Políticas Internas de Gestión y Tratamiento de los Datos Personales de la Casa de Moneda de México.

Contenido.

Introducción..... 3

II. Proposito 4

II. 1 Objetivos de la Política..... 4

II. 2 Alcance..... 5

III. Antescedentes 6

Glosario.....7

IV. Políticas de Gestión y Tratamiento de Datos Personales de Acuerdo con la LGPDPPSO y los Lineamientos Generales: contenido mínimo y requisitos.....8

IV.1 Disposiciones Generales.....9

IV.2 Contenido de la Política General de Gestión y Tratamiento de Datos Deberes para la Protección de Datos Personales.....18

IV.3 Políticas Técnicas Complementarias de Protección de Datos Personales.....22

V. Roles y Responsabilidad de los encargados de Redactar las políticas.....30

VI. Sanciones.....30

VII. Revisión, Evaluación y Mejora de las Políticas de Gestión y Tratamiento.....31

I. INTRODUCCIÓN

La Casa de Moneda de México, por su naturaleza jurídica es un Organismo Descentralizado de la Administración Pública Federal, coordinado sectorialmente por la Secretaría de Hacienda y Crédito Público, y en tal carácter es un sujeto obligado en términos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) que protegerá los datos personales en su posesión, por esta razón, se da a conocer a los usuarios las siguientes políticas, basadas en la normatividad vigente.

El presente documento constituye una política interna de la Casa de Moneda de México, elaborado y basado en el principio de responsabilidad, el cual prevé que las personas responsables del tratamiento de datos personales deberán implementar mecanismos para el cumplimiento de las principios, deberes y obligaciones establecidos en las disposiciones en materia de protección de datos personales.

La Casa de Moneda de México, es responsable de proteger los datos personales garantizando los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, los deberes de seguridad y confidencialidad, y las obligaciones derivadas de la LGPDPPSO. Los mecanismos que prevé la Ley tienen por objeto establecer los elementos y las actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de funciones y atribuciones impliquen un tratamiento de datos personales, a efecto de proteger éstos de manera sistemática y continua.

La instrumentación de esta política de protección de datos personales facilitará a las personas titulares de las unidades administrativas de esta Entidad, realizar un tratamiento de datos personales en estricto apego a los principios, deberes y obligaciones establecidos en las disposiciones aplicables, lo cual permitirá garantizar la adecuada protección de los datos personales y el ejercicio de los derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad (Derechos ARCOP). Asimismo, de conformidad con el artículo 85, fracción VII de la LGPDPPSO, la Unidad de Transparencia de esta Entidad, será la responsable de asesorar a todas las unidades administrativas que la integran en materia de protección de datos personales.

II. PROPÓSITO

El objetivo de esta Política Interna para el Cumplimiento del Tratamiento de Datos Personales en Posesión de la Casa de Moneda de México, es garantizar el cumplimiento de los principios, deberes y obligaciones en materia de protección de datos personales, establecer mejores prácticas y estándares, así como elementos y actividades de dirección, operación y control en los procesos en que las unidades administrativas de esta Entidad, en el ejercicio de sus funciones, realicen algún tratamiento de datos personales y explicar cómo se tratan y protegen los datos personales que sean recolectados por esta Entidad dando la seguridad de que los datos serán almacenados en plataformas seguras

