliten al personal del Banco a ser vigilantes en el manejo seguro de la información.

Las medidas particulares de implementación y homologación de controles de ciberseguridad definidas contribuyen a mitigar el riesgo y proteger la operación de los procesos y sistemas del Banco, así como sus 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

Contexto institucional

Banco de México en su calidad de Sujeto Obligado

De conformidad con lo dispuesto por el artículo 28, párrafos séptimo y octavo, de la CPEUM, el Banco Central del Estado Mexicano tiene como objetivo prioritario procurar la estabilidad del poder adquisitivo de la moneda nacional y fortalecer con ello la rectoría del desarrollo nacional que corresponde al Estado.

Asimismo, este Instituto Central ejerce de manera exclusiva las funciones del Estado en las áreas estratégicas de acuñación de moneda y emisión de billetes. Por otra parte, es facultad del Banco Central, en los términos que determinen las leyes y con la intervención de las autoridades competentes, regular los cambios, así como la intermediación y los servicios financieros, contando con las atribuciones de autoridad necesarias para llevar a cabo dicha regulación y proveer a su observancia. Por lo tanto, de conformidad con las facultades y atribuciones que la Ley confiere al Banco de México, el nivel de interacción con la sociedad, para efectos del tratamiento de datos personales, se encuentra acotado, en virtud de que no celebra transacciones u operaciones financieras con personas particulares, ni les requiere realizar trámites en sus oficinas; tampoco recibe quejas o reclamaciones por parte de personas usuarias de servicios financieros.

Por otra parte, es importante señalar que las interacciones del Banco con el público en general están acotadas a los temas establecidos en los Avisos de Privacidad de este Instituto Central, disponibles para su consulta en Avisos de privacidad, transparencia, Banco de México, particularmente, aquellos listados en las secciones “Fideicomisos y comités” y “Servicios a la sociedad”. Dada su calidad de Sujeto Obligado en términos de la LGPDPPSO y en riguroso cumplimiento a dicha legislación, los datos personales que trata en el ejercicio de sus facultades y atribuciones se encuentran debidamente protegidos, tal como se describe en el apartado de protección de datos personales de la página de internet del Banco de México.[5] De igual manera, se encuentran protegidos por el conjunto de acciones y medidas que se describen en las páginas que integran el presente Documento de Seguridad.

Sujetos Obligados indirectos

Por otra parte, el Banco de México, en términos de la legislación y contratos constitutivos correspondientes, funge como fiduciario de los siguientes fideicomisos públicos no considerados entidades paraestatales y sin estructura orgánica propia:

- Fondo Mexicano del Petróleo para la Estabilización y el Desarrollo (FMPED).
- Fondo de Pensiones para el Bienestar (FPB).

Asimismo, Banco de México, en términos de la legislación y contratos constitutivos correspondientes, funge como fiduciario del siguiente fideicomiso público considerado entidad paraestatal, sin estructura orgánica propia:

- Fondo para el Desarrollo de Recursos Humanos (FIDERH).

[5] Datos personales, protección, Banco de México (banxico.org.mx)

Dichos entes, de conformidad con el marco legal aplicable, al carecer de una estructura orgánica propia que les permita dar cumplimiento a la normatividad en materia de protección de datos personales, cumplen con sus obligaciones en la materia a través del ente público facultado para coordinar su operación, en este caso, el Banco de México.

Por lo anterior, la totalidad de las obligaciones en materia de protección de datos personales a cargo de los referidos sujetos obligados indirectos son cumplidas a través de este Instituto Central. En ese sentido, la normatividad, políticas, mecanismos, acciones y medidas descritas en este Documento de Seguridad son de aplicación transversal para los fideicomisos enlistados y regulan los tratamientos de datos personales que llevan a cabo.

Normatividad

El marco normativo relacionado con la gestión y seguridad de la información, que incluye la protección de datos personales, está conformado principalmente, por los documentos listados a continuación, en los cuales se describe el conjunto de medidas y acciones que el Banco de México tiene implementado para proteger la información que gestiona en el ejercicio de sus atribuciones.

a) Norma Administrativa Interna "Gestión de la Información".

b) Políticas y Lineamientos de Seguridad de la Información del Banco de México.

c) ACUERDO por el que se determina la Política Interna para la Gestión y Tratamiento de Datos Personales, los Criterios para Establecer y Mantener el Sistema de Gestión de Seguridad de Datos Personales, y otras Políticas de Protección de Datos Personales, (Acuerdo SGSDP).

La Norma Administrativa Interna (NAI) denominada "Gestión de la Información"[6] tiene por objeto establecer y regular las actividades requeridas para la gestión de los activos de información, los datos personales o, en su caso, la información equiparable a dato personal[7] que el Banco genera o recibe en el ejercicio de sus funciones, competencias, obligaciones y actividades. Entre las responsabilidades en materia de gestión de la información, se prevén las siguientes:

[6] Norma Administrativa Interna Gestión de la Información

[7] Información concerniente a personas jurídicas colectivas, de carácter económico, comercial o relativos a su identidad, que de revelarse pudieran anular o menoscabar su libre y buen desarrollo, y que en consecuencia deben permanecer ajenos al conocimiento de terceros.

1. Identificación de los activos de información de los procesos.
2. Identificación de los tipos de datos personales tratados en los procesos, así como las finalidades de tratamiento, formatos de almacenamiento, las personas servidoras públicas que tienen acceso al sistema de tratamiento, personas encargadas y transferencias.
3. Categorización de los activos de información, considerando en particular el caso en que los activos de información contengan datos personales.
4. Evaluación de los riesgos de seguridad de la información.
5. Registro de la categoría de los activos de información y de los servicios de Tecnologías de la Información (TI) que los soportan.
6. Establecimiento de roles y responsabilidades para la gestión de los activos de información y el tratamiento de datos personales, conforme a su categoría.
7. Definición de las medidas de seguridad para la información, los datos personales y los servicios de TI que los tratan.
8. Actualización del inventario de activos de información e inventario de datos personales.

Las Políticas y Lineamientos de Seguridad de la Información del Banco de México,[8] tienen por objeto establecer las políticas en materia de seguridad de la información que deben observarse en el Banco para proteger la confidencialidad, disponibilidad e integridad de la información que se genera, recibe o gestiona, como parte de los procesos de la Institución. Adicionalmente, tiene por objeto establecer lineamientos para guiar y delimitar la gestión de la seguridad de la información en el propio Banco. Entre los principales alcances de las citadas Políticas y Lineamientos, están los siguientes:

1. La gestión de la seguridad de la información.
2. La gestión de los activos de la información.
3. La gestión de vulnerabilidades.
4. La gestión de incidentes de ciberseguridad.
5. La seguridad de las soluciones de tecnologías de la información.

Por otra parte, en la política interna para la gestión y tratamiento de los datos personales, establecida por el Acuerdo SGSDP, se definen las siguientes responsabilidades:

1. En la gestión y el tratamiento de datos personales, las personas servidoras públicas del Banco de México deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, conforme a la LGPDPPSO y demás disposiciones aplicables. Las personas servidoras públicas 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.

[8] Políticas y lineamientos de seguridad de la información del Banco de México.

2. La gestión y el tratamiento de datos personales que lleven a cabo las Unidades Administrativas del Banco de México deberán sujetarse a las facultades y atribuciones que a dicho Banco Central confieren la Ley del Banco de México (LBM), el RIBM 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 de la persona titular y la expectativa razonable de privacidad. En su obtención, las personas servidoras públicas 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 de la persona titular, salvo las excepciones previstas en la Ley.

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

6. Las personas 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 las personas 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 y demás disposiciones aplicables. En todo caso, para determinar los plazos de conservación correspondientes, deberán atenderse a 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 de la persona titular, conforme a la LGPDPPSO.

10. Las personas servidoras públicas 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 definida por las Unidades Administrativas competentes del Banco y los análisis de riesgos respectivos.

11. Las personas servidoras públicas 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.[9]

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 el cumplimiento de las obligaciones de transparencia en las plataformas correspondientes, las personas 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 (LGTAIP) y la LGPDPPSO, así como las disposiciones derivadas de tales ordenamientos.

13. Los derechos de las personas titulares en relación con sus datos personales deberán ser respetados por las personas servidoras públicas 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 demás disposiciones aplicables.

14. La Unidad de Transparencia establecerá procedimientos para recibir y responder dudas y quejas de las personas 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, así como a la normativa aplicable.

Asimismo, el Acuerdo SGSDP define criterios y lineamientos para establecer y mantener el Sistema de Gestión del Banco de México. Dicho instrumento establece un marco de coordinación para que las Unidades Administrativas del Banco, en el ámbito de sus atribuciones, lleven a cabo las tareas de planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales.

Finalmente, el referido Acuerdo SGSDP también contempla otras políticas y programas de protección de datos personales encaminadas a garantizar el cumplimiento de la normatividad aplicable en materia de personas encargadas, transferencias de datos personales y gestión y seguridad de la información.

Protección de la información

De conformidad con la LGPDPPSO y demás ordenamientos aplicables en la materia, los sujetos obligados, como el Banco de México, tienen el deber de proteger los datos personales que se traten con motivo del ejercicio de sus funciones o atribuciones. Para tales efectos, conforme a dichas

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

disposiciones, se deben establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico, para la protección de los datos personales contra su daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.[10]

Cabe tener presente que estas medidas de seguridad administrativas, físicas y técnicas se definen conforme a lo siguiente:[11]

a. **Medidas administrativas:** son políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

b. **Medidas físicas:** son el conjunto de acciones, mecanismos y procedimientos para proteger el entorno físico donde se resguardan los datos personales, así como los recursos involucrados en su tratamiento.

c. **Medidas técnicas:** son el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

A continuación, se establece un marco de referencia sobre las medidas de seguridad con las que Banco de México protege la información que posee y maneja, la cual incluye aquella que contiene datos personales. Dicho marco se constituye a través de la interacción coordinada entre las diversas Unidades Administrativas del Banco de México y los diversos hallazgos que cada una ha identificado, desde el ámbito de sus respectivas competencias.