II. 1 Objetivos de la Política

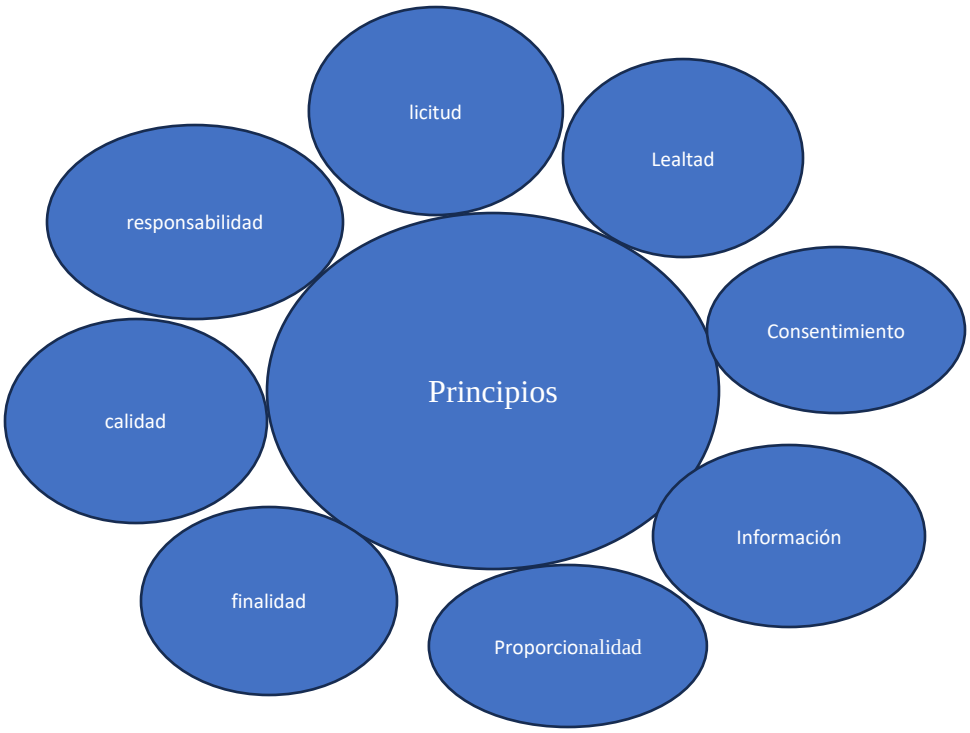
1. Cumplir con las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público, así como la normatividad que derive de los mismos.
2. Proveer el marco de trabajo necesario para el tratamiento y la protección de los datos personales en posesión de esta Entidad.
3. Establecer las directrices y herramientas necesarias, para garantizar la protección de los datos personales en posesión de las unidades administrativas, por medio de la sensibilización, capacitación, implementación, operación, revisión, mantenimiento y mejora de las acciones diseñadas para el tratamiento y la seguridad de los datos personales.
4. Promover la adopción de mejores prácticas en materia de protección de datos personales, a efecto de lograr una mayor participación de los servidores públicos de la Entidad, con relación al ejercicio de los derechos ARCO, así como proporcionar a la ciudadanía la certeza de que sus datos personales en posesión de esta Entidad, están siendo tratados de conformidad con lo establecido en el marco normativo.

II.2 Alcance

La aplicación y cumplimiento de la presente Política Interna para el Cumplimiento del Tratamiento de Datos Personales en Posesión de la Casa de Moneda de México, es de observancia general para todo el personal involucrado en el tratamiento de datos personales.

La aplicación y cumplimiento de la presente es obligatoria para las personas titulares de las unidades administrativas de la Entidad, las cuales son responsables de cualquier tratamiento de datos personales con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización, así como establecer las medidas necesarias que garanticen la seguridad de los datos personales que en el ámbito de su competencia posean, recaben o transmitan, con el fin de evitar su alteración, daño, destrucción o en su uso, acceso o tratamiento no autorizado, pérdida y transmisión, debiendo asegurar su manejo para los propósitos para los cuales se hayan obtenido. Lo anterior de conformidad con lo establecido en los artículos 3, fracción I y XXXIII y 4 de la LGPDPPSO.

Ámbito de Aplicación: El presente documento es de aplicación y observancia general y obligatoria para todas las personas servidoras públicas de la Entidad que conforme a sus atribuciones realicen tratamiento de datos personales.



III. Antecedentes

Es oportuno precisar, que la elaboración de las Políticas de Gestión de Datos Personales es parte de la implementación del cumplimiento de las obligaciones en materia de Protección de Datos Personales, el cual deben sujetarse al Documento de Seguridad de esta Entidad, lo cual facilitará definir los alcances y objetivos de la gestión de datos personales, se trata de definir los límites en la aplicación del sistema de gestión de la seguridad de los datos personales.

Definir el alcance se refiere a entender qué actividades que se realizan en cualquier etapa del tratamiento de los datos personales, definir que unidades administrativas de la entidad manejan datos personales, los procesos, sistemas de datos personales, medidas de seguridad de los datos personales y los sistemas del tratamiento con que cuenta la Entidad, así mismo el impacto que puede causar la vulnerabilidad de los datos para los titulares como resultado de pérdidas de confidencialidad, integridad o disponibilidad.

Es importante precisar, que se realizará una evaluación de identificación de los siguientes elementos para poder precisar y definir las obligaciones y alcances que tiene esta entidad en materia de datos personales.

- Inventario de Datos Personales, de acuerdo con la normatividad aplicable, esto permitirá saber que datos son los que se manejan en los sistemas de tratamiento de esta entidad.

- Medios por los cuales se procesa la información y recaban los datos por parte de la entidad, archivos físicos, digitales y los medios de seguridad para resguardar los mismos.

- Definir que tipo de datos se recaban en los diferentes sistemas o procesos de datos por parte de la entidad y definir de acuerdo con su clasificación si estos son datos sensibles o no.

- Medidas de seguridad implementadas para el tratamiento de datos personales por parte de las áreas administrativas de esta entidad.

Una vez que han sido definidos los alcances y objetivos de la gestión de los datos personales se cuentan con los elementos y herramientas necesarias para comenzar a redactar una política general de gestión y seguridad que ayude al logro de los objetivos planteados, teniendo en cuenta que se trata de un sistema con el que se busca la mejora continua y que se requerirán múltiples políticas de gestión y tratamiento de datos, como se verá adelante.