Medidas administrativas[12]

La normatividad interna del Banco de México, además de las "Políticas y Lineamientos de Seguridad de la Información del Banco de México", prevé la existencia de otras directrices relacionadas con el tratamiento de datos personales, entre las que se encuentran 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; así como la sensibilización y capacitación del personal, en materia de protección de datos personales, incluidas en el ANEXO 1.

Asimismo, el Banco cuenta con una NAI denominada “Gestión de documentos de archivo”[13] 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 destino final, eliminación o conservación permanente, así como la forma en que se otorgarán derechos de

[10] Artículo 25 de la LGPDPPSO.

[11] *Cfr.* Artículo 3, fracciones XIX, XX, y XXI, de la LGPDPPSO.

[12] 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”.

[13] Norma Administrativa Interna Gestión de Documentos de Archivo.

consulta a documentos de archivo. En ese sentido, a través de esta misma NAI se gestiona el ciclo de vida de los datos personales tratados por el Banco de México.

Medidas físicas

El Banco de México tiene la capacidad operativa y tecnológica necesaria para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. Al respecto, cuenta el macroproceso de Seguridad Física[14] debidamente documentado, cuyo propósito es coordinar y ejecutar las actividades correspondientes para salvaguardar la integridad del personal, los valores, a las terceras personas de interés institucional, así como las instalaciones de Banco de México, el cual es de observancia general. Asimismo, el Banco de México cuenta con una NAI que regula la entrada, permanencia y salida de las instalaciones, tanto de las personas servidoras públicas como de terceros: *"Entrada permanencia y salida a los inmuebles que ocupe el Banco de México, así como el control de sus bienes muebles"*[15]*,* en la cual se establece la clasificación de las áreas con base en criterios específicos, entre los cuales destaca el tipo de información que se procese en las mismas.

Entre las medidas físicas, destacan las siguientes:

1. Sistema de control de acceso automatizado, el cual permite a las personas servidoras públicas del Banco de México transitar sólo por las áreas donde tiene autorizado su ingreso, asimismo, permite realizar solicitudes de acceso temporales a sus inmuebles. Para tal efecto, deben utilizar la clave de empleado y una contraseña, de tal manera que ninguna persona ajena al Banco puede autorizar el acceso a dichos inmuebles. Además, los accesos son autorizados por personal con nivel mínimo de jefe de Oficina.

2. Las personas que ingresan de manera recurrente a las instalaciones del Banco Central son identificadas de forma debida, y se les asigna una credencial que permite el acceso sólo a las áreas autorizadas, lo cual es controlado a través de barreras físicas controladas por el sistema de control de acceso automatizado. Al respecto, se encuentra establecida la NAI *"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], a través de la cual se previene el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información. De igual manera, se tiene control respecto de los recursos móviles portátiles y cualquier soporte físico o electrónico que pueda entrar o salir de la Institución.

3. Se encuentran instaladas barreras físicas y equipos de inspección en los puntos de ingreso peatonal y vehicular que evitan el ingreso forzoso o no autorizado como son:

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

[14] Manual General de Macroproceso Seguridad Física.

[15] Norma Administrativa Interna Entrada permanencia y salida a los inmuebles que ocupe el Banco de México, así como el control de sus bienes muebles.

[16] 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.

b. Equipos de inspección de rayos x, así como detectores de metales en los accesos principales a los inmuebles para detectar objetos que puedan emplearse para facilitar un ataque.

c. Barreras físicas vehiculares (pilonas) y plumas de acceso, las cuales son liberadas por medio de la credencial de empleado, cuando está autorizado, o de manera manual por personal de seguridad de servicio en los puntos de acceso a los estacionamientos de los inmuebles, previa validación de solicitud autorizada.

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

e. Cámaras de Circuito Cerrado de Televisión que conforman la principal herramienta para la evaluación de las diferentes situaciones que puedan presentarse, con grabación digital de las mismas.

f. Detección de incendio y sistema de voceo de emergencia, el cual permite al equipo de seguridad alterar al personal del Banco de México sobre cualquier evento de emergencia por incendio para la aplicación de los procedimientos de atención, así como la emisión de mensajes pregrabados por sismo o situaciones de emergencia de seguridad con el propósito de que se ejecuten los procedimientos definidos que le permitan salvaguardar su integridad física.

g. Los sistemas mencionados con anterioridad, envían las señales a los diferentes Centros de Coordinación y Control del Banco, los cuales operan todos los días para atender cualquier emergencia que se presente. Esta infraestructura es empleada por personal del propio Instituto Central debidamente capacitado para responder ante los diferentes escenarios que atañen a la seguridad física institucional.

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.

Medidas técnicas

El 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. Considerando las especificidades técnicas de cada proceso y sistemas que contienen datos personales, de manera enunciativa más no limitativa, se presentan algunas de las medidas técnicas empleadas para garantizar la seguridad de la información:

1. Gestión de accesos y privilegios.

a. Acceso a equipo de cómputo personal exclusivamente con cuentas individualizadas, sus respectivas contraseñas y con segundo factor de autenticación (como biométricos, PIN y tokens de un solo uso).

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

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

d. Doble factor de autenticación para el ingreso a los servicios de TI del Banco.

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

2. Seguridad de equipos de uso personal.

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

b. Distribución automática de actualizaciones de software.

c. Antivirus y Firewall personal.

d. Restricción de uso de software no certificado.

3. Seguridad de la provisión de servicios de TI.

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

b. 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.

c. Protección contra código malicioso en los servicios de TI, que integra el uso de herramienta antivirus, mecanismo de control de ejecuciones basadas en listas de aplicaciones permitidas y herramienta de protección en memoria.

d. Gestión de comunicaciones, operaciones y medios de almacenamiento de la información.

e. Proceso de gestión de vulnerabilidades informáticas.

f. Bitácoras de consulta de información en los sistemas.

4. Seguridad de red y telecomunicaciones.

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

b. Cifrado y encriptación en comunicaciones institucionales.

c. Protección en la red, por medio del uso de herramienta para detectar ligas a sitios y archivos adjuntos maliciosos.

5. Seguridad de los activos de información.

a. Implementación de solución del tipo *Data Loss Prevention* (DLP), para prevenir una posible fuga de información previamente categorizada y etiquetada, hacia el exterior del Banco.

b. Implementación de una herramienta de etiquetado de información.

c. Borrado seguro de los datos contenidos en un bien o insumo informático.

Programa de fortalecimiento de la seguridad de la información y datos personales en Banco de México

El Banco de México a través de su Programa de Reforzamiento Continuo de la Ciberseguridad promueve la mejora constante de la seguridad de los procesos del Banco, sus sistemas y la información que gestionan, la cual incluye los datos personales. Las acciones de dicho Programa están orientadas a implementar la ciberseguridad de forma amplia y proactiva con los responsables de los procesos y a fortalecer la identificación oportuna de amenazas, para favorecer la integridad, confidencialidad y disponibilidad de la información, con base en los objetivos estratégicos siguientes:

1. Fortalecer la normatividad en materia de ciberseguridad. Emitir y actualizar el marco normativo del Banco en materia de ciberseguridad, con base en estándares y principios internacionales.

2. Implementar controles de ciberseguridad. Identificar controles de ciberseguridad que refuercen los procesos del Banco, coordinar su instrumentación, así como verificar y dar seguimiento de su correcta implementación.

3. Crear una cultura de ciberseguridad. Diseñar e implementar el Programa Institucional de Concientización y Capacitación que permita reforzar la cultura de ciberseguridad de todo el personal del Banco, de acuerdo con sus perfiles y roles.

4. Fortalecer la ciberseguridad y ciberresiliencia en el Banco. Realizar evaluaciones, revisiones y pruebas para medir las capacidades de ciberseguridad y ciberresiliencia de los procesos del Banco.

5. Gestionar incidentes en el Banco. Fortalecer las capacidades de respuesta del Banco ante incidentes de ciberseguridad que afecten sus procesos, infraestructura, información o personal.

El referido Programa de Reforzamiento Continuo forma parte de la Estrategia de Ciberseguridad del Banco de México, la cual fue definida considerando el entorno actual de amenazas de ciberseguridad del Banco y del sistema financiero; los estándares y principios internacionales en materia de ciberseguridad; así como los Ejes rectores del Banco de México.

Tomando en cuenta que a través de dicha estrategia se fortalece la confidencialidad, disponibilidad e integridad de la información en posesión de este Banco Central y que, además, se contemplan medidas particulares para la custodia de la seguridad de la información que contiene datos personales, Banco de México en su carácter de Sujeto Obligado, da cumplimiento a las obligaciones establecidas en el marco normativo de protección de datos personales aplicable, entre otras, a través del Sistema de Gestión descrito en el presente Documento, así como de la referida estrategia.

DOCUMENTO DE SEGURIDAD

A continuación, se desarrolla el contenido del Documento de Seguridad requerido por la normatividad aplicable. Para mejor referencia se presenta la siguiente tabla, que relaciona los requisitos legales del mencionado Documento con los elementos a través de los cuáles Banco de México da cumplimiento a sus obligaciones en materia de protección de datos personales:

Requisitos mínimos del Documento de Seguridad[17]	Elemento institucional
Inventario de datos personales y de los sistemas de tratamiento	Identificación de los activos de información y levantamiento del inventario de datos personales contenidos en dichos activos, a través de las actividades y responsabilidades establecidas en la NAI de Gestión de la Información.
Funciones y obligaciones de las personas que traten datos personales	Se tiene definidos roles y responsabilidades en la gestión de la información, a través de lo establecido en la NAI de Gestión de la Información y el Acuerdo SGSDP.
Análisis de riesgos	Evaluaciones de riesgos de seguridad de la información, conforme a la Metodología para la gestión de riesgos no financieros.
Análisis de brecha	
Plan de trabajo	Descripción de las actividades que se ejecutan de manera continua para la gestión de los activos de información y sus datos personales, conforme al Acuerdo SGSDP.
Mecanismos de monitoreo y revisión de las medidas de seguridad	Esquema para el seguimiento del monitoreo de las medidas de seguridad de datos personales en posesión del Banco de México, conforme al Acuerdo SGSDP.
Programa general de capacitación	Programa de capacitación en materia de protección de datos personales y temas relacionados, conforme a lo establecido en los acuerdos emitidos por el Comité de Transparencia, así como su implementación por la Unidad de Transparencia y la Autoridad Garante, en el ámbito de sus respectivas competencias.