III. 1 GLOSARIO

Comité de Transparencia: Es la autoridad máxima en materia de protección de datos personales y está encargado de conducir la política de transparencia de acuerdo con el marco normativo vigente. Para ello instituye, coordina y supervisa los procedimientos que aseguran la mayor eficacia en la gestión de las solicitudes de información y confirma, modifica o revoca las determinaciones sobre plazos de respuesta y reserva, clasificación de la información y declaración de inexistencia o incompetencia; ordena a las áreas competentes generar la información que dicta sus facultades y competencias aunado a las demás atribuciones que pacte la normatividad en materia de transparencia, acceso a la información y protección de datos personales.

Datos personales: Cualquier información relativa a una persona física identificada o identificable, con independencia del carácter íntimo o privado que pudiera reconocérsele, cuya manifestación puede ser numérica, alfabética, gráfica, acústica, o fotográfica, entre otras. No obstante, suele distinguirse una categoría especial de datos personales, denominados datos sensibles, cuyos estándares legales de protección se elevan.

Derechos ARCOP: Derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad, todos ellos relacionados con el tratamiento de datos personales.

Inventario de Sistemas de datos personales: Identificación de las bases de datos de tratamiento de datos personales en posesión de las unidades administrativas, por el cual, se documenta la información básica de cada tratamiento realizado, con independencia de su forma de almacenamiento, entre lo cual se incluye el ciclo de vida del dato personal.

CMM: Casa de Moneda de México

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Órgano Garante: Es el Órgano especializado y colegiado responsable de coordinar y supervisar la puesta en marcha de la política de acceso a la información y el cumplimiento de las obligaciones que desprende de ella.

Portabilidad de Datos Personales: Prerrogativa de las personas titulares de datos personales que les permite, bajo las condiciones establecidas en la normatividad aplicable, recibir los datos personales que han proporcionado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable del tratamiento sin impedimentos.

Principios: El derecho a la protección de los datos personales se regula a través de dichos principios, los cuales se traducen en obligaciones, estos son: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

Responsable: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos que deciden sobre el tratamiento de datos personales.

Titular: La persona física a quien corresponden o conciernen los datos personales sujetos a tratamiento y por tanto es quien se considera como sujeto de protección del derecho a la protección de datos personales.

Tratamiento de datos personales: Conjunto de acciones de procesamiento de los datos personales (pueden ser: obtención, uso, divulgación o almacenamiento). El uso puede abarcar cualquier acción de acceso, manejo, aprovechamiento, transferencias o disposición de éstos.

Unidad administrativa: Las previstas en el Manual de Organización de la Casa de Moneda de México.

Unidad de Transparencia: Es la oficina administrativa, dentro del inmueble que ocupan las oficinas corporativas de Casa de Moneda de México,; encargada de publicar la información generada en el ejercicio de sus competencias y recabar, difundir y dar trámite a las solicitudes de acceso a la información, a fin de que se otorgue una respuesta en tiempo y forma. La Unidad de Transparencia cuenta con un responsable cuyas funciones principales son publicar vía internet y a través de la PNT y difundir toda la información como resultado de las obligaciones de transparencia, así como de las políticas de transparencia proactiva.

IV. Políticas de Gestión y Tratamiento de Datos Personales de Acuerdo con la LGPDPPSO y los Lineamientos Generales: contenido mínimo y requisitos.

De conformidad al contenido de las políticas internas de gestión y tratamiento de los datos personales Artículo 56. Con relación a lo previsto en el artículo 33, fracción I de la Ley General, el responsable deberá incluir en el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, al menos, lo siguiente:

l. El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General y los presentes Lineamientos generales;

II. Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen;

III. Las sanciones en caso de incumplimiento;

IV. La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento,

divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados;

V. El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales, y

VI. El proceso general de atención de los derechos ARCO

IV. 1 Disposiciones Generales

La presente Política Interna para el Cumplimiento del Tratamiento de Datos Personales en Posesión de la Casa de Moneda de México es de observancia general para el personal involucrado en el tratamiento de datos personales.

El Comité de Transparencia como autoridad máxima en la materia velará por el debido cumplimiento y aplicación de la presente Política.

La Unidad de Transparencia de la CMM asesorará a las Unidades Administrativas en materia de protección de datos personales conforme a los principios, deberes y obligaciones establecidos en la normativa aplicable.

Para las actividades señaladas en la presente Política, serán las personas titulares de las unidades administrativas de CMM, quienes se encarguen de la protección de datos personales y así mismo establecer un canal de comunicación efectiva con la Unidad de Transparencia de la CMM.

Las personas titulares de las unidades administrativas son los responsables del tratamiento de los datos personales en el ámbito de sus facultades y atribuciones; y, por lo tanto, tendrán la obligación de cumplir los principios, deberes y obligaciones establecidos en la normatividad aplicable.

El Comité de Transparencia de CMM podrá sugerir a las unidades administrativas que realicen o eviten ciertas acciones con el fin de prevenir algún incumplimiento a las disposiciones en materia de protección de datos personales.