[17] Conforme a lo establecido en el artículo 29 de la LGPDPPSO.

Inventario de datos personales y sistemas de tratamiento

La integración del inventario de datos personales forma parte de las actividades institucionales que se realizan para la gestión de activos de información, previstas en la NAI de Gestión de la Información, las cuales se describen a continuación:

1. **Identificación de los activos de información**. Se identifican y registran los tipos de activos de información que se gestionan en los procesos o actividades del Banco, y se describen sus características y relaciones para una gestión segura, eficiente y eficaz de los mismos. El inventario de activos de información contempla los siguientes elementos:

Tipo de característica	Característica
Definición del tipo de activo de información	Identificador
	Nombre
	Descripción
Responsable y relación con otros procesos	Responsable de información
	Proceso gestor[18]
	Proceso proveedor[19]
Contenido	Datos personales
	Información equiparable a dato personal[20]
	Microdatos
	Datos agregados o estadísticas
	Registros operativos
	Material normativo
	Material administrativo
	Material jurídico, legal o civil
	Información de fuentes abiertas
	Información de propiedad intelectual
Formato	Formato físico
	Formato electrónico

[18] Nombre del proceso al cual pertenece el inventario.

[19] Nombre del proceso que genera y comparte el activo de información identificado.

[20] Información concerniente a personas jurídicas colectivas, de carácter económico, comercial o relativos a su identidad, que de revelarse pudieran anular o menoscabar su libre y buen desarrollo, y que en consecuencia deben permanecer ajenos al conocimiento de terceros.

Tipo de característica	Característica
Uso	Contribución en los Ejes Rectores
	Contribución en otros procesos
Ubicación	Ubicación física
	Ubicación electrónica
Gestión	Referencia específica a los componentes o servicios de TI utilizados
	Participación de un tercero
	Periodicidad de gestión
	Normatividad interna
	Categoría de información

2. **Inventario de datos personales**. Una vez que se tienen identificados los activos de información, se lleva a cabo la identificación de los datos personales, así como los aspectos relevantes enlistados a continuación:

Sección	Subsección
Datos personales	Datos de identificación
	Datos de contacto
	Datos laborales
	Datos académicos
	Datos patrimoniales o financieros
Datos personales sensibles	Datos biométricos
	Datos ideológicos
	Datos sobre opiniones políticas
	Datos sobre afiliación sindical
	Datos sobre características físicas
	Datos de salud
	Datos sobre sexualidad
	Datos sobre origen étnico o racial
Características del tratamiento de datos personales	Medio Principal de Obtención (físico y/o electrónico)

	Requiere consentimiento[21] del titular
	Aviso de privacidad[22]
	Los datos fueron sometidos a un proceso de disociación[23] previo al tratamiento
	Finalidad de tratamiento[24]
	El tratamiento se realiza de manera manual o automatizada
	Medidas de seguridad que los resguardan
	Servidor (es) Público (s) con acceso al Sistema de tratamiento
	Datos de contacto de la Unidad Administrativa que realiza el tratamiento
	Instrumento jurídico que formaliza el tratamiento
	Periodo estimado de conservación de los datos Personales
Participación de personas encargadas[25] en el tratamiento de los datos Personales	Nombre de los encargados
	Instrumento jurídico con el que se formaliza la relación entre el responsable y el encargado

[21] Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos. El consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología. El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

[22] Aviso de privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

[23] Procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo. Cuando los datos personales se sometan a un procedimiento previo de disociación, el responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales.

[24] 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.

[25] La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

	Finalidad del tratamiento por parte del encargado
	El encargado subcontrata servicios para el tratamiento de los datos personales
Transferencias de datos personales	Destinatario o tercero receptor a los que se transfieren los datos personales
	Instrumento jurídico que formaliza las transferencias
	Finalidad de la transferencia
Conservación de datos personales	Formato de almacenamiento.[26]
	Bloqueo de datos personales
	Supresión de datos personales
	Volumen histórico estimado de registros de personas físicas diferentes

3. **Categorización de los activos de información**. Se determina la categoría de los activos de información, considerando en particular el caso en que los tipos de activos de información contengan datos personales, y se registra en el inventario de activos de información.

   Asimismo, los servicios de TI y sus componentes son categorizados en concordancia con la categoría de información de los activos que se gestionan en éstos.

   La categorización de los activos de información y de los servicios de TI que los contienen, permite dirigir los recursos de protección a la información que impacta y contribuye en mayor medida a los procesos que respaldan la misión del Banco.

4. **Etiquetado de los activos de información**. Una vez determinada la categoría, los activos de información son etiquetados o identificados conforme a ésta, a fin de ser fácilmente identificables y gestionarse de acuerdo con la categoría asignada a su tipo.

[26] El detalle de la ubicación (física y/o tecnológica), es recabada en inventario de activos de información.

Funciones y obligaciones de las personas que tratan datos personales

En Banco de México, los roles y responsabilidades de las personas servidoras públicas para el tratamiento de datos personales se encuentran definidas en la NAI de Gestión de la Información, así como en el Acuerdo SGSDP, conforme a lo que se indica a continuación:

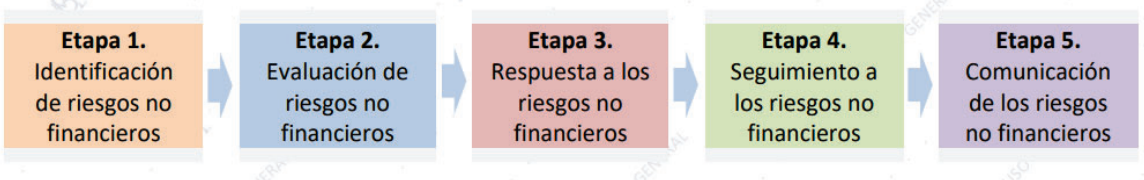
Rol	Cargo	Responsabilidad
Responsable de información	Persona trabajadora con puesto de subgerente o superior que es responsable de la gestión de activos de información que se realiza en algún proceso del Banco.	Instruye, organiza y supervisa las actividades para la gestión de activos de Información, incluyendo datos personales, en los procesos a su cargo, conforme a los establecido en la NAI de Gestión de la Información.
Personal del Banco de México	Todos.	Lleva a cabo la gestión de activos de información, incluyendo datos personales, en los procesos en los que participa, conforme lo establecido en la NAI de Gestión de la Información.
Responsable Tecnológico de Información	Persona titular de una Unidad Informática que asiste con Servicios de TI para la automatización total o parcial de un proceso que gestiona activos de información.	Instruye, organiza y supervisa las actividades para la gestión de activos de información, incluyendo datos personales, asociados a los procesos que son soportados por los Servicios de TI a su cargo.
Dirección de Administración de Riesgos	Gerente/Subgerente/Líder de Especialidad/Analistas de la Gerencia de Riesgos No Financieros.	Establece la metodología para categorizar los tipos de activos de información y para evaluar los riesgos de seguridad de la información. Apoya a los responsables de información en la categorización de sus activos de información, así como en la realización de evaluaciones de riesgos para su gestión, incluyendo los datos personales contenidos en los mismos.
Dirección de Seguridad y Organización de la Información	Persona titular de la Subgerencia de Seguridad Informática.	Proporciona las guías de implementación de las medidas de seguridad en los componentes de TI que soportan el sistema de información.
Unidad de Transparencia.	Líder de Especialidad en datos personales.	Documenta el inventario de datos personales y sus respectivos sistemas de tratamiento.

		Promueve las prácticas de protección de datos personales en el Banco.
Dirección de Control Interno y Dirección de Ciberseguridad	Personas titulares de la Gerencia de Control Normativo, Gerencia de Evaluación y Seguimiento de Control, y Gerencia de Seguimiento.	Dan seguimiento al monitoreo de la seguridad de los datos personales.
Dirección de Seguridad y Organización de la Información	Persona titular de la Subgerencia de Arquitectura de la Información.	Mantiene el inventario de activos de información y datos personales, procurando la oportuna actualización ante la modificación de los procesos y sistemas de tratamiento. Capacita al personal del Banco en aspectos de gestión y seguridad de la información, así como en la normatividad interna aplicable.

Cabe señalar que toda actuación de las personas servidoras públicas del Banco de México queda sujeta a la legislación y normatividad que regula la operación de este Banco Central. En ese sentido, las consecuencias ante el incumplimiento de las responsabilidades en materia de protección de datos personales, dan lugar a la aplicación de medidas disciplinarias o sanciones en términos de las disposiciones aplicables, y de conformidad con lo dispuesto en los Códigos de Ética y de Conducta del Banco de México.

Análisis de riesgos y brecha

El Banco de México lleva a cabo el análisis de riesgos y brecha mediante la aplicación de la metodología para la Gestión de Riesgos No Financieros, la cual tiene como objetivo llevar a cabo la identificación, evaluación, respuesta, seguimiento, y comunicación de los riesgos a los que está expuesto el Banco, con el propósito de que todos los involucrados, desde la Alta Dirección, hasta el personal que ejecuta los procesos o administra los recursos necesarios para ejecutarlos[27], conozcan tanto el nivel de exposición a riesgos, como su participación en el control y seguimiento de los mismos. La Metodología está conformada por las etapas siguientes:



[27] Servicios de TI, inmuebles, equipamiento, etc.

1. Identificación de riesgos no financieros: Identificar aquellos eventos que en caso de materializarse pueden afectar la entrega o provisión de los productos o servicios intermedios o finales que genera el proceso, la información u otros recursos del Banco.

2. Evaluación de riesgos no financieros: Estimar la probabilidad o frecuencia con la que pueden materializarse los riesgos y el impacto que tendrían.

3. Respuesta a los riesgos no financieros: Determinar la estrategia de respuesta a cada riesgo residual identificado, la cual puede ser cualquiera de las siguientes: Reducir, Transferir, Evitar o en el caso de contar con los controles suficientes para mitigar el riesgo residual, se considerará que el riesgo se encuentra Gestionado. Se identifican también las acciones de mitigación del riesgo residual y el plan de trabajo para implementarlas.

4. Seguimiento a los riesgos no financieros: Dar seguimiento a la implementación de las acciones de mitigación establecidas en la etapa de Respuesta, así como verificar selectivamente su implementación.

5. Comunicación de los riesgos no financieros: Dar a conocer a todos los involucrados el informe sobre la exposición a riesgos no financieros del Banco, principalmente a los grupos de interés: a) a la Alta Dirección; b) al personal encargado de la ejecución de los procesos y responsables de los servicios de TI, y c) a distintos comités.

Con base en la referida metodología, se realiza la **Evaluación de Riesgos de Seguridad de la Información** (**ERSI**), a fin de identificar aquellos factores de riesgo que puedan afectar la gestión segura de los activos de información del Banco, incluyendo aquellos que contienen datos personales, considerando el ciclo de vida de la información[28] y los servicios de TI utilizados para su uso y tratamiento. La ERSI contempla las fases siguientes:

[28] Conjunto de etapas por las que atraviesan los activos de información, desde su creación hasta su destrucción. Conforme a la NAI "Gestión de la Información" estas etapas son la planeación, la creación, el almacenamiento, la compartición, el enriquecimiento, la depuración y la destrucción de los activos de información.

En la fase 1, **recopilación de información**, se identifica aquella relacionada con la creación, almacenamiento, uso, compartición, resguardo y disposición de la información utilizada en la gestión del proceso, así como la información técnica y operativa de los servicios de TI que lo automatizan, lo anterior en coordinación con los responsables de la gestión del proceso y de las soluciones de TI.

En la fase 2, **identificación y evaluación de riesgos**, se identifican los controles de seguridad implementados en el proceso y en los servicios de TI utilizados para la gestión de la información y se valida que éstos se encuentren alineados a lo establecido en la normatividad interna. Posteriormente, se obtienen los factores de riesgo a partir de la identificación de los controles que son requeridos conforme al marco normativo del Banco de México y que aún no han sido implementados (la determinación de los factores de riesgo y el establecimiento posterior de acciones de mitigación corresponden al análisis de brecha en el Banco de México). Finalmente, se estima la probabilidad de materialización de los factores de riesgo y del impacto que tendría a la Institución la vulneración de los atributos de seguridad de la información, considerando los controles implementados.

La estimación del impacto se determina con base en la afectación negativa que pudiera ocasionar al Banco y, en su caso, al titular de los datos personales, el que se comprometa la confidencialidad, integridad o disponibilidad de los activos de información del proceso evaluado. Para realizar esta estimación se consideran cuatro dimensiones de impacto: operativo, monetario, reputacional y, al titular de los datos personales, este último sólo en caso de que el activo de información contenga dichos datos.

Respecto a la estimación de la probabilidad, se tienen definidos criterios que evalúan qué tan factible es que un atacante pueda aprovechar el factor de riesgo identificado para perpetrar un ataque.

En la fase 3, **elaboración de matriz de riesgos e informe de resultados**, se elaboran los referidos entregables, en los cuales se incluyen los controles implementados para la gestión de la información, los factores de riesgo identificados, la estimación de impacto y probabilidad de que el factor de riesgo se materialice, y la propuesta de acciones de mitigación para implementar nuevos controles o fortalecer los existentes, a fin de atender los factores de riesgo identificados (con ello se complementa el análisis de brecha). Estos resultados se comunican a las áreas correspondientes.

Plan de trabajo

La instrumentación de las acciones descritas, hasta ahora, es esencial en la selección adecuada de las medidas de seguridad para garantizar la confidencialidad, integridad y disponibilidad de los datos personales y los sistemas de tratamiento.

A continuación, se define el Plan de trabajo, el cual está compuesto por acciones de ejecución constante y prolongada en el tiempo, cuyo objetivo es contribuir a la mejora continua y robustecimiento de la seguridad de la información en posesión de este Instituto Central, particularmente, aquella que contiene datos personales. No se omite señalar que dicho Plan es susceptible de ser modificado, en caso de requerirse por nuevas necesidades institucionales.

Unidad Administrativa	Acción	Descripción
Dirección de Seguridad y Organización de la Información	Identificación de activos de información	Desarrollo de las actividades relacionadas con el inventario de activos de información.
	Identificación de roles y personal que realicen tratamientos de datos personales	Identificación del personal cuyas actividades impliquen tratamiento de datos personales.
	Implementación de medidas de seguridad técnicas	Diseño de las medidas de seguridad de la información conforme a las necesidades operativas del Banco.
Unidad de Transparencia	Revisión de instrumentos jurídicos relacionados con protección de datos personales	Revisión, actualización, baja o creación de Avisos de Privacidad. Brindar asesoría a las Unidades Administrativas que pretendan celebrar instrumentos legales que estipulen la contratación de personas encargadas, servicios tecnológicos que impliquen el tratamiento de datos personales o que conlleven la transferencia de datos personales.
	Revisión de normatividad interna en materia de protección de datos personales	Revisión y en su caso, actualización de la normatividad que establezca obligaciones a cargo de las personas servidoras públicas del Banco en materia de protección de datos personales.
	Capacitación en materia de protección de datos personales	Colaboración, de manera conjunta, con la Autoridad Garante para asegurar que las personas servidoras públicas del Banco reciban capacitación en la materia acorde al nivel de

Unidad Administrativa	Acción	Descripción
		tratamiento de datos personales que realicen, de conformidad con sus atribuciones.
	Identificación de datos personales en activos de información	Ejecución de las tareas relacionadas con el levantamiento de inventario de datos personales.
	Actualización del inventario de datos personales	Asesoramiento a las Unidades Administrativas que requieran actualizar sus respectivos inventarios, ante cambios operativos en sus procesos.
Dirección de Administración de Riesgos	Categorización de activos de información	Coordinación y asesoramiento a los responsables de información en la determinación de la categoría de información asociada a la afectación negativa que puede generar al Banco o en su caso, al titular de datos personales, el que se comprometa la confidencialidad, integridad o disponibilidad de los activos de información.
	Evaluación de riesgos de seguridad de la información	Identificación de los factores de riesgo que puedan afectar la gestión segura de los activos de información del Banco, incluyendo aquellos que contienen datos personales. Como parte de las evaluaciones, se establecen las acciones de mitigación para fortalecer la seguridad de la información de los procesos y servicios de TI que los soportan.

Unidad Administrativa	Acción	Descripción
Dirección de Control Interno	Seguimiento al monitoreo de la seguridad de datos personales	Ejecución de las acciones del esquema de seguimiento del monitoreo de las medidas de seguridad de datos personales.
Dirección de Ciberseguridad	Evaluación, revisión y comprobación del control de la ciberseguridad	Establecimiento y ejecución de los procedimientos de verificación del diseño y la efectividad de los controles en operación, así como de su implementación.
	Seguimiento y verificación de la atención de vulnerabilidades informáticas	Establecimiento y ejecución de los procedimientos de seguimiento y verificación de la atención de las vulnerabilidades que son identificadas.
Unidad de Auditoría	Verificación de tratamientos de datos personales	Realización de pruebas específicas de verificación de tratamientos de datos personales en las auditorías que se realicen.

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, para una adecuada gestión de la seguridad de la información.

Monitoreo y revisión de medidas de seguridad

La LGPDPPSO prevé que los sujetos obligados deben implementar una serie de actividades interrelacionadas para establecer y mantener sus medidas de seguridad, las cuales deberán estar documentadas y contenidas en un Sistema de Gestión.[29] Asimismo, en el Documento de Seguridad de cada sujeto obligado, se deben señalar, entre otros aspectos, los mecanismos de monitoreo y revisión de dichas medidas de seguridad.[30]

[29] Cfr. Artículos 27 y 28 de la LGPDPPSO.

[30] Artículo 29, fracción VI, de la LGPDPPSO.

En términos del Acuerdo SGSDP, las personas servidoras públicas del Banco de México tienen la obligación de actualizar, monitorear y revisar las medidas de seguridad implementadas para la protección de los datos personales, con base en la metodología que determinen las áreas competentes del Banco y los análisis de riesgos respectivos.[31]

Asimismo, en relación con los alcances de dicho monitoreo, el Acuerdo SGSDP establece que la Dirección de Control Interno y la Dirección de Ciberseguridad deberán llevar a cabo el seguimiento del monitoreo de la seguridad de los datos personales, a través de la implementación de un esquema que se basa en la aplicación de un cuestionario que se proporciona de forma bienal a las Unidades Administrativas del Banco, para que, conforme a sus respuestas, se pueda conocer el estado de las medidas de seguridad administrativas, físicas y técnicas que tengan implementadas para la protección de los datos personales. Lo anterior, con el propósito de conocer periódicamente el estado de control, con la finalidad de obtener una seguridad razonable sobre el funcionamiento del Sistema de Gestión, así como de las acciones de mejora continua.[32]

En particular, el objetivo de la aplicación de este cuestionario es conocer lo siguiente:[33]

a) En materia de medidas administrativas: el estado que guarda, en su caso, la normatividad que las Unidades Administrativas del Banco hayan emitido relacionada con dichas medidas, así como si requiere en su caso de alguna actualización.

Adicionalmente, la Dirección de Control Interno, por conducto de la Gerencia de Control Normativo, en coordinación con la Unidad de Transparencia,[34] podrán solicitar a las Unidades Administrativas, previo a la aplicación del cuestionario, que confirmen si han emitido normatividad adicional relacionadas con estas medidas.

Lo anterior con la finalidad de que, la Unidad de Transparencia, con base en sus atribuciones, pueda asesorar a las Unidades Administrativas del Banco sobre la normatividad interna que será considerada como parte de las medidas de seguridad administrativas de datos personales[35].

Cabe señalar que, como parte de las medidas de seguridad administrativas, el Banco cuenta con dos canales de comunicación para difundir la normatividad interna relacionada con las mismas, así como sus actualizaciones: i) el Catálogo de Normas Internas y ii) el correo electrónico institucional. El primero es el medio de difusión oficial, para que el personal del Banco de México tenga conocimiento del contenido de la normatividad interna que les resulta de observancia obligatoria. En el segundo caso, se notifican al personal, las actualizaciones correspondientes a través de ese medio, incluyendo las relativas al tratamiento de datos personales, y en su caso, sus nuevas responsabilidades a fin de garantizar un manejo adecuado de la información.