Si el Comité de Transparencia de CMM advierte un hecho que conlleve a constituir una probable falta administrativa en materia de datos personales en términos de la norma aplicable, darán vista al Jefe de la Oficina de Representación de la Secretaría de la Función Pública en CMM para su conocimiento y realizará las acciones procedentes conforme a la normativa aplicable.

El Comité de Transparencia se auxiliará de la Unidad de Transparencia de CMM para el ejercicio de sus funciones previstas en la presente Política.

Principios de Protección de Datos Personales

De acuerdo a lo estipulado en el artículo 16 de la Ley General en relación con el artículo 7 de los Lineamientos Generales, los principios de protección de datos personales son las herramientas para garantizar la efectiva protección de los datos personales de sus titulares cuando son tratados; herramientas de uso obligatorio para interpretar y aplicar la Ley General y demás normativa aplicable y representan un límite al tratamiento de datos personales que se encuentran en posesión de sujetos obligados.

El derecho a la protección de datos personales se rige a través de ocho principios, que son, Licitud, Finalidad, Lealtad, Consentimiento, Calidad, Proporcionalidad, Información y Responsabilidad. Por lo tanto, las personas titulares de las unidades administrativas de CMM responsables del tratamiento de datos personales deberán observar estos principios rectores de la protección de estos.

1.Principio de Licitud: Significa que las personas servidoras públicas deberán asumir un comportamiento ético y responsable, en el tratamiento de los datos personales que poseen en sus unidades administrativas, sujetándose a las atribuciones o facultades que la normatividad aplicable les confiera.

2. Principio de Finalidad: Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales, y solo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas a la persona titular en el aviso de privacidad y, en su caso, consentidas por éste.

Las finalidades deben ser concretas, explicitas, lícitas y legítimas, siendo importante que las personas servidoras públicas consideren lo siguiente:

Concretas: Cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.

Explícitas: Tienen lugar cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.

Lícitas: Cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable.

Legítimas: Cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento de la persona titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.

Las finalidades del tratamiento de datos personales deberán ser determinadas, es decir, las personas servidoras públicas están obligadas a especificar para que se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad.

3.-Principio de Lealtad: De acuerdo con el principio de lealtad, en la obtención de los datos personales las personas servidoras públicas no podrán usar medios engañosos, ni fraudulentos, lo que implica que:

i. No se recaben datos personales con dolo, mala fe o negligencia;
ii. No tratar los datos de tal manera que genere discriminación o un trato injusto contra las personas titulares.
iii. No se vulnere la confianza de las personas titulares con relación a que sus datos personales serán tratados conforme a lo acordado; y
iv. Se informen todas las finalidades del tratamiento en el aviso de privacidad.

4.-Principio de Consentimiento: Previo al tratamiento de los datos personales, las personas titulares de las unidades administrativas deberán obtener el consentimiento de las personas titulares de los datos personales de manera expresa o tácita, salvo que no sea requerido, en virtud de las siguientes causales de excepción descritos en el artículo 22 de la ley General:

1) Cuando una ley así lo disponga, en cuyo caso, los supuestos de excepción deberán ser acordes con las bases, principios y disposiciones establecidos en la Ley General que, en ningún caso podrán contravenirla;

2) Cuando las transferencias que se realicen entre CMM y otro sujeto responsable sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o acordes con la finalidad que motivó el tratamiento de los datos personales;

3) Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;

4) Para el reconocimiento o defensa de derechos de la persona titular ante la autoridad competente;

5) Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre las personas titulares y CMM;

6) Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

7) Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la prestación de asistencia sanitaria;

8) Cuando los datos personales figuren en fuentes de acceso público;

9) Cuando los datos personales se sometan a un procedimiento previo de disociación;

10) Cuando la persona titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley de la materia.

Como regla general, las personas servidoras públicas de CMM deberán contar con el consentimiento de la persona titular para el tratamiento de sus datos personales. Para obtener el consentimiento tácito, expreso o por escrito y dependiendo del tipo de datos personales, la solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general.

Aunado a ello, el consentimiento debe ser informado, por lo que previo a su obtención, es necesario que la persona titular conozca el aviso de privacidad, además de que debe ser libre tal y como lo refiere la LGPDPPSO, en el sentido que no medie error, mala fe, violencia o dolo que afecten la voluntad de la persona titular.

5.- Principio de Calidad: Significa que, conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos deben ser exactos, correctos, completos y actualizados. Las personas servidoras públicas están obligadas a:

- Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que la persona titular se vea afectado por dicha situación;

- Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo;

- Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales;

- Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación de conformidad con lo establecido por la Ley General de Archivos;

- Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales.

A efecto de cumplir con el principio de calidad, es necesario tomar en consideración los siguientes aspectos:

Conservación de los datos personales

El plazo de conservación de los datos personales no debe exceder el tiempo estrictamente necesario para llevar a cabo las finalidades que justificaron el tratamiento, ni aquél que se requiera para cumplir con:

- Las disposiciones legales establecidas en la Ley General de Archivos;
- Las disposiciones aplicables en la materia de que se trate;
- Los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información, y
- El periodo de bloqueo.

Es importante señalar que, en particular, el artículo 24 la Ley General, establece que se deben documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales respecto de cada tratamiento que se efectúe por las unidades administrativas.

Conclusión del plazo de conservación

Una vez concluido el plazo de conservación, y siempre que no exista disposición legal o reglamentaria que establezca lo contrario, las unidades administrativas de CMM deben proceder a la supresión de los datos personales. En este caso, deberán de informarlo a la Unidad de Transparencia, quien lo hará del conocimiento del Comité de Transparencia, a efecto de que determine lo conducente. Es importante recordar que el plazo de conservación debe incluir un periodo de bloqueo, ya que los datos personales deben ser bloqueados antes de que sean eliminados o suprimidos.

Además, en cuanto a los datos personales sensibles, el responsable debe realizar esfuerzos razonables para limitar el periodo de tratamiento al mínimo indispensable.

Bloqueo de los datos personales

El bloqueo se define como la acción que tiene por objeto impedir el tratamiento de los datos personales para cualquier finalidad, con excepción de su almacenamiento y acceso para determinar posibles responsabilidades en relación con el tratamiento de los datos personales, hasta el plazo de prescripción correspondiente. Las personas servidoras públicas están obligadas a: Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales. Concluido dicho periodo se deberá proceder a su supresión.

6.- Principio de Proporcionalidad: Las personas titulares de las unidades administrativas de CMM, recabarán aquellos datos personales que resulten necesarios, adecuados y relevantes para la finalidad que justifica su tratamiento. Se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas.

Las obligaciones para su cumplimiento por parte de las unidades administrativas de CMM que traten datos personales, son las siguientes:

- Recabar y tratar sólo aquellos datos personales necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron y, en su caso, privilegiar la utilización de datos generados por la propia CMM, para que el tratamiento de datos personales de la persona titular no sea excesivo, como por ejemplo usar el número de empleado en lugar de la CURP o el RFC.

Realizar esfuerzos razonables para limitar los datos personales tratados al mínimo necesario, considerando las finalidades que motivan su tratamiento.

- Limitar al mínimo posible el periodo de tratamiento de datos personales;
- Verificar si los datos personales que serán requeridos por la persona titular de la unidad administrativa para su tratamiento, ya son tratados por otra persona titular de una unidad administrativa diversa a la anterior.

Para acreditar el debido cumplimiento a este principio por parte de las personas titulares de las unidades administrativas de CMM, deberá realizar lo siguiente:

- Analizar y revisar que en su área se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate;
- Establecer con precisión los datos personales que deberán tratarse para cumplir con la finalidad, cuando una normativa establezca su obtención, sólo se deberán solicitar dichos datos;
- Promover prácticas que minimicen la obtención de datos personales.

7.-Principio de Responsabilidad: El principio de responsabilidad cierra el círculo con relación a los principios que regulan la protección de los datos personales. Este principio establece la obligación de las unidades de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y el órgano garante, que cumple con sus obligaciones en torno a la protección de los datos personales. Bajo este principio, las personas servidoras públicas responsables del tratamiento están obligados a velar por la protección de los datos personales aún y cuando los datos estén siendo tratados por encargados.

Asimismo, este principio supone que se tomen las medidas suficientes para que los términos establecidos en el aviso de privacidad sean respetados por aquéllos con los que

mantenga una relación jurídica, así como al momento de realizar transferencias nacionales o internacionales de datos personales.

También es conocido por el principio de rendición de cuentas, ya que como bien se dijo en el párrafo anterior, establece la obligación de velar por el cumplimiento del resto de los principios, así como los deberes que establece la normativa aplicable para dar cuenta a las personas titulares y la autoridad de que se cumple con las obligaciones de protección de datos personales.

Obligaciones Vinculadas al Principio de Responsabilidad

Las obligaciones para el cumplimiento del principio de Responsabilidad por parte de las personas titulares de las unidades administrativas de CMM que traten datos personales, son las siguientes:

- Participar en los programas de capacitación y actualización en materia de protección de datos personales;
- Establecer procedimientos para recibir y responder dudas y quejas de las personas titulares;
- Diseñar o modificar las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología con que cuente y que implique el tratamiento de datos personales, para que desde el inicio cumplan por diseño con las obligaciones previstas en la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable, previa opinión del Comité de Transparencia;
- Cumplir con los principios y deberes que establece la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

Las obligaciones para el cumplimiento del Principio de Responsabilidad, por parte de la Unidad de Transparencia:

- Recopilar de las Unidades Administrativas que traten datos personales, los insumos necesarios para elaborar un Programa de Protección de Datos Personales que provea los elementos y actividades de dirección, operación y control de los procesos en CMM, para proteger de manera sistemática y continua los datos personales en posesión de CMM;
- Diseñar e implementar a través del enlace de capacitación de CMM, los programas de capacitación y actualización que tengan por obligación capacitar al personal involucrado en el tratamiento de datos personales;
- Coordinar a las Unidades Administrativas de CMM para que se recopilen los datos personales que traten, así como los insumos necesarios para la elaboración del Documento de Seguridad que contemple las medidas de carácter administrativo, técnico, físico o cualquier otra;
- Revisar el cumplimiento de los procedimientos para recibir y responder dudas y quejas de las personas titulares.