---

[31] Primero, numeral 10, del Acuerdo SGSDP.

[32] *Cfr.* Séptimo y Anexo Único del Acuerdo SGSDP.

[33] *Cfr.* Anexo Único, fracción II, del Acuerdo SGSDP.

[34] *Cfr.* Anexo Único, fracción II, segundo párrafo, del Acuerdo SGSDP.

[35] *Cfr*. Artículo 31 Bis, fracción XXIV, del Reglamento Interior del Banco de México.

b) **En materia de medidas de seguridad físicas y técnicas:** identificar los cambios en los activos de información en los que se gestionan datos personales, y que no hayan sido reflejados en los inventarios respectivos, así como la existencia de amenazas no valoradas, nuevas vulnerabilidades o cambios en su impacto o consecuencias, así como si se han presentado incidentes de seguridad. Cabe señalar, que para conocer lo anterior, el referido cuestionario se aplica a las Unidades Administrativas que han concluido con el levantamiento del inventario de datos personales, y la categorización de los activos de información respectivos.

El resultado de las actividades de seguimiento del monitoreo realizadas por la Dirección de Control Interno y la Dirección de Ciberseguridad, son presentadas a través de un informe que se rinde ante el Comité de Transparencia del Banco de México, a efecto de que este órgano colegiado esté en posibilidad de actuar en el ámbito de sus atribuciones. Asimismo, estos resultados también se hacen del conocimiento de la Unidad de Transparencia, la Dirección de Seguridad y Organización de la Información, y de la Dirección de Administración de Riesgos, para que programen, en su caso y en el ámbito de su competencia, el asesoramiento a las áreas responsables de la información.[36]

Programa General de Capacitación

De conformidad con la LGPDPPSO, es responsabilidad de los Sujetos Obligados diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades, respecto del tratamiento de los datos personales, como parte de las actividades para establecer y mantener las medidas de seguridad para la protección de los datos personales.

Asimismo, conforme al Acuerdo SGSDP, la Unidad de Transparencia deberá presentar anualmente ante el Comité de Transparencia, el programa que prevea la capacitación del personal en materia de protección de datos personales, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.[37]

El Banco de México constantemente brinda e incentiva la capacitación de sus personas servidoras públicas en materia de protección de datos personales. De manera particular se ha enfocado en las personas servidoras públicas que tratan datos personales de manera preponderante. Ha desarrollado cursos especializados en temas como vulneración de datos personales, sistema de gestión de datos personales, ciclo de vida de datos personales, entre otros.

Por otra parte, el artículo 83 de la LGPDPPSO prevé la atribución de las Autoridades Garantes de promover la capacitación y actualización en materia de protección de datos personales entre los responsables; asimismo, el artículo 84 del ordenamiento citado, establece que los responsables deberán colaborar con las Autoridades Garantes para capacitar y actualizar a las personas servidoras públicas que tengan adscritas en materia de protección de datos personales. Por las razones anteriores, la Autoridad Garante y la Unidad de Transparencia de este Instituto Central colaborarán en la promoción y el desarrollo de cursos de capacitación en dicha materia, respectivamente.

[36] *Cfr.* Séptimo, último párrafo, y Anexo Único, fracción IV, del Acuerdo SGSDP.

[37] Noveno, del Acuerdo SGSDP.

En tal sentido, las personas servidoras públicas del Banco de México deberán participar en los programas y cursos de capacitación en materia de Protección de Datos de Personales, conforme al programa de capacitación que establezca el Comité de Transparencia de conformidad con lo dispuesto en los artículos 31, fracción VII, y 31 Bis, fracción XXVIII, del RIBM.

El 30 de septiembre de 2025, 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 1o., 29, 77 y 78, fracciones I, IV y V, de la LGPDPPSO, así como 4o. y 31, fracciones II, V, XVI, y XX, del RIBM. Conste. ----------

COMITÉ DE TRANSPARENCIA

_____

CLAUDIA TAPIA RANGEL
Integrante
Unidad de Transparencia

_____

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante
Dirección de Seguridad y Organización de la Información

_____

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente
Dirección Jurídica

ANEXO 1 – NORMATIVIDAD INTERNA RELACIONADA CON MEDIDAS DE SEGURIDAD ADMINISTRATIVAS

No.	Tipo de norma	Título
1.	Condiciones	Condiciones Generales de Trabajo del Banco de México
2.	Código	Código de conducta del Banco de México
3.	Código	Código de ética del Banco de México
4.	Acuerdo	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 de protección de datos personales
5.	Acuerdo	Acuerdo por el que se establece el procedimiento interno de atención de solicitudes de acceso a la información
6.	Acuerdo	Acuerdo por el que se establece la obligación de las personas servidoras públicas del Banco de México para participar en los cursos de capacitación en materia de transparencia, acceso a la información y protección de datos personales
7.	Acuerdo	Acuerdo por el que se establecen los criterios para determinar plazos aplicables para el bloqueo y supresión de datos personales
8.	Acuerdo	Acuerdo por el que se establecen los formatos de avisos de privacidad del Banco de México
9.	Acuerdo	Acuerdo que regula la relación del Banco de México con personas encargadas y las transferencias de datos personales
10.	Acuerdo	Criterios para determinar valores documentales y plazos de conservación de documentos de archivo
11.	NAI	Actuación ante incidentes de ciberseguridad en el Banco de México
12.	NAI	Capacitación y adiestramiento
13.	NAI	Entrada, permanencia y salida a los inmuebles que ocupe el Banco de México, así como el control de sus bienes
14.	NAI	Gestión de documentos de archivo
15.	NAI	Gestión de la Información
16.	NAI	Gestión de riesgos derivados de la relación con terceras personas proveedoras del Banco de México
17.	NAI	Lineamientos en materia de gestión de riesgos no financieros, continuidad operativa y ciberseguridad de los Sistemas de Pagos por Banco de México

No.	Tipo de norma	Título
18.	NAI	Lineamientos para el testado seguro de información en formato electrónico
19.	NAI	Lineamientos para la gestión de eventos de seguridad informática del Banco de México
20.	NAI	Medidas de seguridad para el control de acceso de los proveedores y contratistas
21.	NAI	Políticas y lineamientos de seguridad de la información del Banco de México
22.	NAI	Provisión de servicios de tecnologías de la información
23.	NAI	Reglamento del Servicio Social
24.	NAI	Tecnologías de información para las personas usuarias
25.	MPO	Administración de antivirus para servidores y computadoras personales
26.	MPO	Administración del archivo de concentración y servicios de apoyo a los archivos de trámite
27.	MPO	Administración del Archivo Histórico
28.	MPO	Administrador Institucional de Documentos de Archivo
29.	MPO	Aplicación de parches en servidores institucionales
30.	MPO	Atención de actualizaciones del Inventario de Activos de Información
31.	MPO	Atención de Vulnerabilidades en la Dirección de Desarrollo de Sistemas
32.	MPO	Borrado seguro de información en bienes e insumos informáticos
33.	MPO	Carpetas compartidas
34.	MPO	Control de bienes e insumos informáticos
35.	MPO	Control de la infraestructura de Ciberseguridad y Ciberresiliencia
36.	MPO	Detección de vulnerabilidades informáticas de la Subgerencia de Seguridad Informática
37.	MPO	Evaluación y seguimiento del Sistema de Control Interno
38.	MPO	Gestión y Soporte de Información
39.	MPO	Identificación y evaluación de riesgos no financieros y seguimiento de control
40.	MPO	Pruebas Internas de Seguridad Informática
41.	MPO	Recolección Evaluación y Registro de Vulnerabilidades Informáticas

No.	Tipo de norma	Título
42.	MPO	Seguimiento y verificación de la atención de vulnerabilidades informáticas
43.	MPO	Servidores Institucionales

Banco de México publica su normatividad interna en cumplimiento a las obligaciones comunes en materia de transparencia y acceso a la información. En este sentido, dicha información puede ser consultada a través del Sistema de Obligaciones de Transparencia (SOT) del Banco de México, a través de los siguientes pasos:

a. Ingresar a la página oficial del Banco de México: https://www.banxico.org.mx/;

b. Hacer clic en el botón "Transparencia", ubicado en la esquina superior derecha;

c. Dirigirse a la parte inferior de la página electrónica y seleccionar el apartado de "Obligaciones de transparencia" y seleccionar "Sistema de Obligaciones de Transparencia del Banco de México";

d. Ingresar a la sección de Transparencia de la página oficial del Banco de México: https://transparencia.banxico.org.mx/VisorTransparencia/?BMXC_sujeto=BM&BMXC_articulo=Art70;

e. Seleccionar el ejercicio actual a la fecha de consulta;

f. Seleccionar la sección que quiere consultar (en este caso, fracción "*I. Marco normativo*").

La referida información también puede ser consultada directamente en la Plataforma Nacional de Transparencia (PNT), a través de los siguientes pasos:

a) Ingresar a la liga de Internet: https://consultapublicamx.plataformadetransparencia.org.mx/vut-web/faces/view/consultaPublica.xhtml#inicio (sugerimos copiar y pegar la liga en su navegador de Internet);

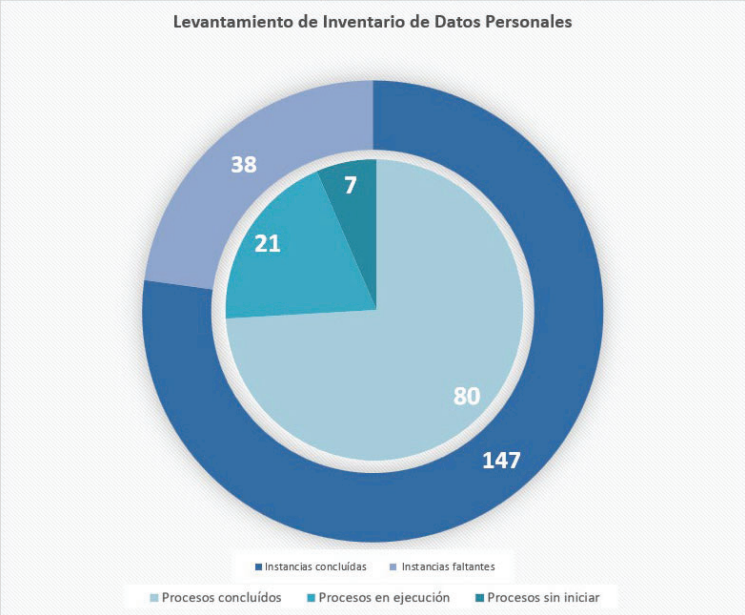
b) Seleccionar el ámbito de gobierno de la institución: en el campo "*Estado o Federación*", seleccionar "*Federación*";

c) Seleccionar la Autoridad Garante Federal: "OIC- *Banco de México*";

d) Seleccionar en el listado de "*Institución*", el registro correspondiente a "*FED - Banco de México (BANXICO)*";

e) Buscar y seleccionar el ícono "*NORMATIVIDAD*".