Para acreditar el debido cumplimiento al Principio de Responsabilidad por parte de las Unidades Administrativas de CMM, se deberá realizar lo siguiente:

- Contar con las constancias de capacitación en materia de protección de datos personales;

- Llevar un registro de las dudas y quejas de las personas titulares de datos personales;

- Documentar la comunicación relacionada con el diseño o modificación de las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología con que cuente y que implique el tratamiento de datos personales;

- Documentar la comunicación relacionada con el cumplimiento de los principios y deberes que establece la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

Para acreditar el debido cumplimiento del Principio de Responsabilidad por parte de la Unidad de Transparencia de CMM, se deberá realizar lo siguiente:

- Coordinar a través del enlace de capacitación de CMM la implementación del Programa en materia de Protección de Datos Personales;

- Acreditar la capacitación con las constancias de los cursos en materia de protección de datos personales que al efecto proporcione el INAI.

- Realizar en su caso, la actualización del Programa de Protección de Datos Personales y revisar el Documento de Seguridad;

- Evidenciar del cumplimiento de los procedimientos para recibir y responder dudas y quejas de las personas titulares en caso de que existan;

- Observar el cumplimiento del procedimiento para el tratamiento de datos personales en políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología de diseño o modificación que cumplan con las obligaciones previstas en la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

- Guardar evidencia de las acciones realizadas para asegurar y acreditar el cumplimiento de los principios y deberes que establece la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

Principio de Información: Por virtud de este principio, las personas servidoras públicas de CMM se encuentran obligadas a informar a las personas titulares, las características principales del tratamiento al que será sometida su información personal, lo que se materializa a través del aviso de privacidad.

A fin de que las personas titulares puedan tomar decisiones informadas al respecto y puedan ejercer su derecho a la protección de su información personal, toda área que trate datos personales, sin importar la actividad que realice, requiere elaborar y poner a disposición los avisos de privacidad que correspondan a los tratamientos que lleven a cabo.

Es importante tomar en cuenta que con independencia de que se requiera o no el consentimiento de las personas titulares para el tratamiento de sus datos personales, el responsable está obligado a poner a su disposición el aviso de privacidad.

Las obligaciones para el cumplimiento del principio de Información por parte de las personas titulares de las unidades administrativas que traten datos personales, son las siguientes:

Redactar y elaborar el aviso de privacidad en sus dos modalidades: integral y simplificado, con las características principales del tratamiento al que serán sometidos los datos personales de la persona titular, estructurado de manera clara y sencilla que facilite su entendimiento y con los elementos establecidos por la Ley General y los Lineamientos Generales y tomando en consideración los Criterios de elaboración del INAI emitidos para tal efecto.

- Poner a disposición de las personas titulares el aviso de privacidad en los términos que fije la Ley General y los Lineamientos Generales, aunque no se requiera el consentimiento para el tratamiento de sus datos personales;

- Difundir, poner a disposición o reproducir el aviso de privacidad en formatos físicos y electrónicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su eficaz comunicación y permitan la accesibilidad para grupos vulnerables;

- Comunicar en el aviso de privacidad simplificado e integral, la información relativa en caso de haber transferencias;

Para acreditar el cumplimiento del principio de información, se deberá realizar lo siguiente:

- Contar con los avisos de privacidad integral y simplificado por cada proceso de tratamiento de datos personales que se lleve a cabo en CMM;

- Implementar un procedimiento o medio para la puesta de disposición del aviso de privacidad;

- Realizar las gestiones para que los avisos de privacidad, en su modalidad simplificada e integral, sean plasmados en un lugar visible que permita la consulta de las personas titulares;

- lugares y medios en los que se difunden y colocan los avisos de privacidad; como lo es medios electrónicos y para Casa de Moneda de México, será puede consultar los avisos de privacidad en la siguiente página: http://www.cmm.gob.mx/tienda/transparencia/proteccion_datos.html en el apartado de Transparencia, Datos Personales.

- Documentar la comunicación realizada del aviso de privacidad a terceras personas a las que se transfieran los datos personales si fuera el caso.

IV.2 Contenido de la Política General de Gestión y Tratamiento de Datos Deberes para la Protección de Datos Personales.

La protección de los datos personales prevé dos deberes, el de confidencialidad y el de seguridad.

La importancia de estos deberes es proteger los datos personales de cualquier amenaza de riesgo con potencial para provocarles un daño o perjuicio, como el robo, extravío o copia no autorizada, pérdida o destrucción no autorizada, uso, acceso, daño, alteración o modificación no autorizada.

Con estos deberes se garantiza la Confidencialidad, Integridad y Disponibilidad, entendiéndose por éstos:

Confidencialidad: Es la obligación de la persona responsable de guardar secrecía de los datos personales, para que no estén a disposición o sean revelados a terceras

Integridad: Es la obligación de la persona responsable de salvaguardar la exactitud y completitud de los datos personales.

Disponibilidad: Es la obligación de la persona responsable de que los datos personales, sean accesibles y utilizables cuando se requiera.

Las personas titulares de las unidades administrativas responsables del tratamiento de datos personales en CMM, con independencia del tipo de soporte en el que se encuentren o el tipo de tratamiento que se realice, deberán establecer las medidas de seguridad de carácter administrativo, físico y técnico para la protección de datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, y así garantizar su confidencialidad, integridad y disponibilidad; por lo tanto deberán observar los deberes de seguridad, contemplados en los artículos 31, 32, 33, 34, 35 y 36 Ley General y artículos 55 al 65 Lineamientos

Generales; y de Confidencialidad dispuesto en los artículos 42 y 71 de la Ley General y Lineamientos Generales, respectivamente.

Deber de Seguridad: Se refiere a la obligación de establecer y mantener medidas de seguridad técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Para cumplir con este deber, las áreas deberán:

1. Establecer y mantener medidas de seguridad administrativas, físicas y técnicas.

2. No adoptar medidas de seguridad menores a aquéllas que mantengan para el manejo de su información.

3. Tomar en cuenta el riesgo inherente por tipo de dato personal; las posibles consecuencias para las personas titulares por una vulneración; la sensibilidad de los datos personales tratados y el desarrollo tecnológico.

4. Notificar a las personas titulares las vulneraciones de seguridad que se presenten, con la información y en el momento antes señalados;

5. Llevar a cabo las acciones correctivas que sean necesarias

Las personas titulares de las unidades administrativas de CMM, adoptarán e instrumentarán las medidas físicas, técnicas y administrativas a través de las cuales garantice la protección de datos personales.

Las obligaciones vinculadas con el cumplimiento del deber de seguridad por parte de las personas titulares de las unidades administrativas que traten datos personales en CMM serán:

- Generar e implementar políticas de gestión, en las cuales se considere el tipo de datos personales recabados, el tratamiento que se les dará y el ciclo de vida, es decir, su obtención, uso y posterior supresión;
- Designar a las personas servidoras públicas que podrán intervenir en el tratamiento de los datos personales y definir las funciones y obligaciones que tendrán;
- Realizar un análisis de riesgo de los datos personales tratados, así como de los sistemas físicos y/o electrónicos en los cuales se desarrolle dicho tratamiento;
- Realizar un análisis de brecha y desarrollar acciones de prevención y mitigación de amenazas o vulneraciones de datos personales;
- Monitorear y revisar las medidas de seguridad adoptadas para garantizar la protección de datos;

- Incentivar la capacitación de las personas servidoras públicas involucradas en el tratamiento de datos personales, conforme al nivel de responsabilidad que tengan asignado.

Para acreditar el cumplimiento de este deber por parte de las personas titulares de las unidades administrativas de CMM, se deberá realizar lo siguiente:

- Contar con un inventario de las bases de datos personales;
- Describir los roles y las responsabilidades específicas de las personas servidoras públicas relacionadas con el tratamiento de datos personales;
- Implementar mecanismos y/o políticas para la protección de datos y guardar evidencia de ello;
- Llevar una bitácora en la cual se asiente cualquier amenaza o vulneración de datos personales suscitada, así como de las acciones realizadas para su mitigación;
- Instrumentar las medidas de seguridad físicas, técnicas y administrativas adoptadas para garantizar el tratamiento de los datos recabados, así como las acciones de monitoreo, análisis y revisión a implementar; a fin de mantenerlas actualizadas y, en su caso, detectar áreas de oportunidad para su desarrollo y ejecución;
- Tener la evidencia documental de los cursos, talleres, seminarios o similares en los que haya participado el personal adscrito a la Unidad Administrativa y se encuentren relacionados con la materia de protección de datos personales.

Deber de Confidencialidad: Las personas titulares de las unidades administrativas de CMM que traten datos personales deberán establecer controles o mecanismos de observancia obligatoria para las personas servidoras públicas que intervengan en cualquier fase del tratamiento, mantengan en secreto la información, así como evitar que los datos personales sean revelados a personas no autorizadas y prevenir la divulgación no autorizada de los mismos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

Por lo anterior, todas las personas servidoras publicas adscritas a CMM que traten datos personales, tendrán la obligación de guardar secreto respecto de los datos personales, para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información y hacer mal uso de esta.