ANEXO 2 – INVENTARIO DE DATOS PERSONALES



Banco de México cuenta con 108 procesos institucionales. Dichos procesos pueden ser ejecutados por una o varias Unidades Administrativas en colaboración. En el segundo caso, la participación de cada Unidad Administrativa es referida como "instancia". Los activos de información son inventariados según las instancias de cada proceso.

El levantamiento de inventarios de datos personales, de igual manera, se realiza respecto de cada una de ellas por lo que, considerando la cantidad de activos de información gestionados a través de cada Unidad Administrativa, este Instituto Central continúa con el levantamiento de los inventarios descritos en el presente apartado.

No obstante, se informan las principales actividades que la Unidad de Transparencia lleva a cabo en seguimiento a los hallazgos resultantes de la aplicación del inventario de datos personales:

- Determinar la necesidad de actualizar los Avisos de Privacidad correspondientes o de generar los que fueran necesarios, en su caso.
- Identificar a los proveedores que lleven a cabo tratamientos de datos personales y, en consecuencia, adquieren la calidad de personas encargadas.
- Identificar las transferencias de datos personales realizadas por el Banco de México a terceros, ya sea a autoridades o particulares.
- Promover la actualización de los instrumentos jurídicos a través de los que se formalizan las relaciones del Banco de México con personas encargadas, receptores de transferencias y proveedores de servicios de cómputo en la nube que conllevan el tratamiento de datos personales.
- Emitir recomendaciones relacionadas con el tratamiento de datos personales desde una perspectiva archivística y de gestión documental.
- Contribuir al análisis de la pertinencia de las medidas de seguridad adoptadas.

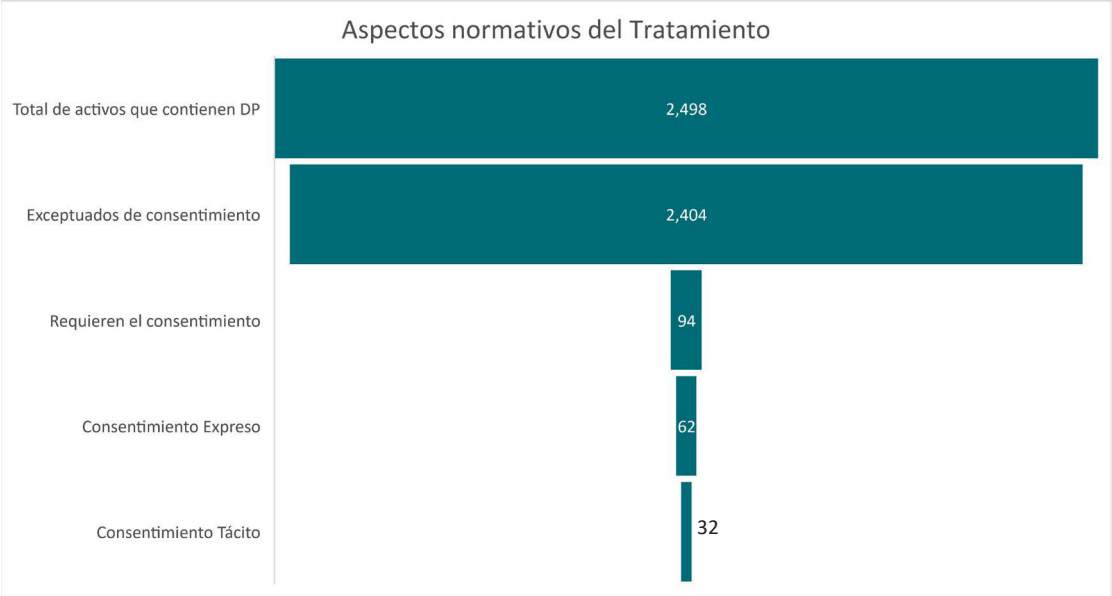
Procesos inventariados

En los 80 procesos cuyas instancias han sido inventariadas en su totalidad hasta ahora, **se han identificado un total de 4,002 activos de información, de los cuáles, 2,498 contienen datos personales. Es decir, el 62% de los activos de información inventariados hasta ahora contienen algún tipo de dato personal.** Cabe recordar que este Instituto Central, a diferencia de otros Sujetos Obligados y en virtud de sus competencias, facultades y atribuciones, lleva a cabo interacciones con el público en general, limitadas a ámbitos específicos. En consecuencia, la mayor parte de los datos personales en su posesión corresponden al personal que labora en esta institución. A continuación, se presenta la cantidad de activos de información en los que se han detectado diferentes tipos de datos personales:

Tipo de dato personal	Descripción	Número de activos	Porcentaje
De identificación	Información concerniente a una persona física que permite diferenciarla de otras en una colectividad, principalmente, respecto de personas servidoras públicas de la Institución.	2,444	98%
Laborales	Información concerniente a una persona física relativa a su empleo, cargo o comisión; desempeño laboral y experiencia profesional generada a partir de procesos de reclutamiento, selección, contratación, nombramiento, evaluación y capacitación.	1,690	68%
De contacto	Información que permite mantener o entrar en contacto con su titular.	953	38%
Académicos	Información concerniente a una persona física que describe su preparación, aptitudes, desarrollo y orientación profesional o técnica, avalada por instituciones educativas.	699	28%
Patrimoniales o financieros	Información concerniente a una persona física relativa a sus bienes, derechos, cargas u obligaciones susceptibles de valoración económica.	556	22%
Datos personales sensibles	Datos biométricos, de salud, opiniones políticas, características físicas, sobre sexualidad, ideológicos, sobre origen étnico o racial, sobre afiliación sindical.	269	11%

Obtención del consentimiento

Considerando la naturaleza de las personas titulares de datos personales, que en su mayoría son las personas servidoras públicas de esta institución, se ha identificado que únicamente se requiere obtener el consentimiento de las personas titulares previo al tratamiento realizado a través de 94 activos de información. De los cuales, se identificó la necesidad de recabar el consentimiento de forma expresa para los datos personales tratados solo en 62 activos de información, así como de manera tácita en 32 activos. Por cuanto hace a los 2,404 activos de información restantes, se ha concluido que su tratamiento se encuentra exceptuado de la obligación de obtención del consentimiento, dado que actualiza alguno o varios de los supuestos previstos por el artículo 16 de la LGPDPPSO.



El registro de los inventarios de datos personales también ofrece información relevante sobre la manera en que se realizan los tratamientos a que son sometidos los datos personales en el Banco de México.

Medio principal de obtención de los datos personales

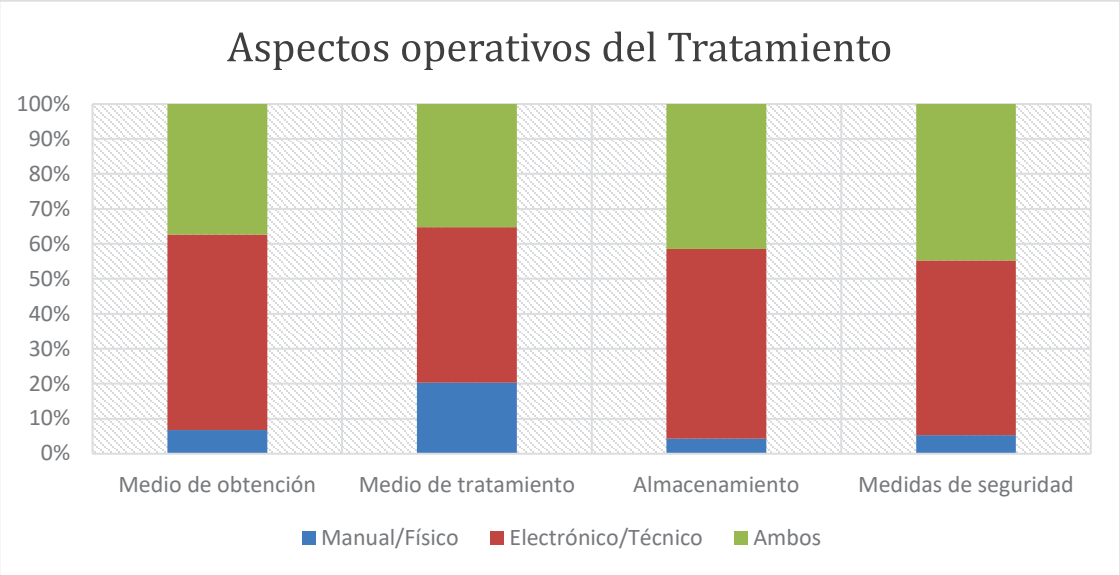
Prepondera el uso de medios de recolección electrónicos, que son utilizados en 1,395 activos de información. El uso mixto de medios electrónicos y físicos para recabar datos personales se encuentra en 933 activos de información y finalmente, en 170 activos, se utilizan medios exclusivamente físicos.

Formas de tratamiento, almacenamiento y medidas de seguridad

Primordialmente se emplean medios electrónicos en 1,111 activos de información. La combinación de tratamientos llevados a cabo de forma tanto manual como electrónica fue reportada en 880 activos, mientras que en los 507 que restan solo se utilizan medios manuales para efectuar el tratamiento.

En este contexto, destaca la información relativa al formato de almacenamiento de la información. Se ha identificado que 1,355 activos de información son conservados en formato electrónico. Por otro lado, 1,035 activos se almacenan de manera tanto electrónica como física y finalmente, 108 son guardados de forma física.

Tomando en cuenta lo anterior y considerando que la normatividad interna en materia de Gestión de la Información es una medida de seguridad administrativa, se ha reportado la implementación de medidas técnicas para resguardar 1,249 activos de información. Por otro lado, se utilizan medidas de seguridad tanto técnicas como físicas en 1,117 activos. Finalmente, se cuenta con registros de que 132 activos son protegidos únicamente con medidas de seguridad físicas.



Ciclo de vida de los activos de información que contienen datos personales.

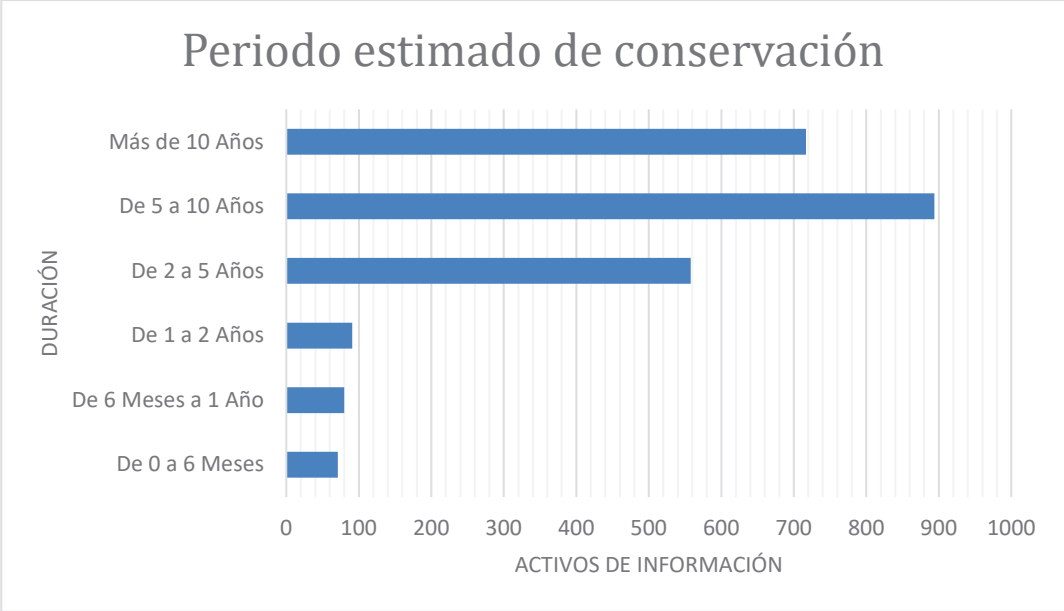
De conformidad con lo dispuesto por la Ley General de Archivos (LGA), el ciclo vital de los documentos de archivo comprende las etapas por las que estos atraviesan, desde su producción o recepción hasta su baja documental o transferencia a un archivo histórico[38]. Por otro lado, la LGPDPPSO identifica las etapas del ciclo de vida de los datos personales.[39] A fin de compaginar los ciclos de vida entre ambas legislaciones, este Instituto Central asoció las etapas de estos dos ciclos de vida de la siguiente manera:

FASE	Protección de datos personales	Materia archivística
1	Tratamiento	Archivo de trámite
2	Bloqueo	Archivo de concentración
3	Supresión	Baja documental

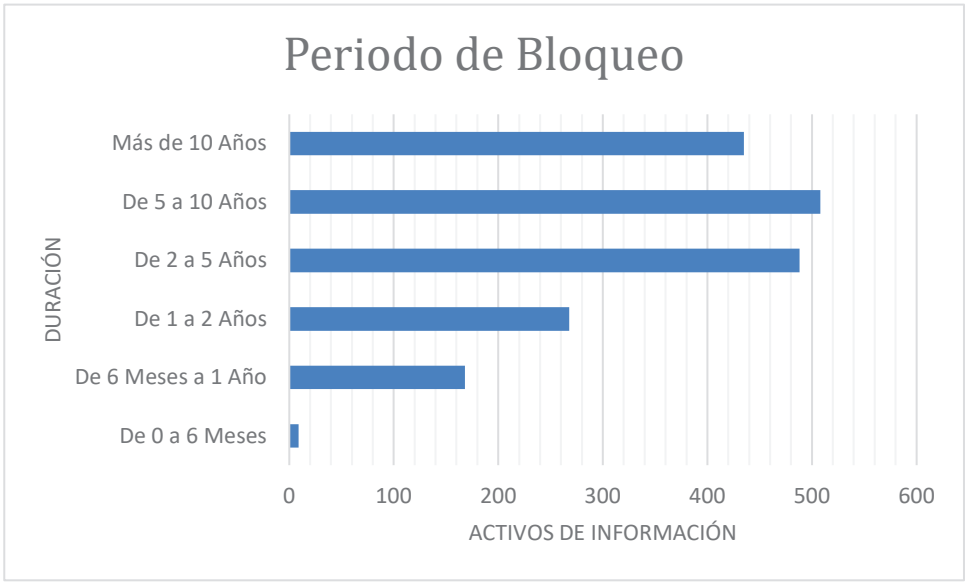
[38] LGA, artículo 4, fracción XIV.

[39] LGPDPPSO, artículo 27, fracción I.

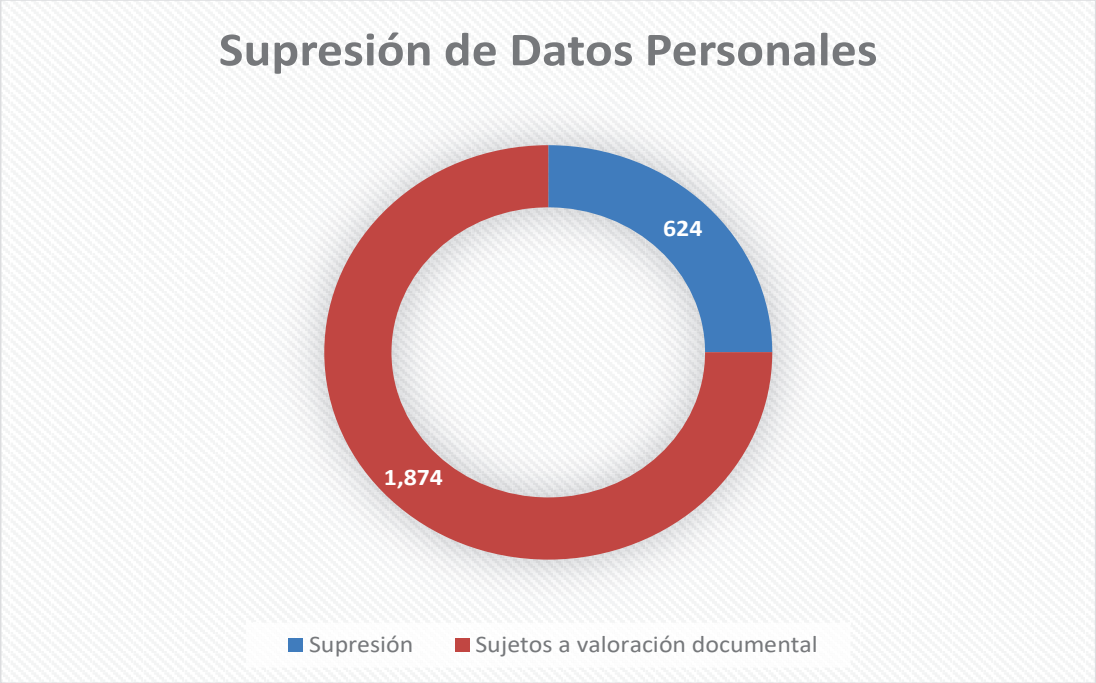
En este sentido, el inventario de datos personales guarda registro del periodo total de conservación de los activos de información que contienen datos personales. A continuación, se visualiza la distribución del tiempo que comprende el ciclo de vida de los datos personales en este Instituto Central.



A continuación, se muestra la distribución de la duración del periodo de bloqueo para los activos de información a los que resulta aplicable.



Finalmente, se tiene prevista la supresión como técnica de disposición documental para 624 activos. En lo relativo a los 1,874 activos restantes, su conservación se sujetará a la valoración documental que realicen las Unidades Administrativas responsables de los activos de información, con la finalidad de decidir si los eliminan o si en su caso los conservan permanentemente.



Personas encargadas del tratamiento

A través del levantamiento de Inventarios de datos personales, se ha identificado el uso de servicios prestados por terceros ajenos a la organización del Banco que implican el tratamiento de datos personales a nombre y por cuenta de este Instituto Central, actualizando así la figura de persona encargada prevista en la LGPDPPSO. Esta relación ha sido registrada en 8 activos de información, lo que equivale al 0.3% de los activos de información que contienen datos personales. Cabe señalar que ninguna de estos proveedores lleva a cabo subcontrataciones para la prestación de sus servicios. Las finalidades del tratamiento que realizan las personas encargadas son:

- Prestación de servicios de cómputo en la Nube.
- Asesoría y gestoría jurídica y contable.
- Levantamiento de estudios y encuestas.

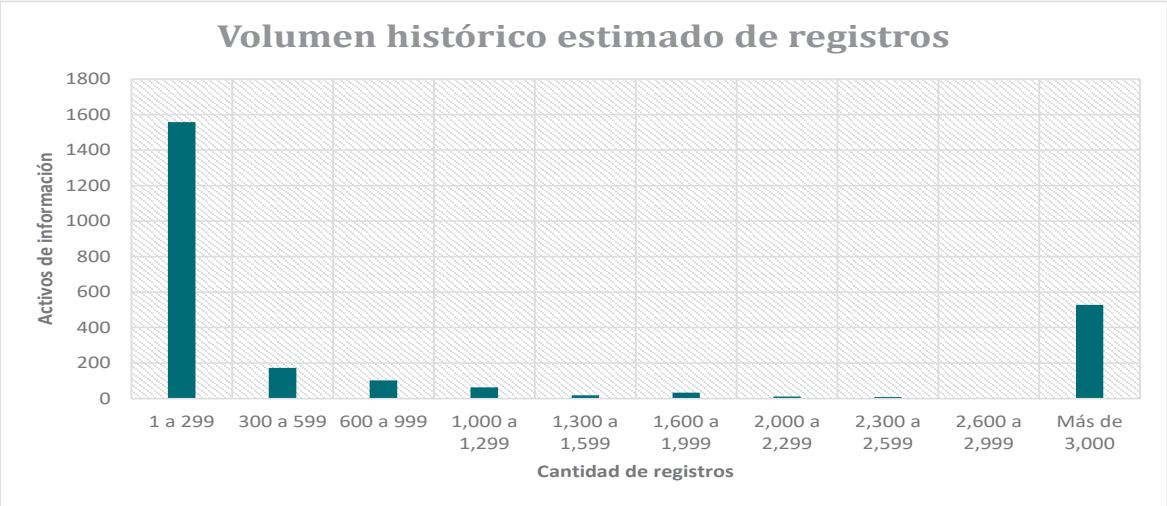
Transferencias de datos personales

Asimismo, se tiene registro de la realización de transferencias de los datos personales contenidos en 213 activos de información, lo que equivale al 9% de los activos. De conformidad con las disposiciones legales vigentes, estas transferencias se encuentran exentas de documentarse, toda vez que se realizan para dar cumplimiento a disposiciones legales o en el ejercicio de atribuciones expresamente conferidas a los responsables involucrados.

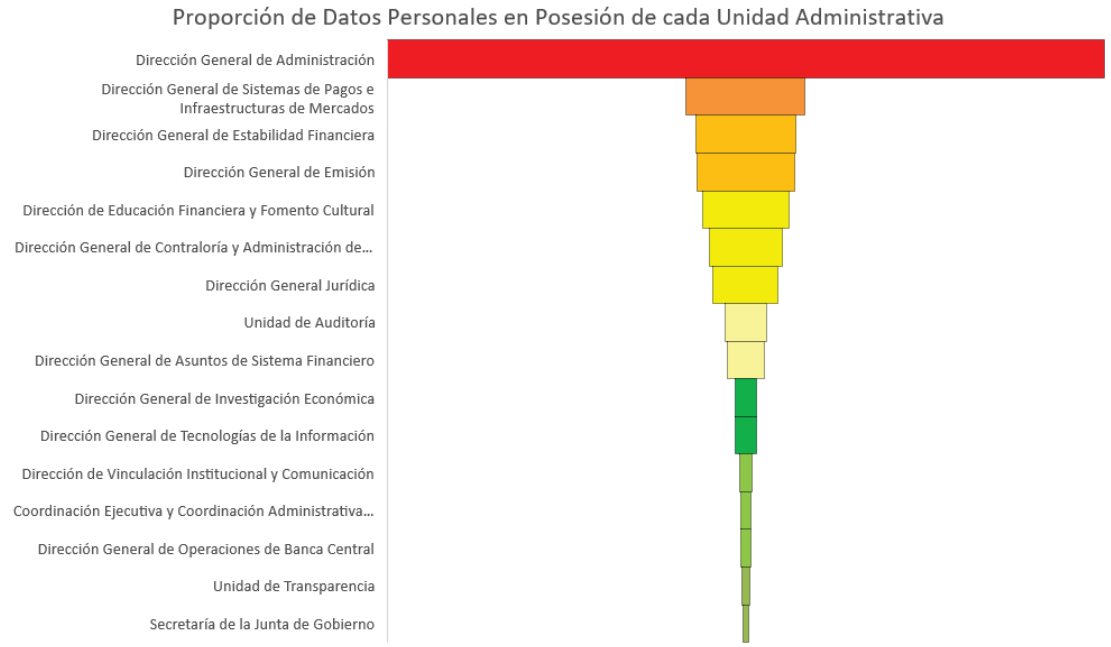
Al respecto, los instrumentos jurídicos que formalizan las relaciones de Banco de México con personas encargadas y receptores de trasferencias pueden ser consultados en la sección “Deberes” del aparatado virtual de protección de datos personales.

Volumen aproximado de registros de personas titulares de datos personales

El número de personas titulares de las que se tiene registro en los activos de información, se proyecta en rangos que van desde 1 a 299 personas titulares y hasta más de 3,000 personas titulares.

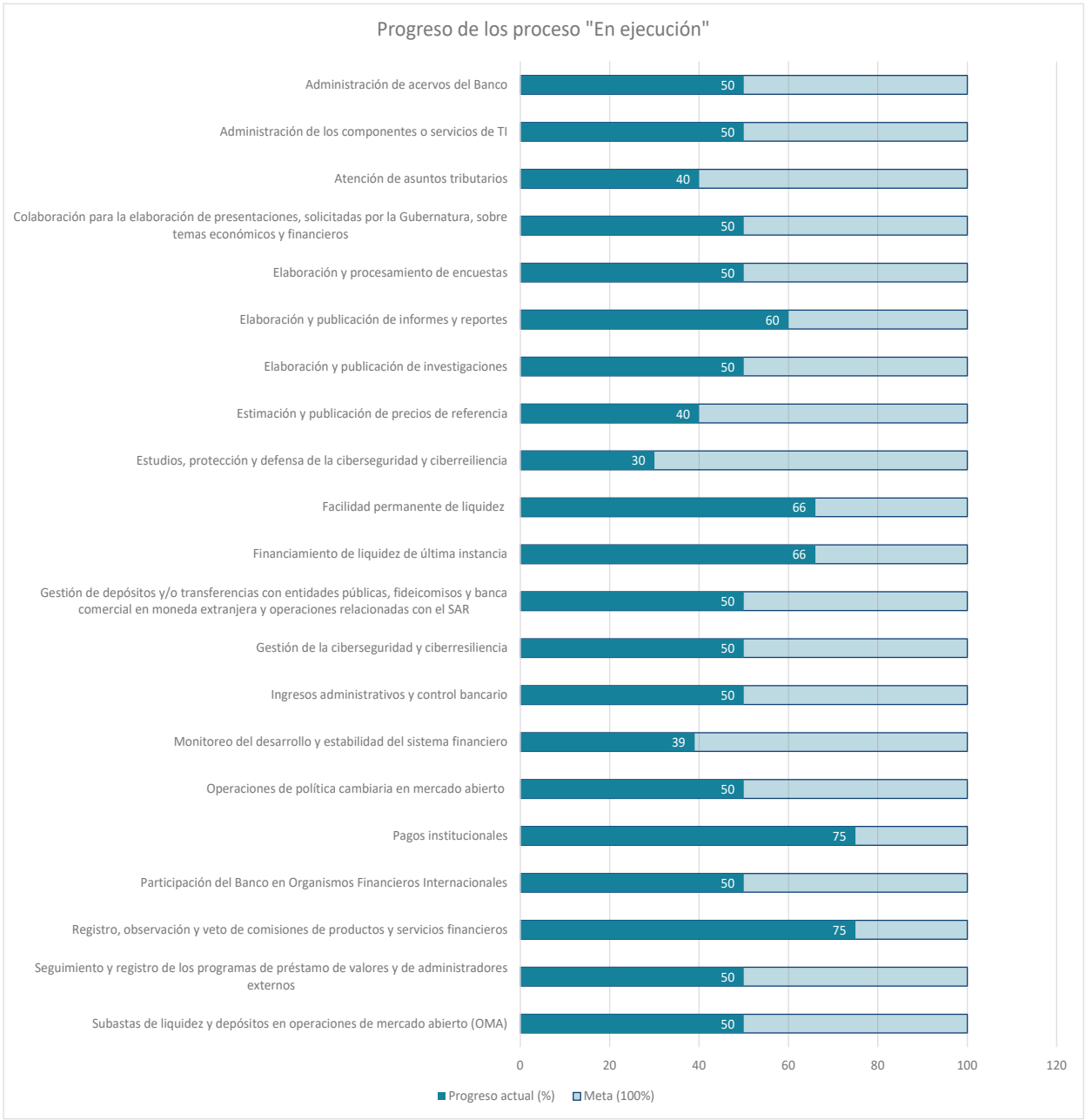


A partir de esta información es posible distinguir a las Unidades Administrativas del Banco de México con más datos personales bajo su resguardo, mismas que se visualizan de manera proporcional en el siguiente mapa de calor.



Como se ha explicado anteriormente, la mayoría de los datos personales tratados por este Instituto Central corresponden a las personas servidoras públicas que trabajan en esta Institución, lo que explica que la Dirección General de Administración, a la que se encuentra adscrita la Dirección de Recursos Humanos, concentre una mayor cantidad de información relativa a personas físicas, en comparación con otras Unidades Administrativas.

Finalmente, las Unidades Administrativas encargadas de los procedimientos relativos al levantamiento de inventarios de datos personales continúan trabajando para finalizar las tareas correspondientes a los 21 procesos reportados como “En ejecución”, así como para dar inicio y pronta conclusión a los 7 procesos reportados como “Procesos sin iniciar”. El siguiente cuadro visualiza el porcentaje de avance en las tareas relativas al levantamiento de inventarios de información respecto a los procesos en estado de ejecución:



BANCO DE MÉXICO®

www.banxico.org.mx

Documento firmado digitalmente, su validación requiere hacerse electrónicamente.
Información de las firmas:

FECHA Y HORA DE FIRMA	FIRMANTE	RESUMEN DIGITAL
30/09/2025 12:31:42	Edgar Miguel Salas Ortega	8d5ff6660fa7e4804f06dcf1cf824dd39ff1b2afeef0bf54cab63a79bbb19655
30/09/2025 14:38:17	VICTOR MANUEL DE LA LUZ PUEBLA	48b16e1ebf46511c9a5d35b0bfbdae9fa517c6c0d3fe528d06a6d2e36ab25de4
30/09/2025 14:45:43	Claudia Tapia Rangel	4fd6d0441e600368179f5025b63a01c3da808efe631ec92f4c6f414f31e21ff9