Las obligaciones vinculadas para su cumplimiento por parte de las personas titulares de las unidades administrativas de CMM que traten datos personales son:

- Prever controles mediante los cuales se garantice la confidencialidad de los datos personales que son tratados;
- Establecer cláusulas en los contratos para que los sujetos obligados del ámbito público o privado a los cuales les sean transferidos o remitidos datos personales

se obliguen a la confidencialidad de éstos durante y posterior a la vigencia del instrumento jurídico;

- Implementar campañas de sensibilización para las personas servidoras públicas, sobre la importancia de la confidencialidad de los datos personales;
- Proponer la implementación de mejores prácticas al interior de CMM para garantizar la secrecía de los datos personales.

Para acreditar el cumplimiento a este deber por parte de las personas titulares de las unidades administrativas, se deberá realizar lo siguiente:

- Incluir en el Documento de Seguridad, los controles y las medidas de seguridad implementadas para garantizar la secrecía de los datos personales;
- Generar evidencia de los controles implementados para garantizar la confidencialidad de los datos;
- Tener la evidencia documental de los cursos, talleres, seminarios o similares en los que haya participado el personal adscrito a las unidades administrativas y se encuentren relacionados con la materia de protección de datos personales;
- Documentar la implementación de mejores prácticas que garanticen la confidencialidad de los datos tratados

Las áreas que realizan tratamiento de datos personales deberán:

1. Identificar el flujo y ciclo de vida de los datos personales: medios por los cuales se recaban, en qué procesos se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen.

Ciclo de vida de los datos personales:

OBTENCIÓN: (licitud, información, consentimiento, proporcionalidad, seguridad, confidencialidad)

USO: registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia, disposición. (calidad, finalidad, lealtad, seguridad, confidencialidad)

ELIMINACIÓN: (calidad, seguridad)

2. Elaborar un inventario de datos personales relacionando el tipo de tratamiento con el ciclo de vida.

3. Bloquear, cancelar, suprimir o destruir los datos personales, en los casos establecidos en la normatividad aplicable.

IV.3 Políticas Técnicas Complementarias de Protección de Datos Personales.

Como implementación de las mejoras continuas en esta Entidad, se realizará la implementación periódica en las áreas que manejan datos personales de procedimientos y medidas de seguridad para la protección de los datos personales de manera más específica y técnica. Estas son importantes para operar los sistemas que se manejan en CMM a fin de que contribuyen a mejorar el deber de seguridad de los datos personales ya que son consecuencia de los resultados obtenidos del análisis de riesgo y el análisis de brecha, posteriormente se debe implementar priorizando la atención de los riesgos más graves, y dentro de estas medidas de seguridad se encuentran las administrativas referentes a políticas de seguridad de los datos personales, las cuales son complementarias a la política rectora o general de gestión y tratamiento de datos personales.

En el caso de CMM, las medidas complementarias que se están integrando y que estarán realizando, todas y cada una de las áreas administrativas en el tratamiento y sistemas de datos personales, son las siguientes:

Documentos para la Protección de Datos Personales

Para la Protección de Datos Personales, Casa de Moneda de México, contará con los siguientes documentos:

Documento de Seguridad: Documento elaborado con información provista por cada una de las unidades administrativas de CMM, cuyo propósito es establecer las medidas administrativas, físicas y técnicas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Programa de Protección de Datos Personales: Documento de planeación que tiene por objeto establecer elementos y actividades de dirección, operación y control de los procesos de CMM para proteger de manera sistemática y continúa los datos personales en posesión de ésta.

Aviso de Privacidad: Documento generado por las unidades administrativas de CMM que realicen cualquier tipo de tratamiento de datos personales, para dar a conocer a las personas titulares los mismos y las finalidades de su tratamiento.

Programa de Capacitación: Documento en el cual se prevén actividades de capacitación y actualización para todas las personas servidoras públicas adscritas a CMM, considerando sus roles y responsabilidades asignadas para el tratamiento de datos personales.

La Casa de Moneda de México deberá contar con los documentos para la protección de datos correspondientes, como parte de los mecanismos implementados para asegurar el cumplimiento del deber de seguridad, cuyo objeto es describir y dar cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas, para la

protección de datos personales que permitan protegerlos contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Actualizaciones al Documento de Seguridad de CMM

En las actualizaciones que se realicen al Documento de Seguridad deberán participar las personas titulares de las unidades administrativas, a través de sus enlaces en materia de datos personales, quienes en todo momento observarán los principios, deberes y obligaciones a los que se refieren la Ley General, los Lineamientos Generales, la presente Política y demás normativa aplicable.

De conformidad con lo dispuesto en la Ley General, el Documento de Seguridad se actualizará en los supuestos siguientes:

- Se produzcan modificaciones sustanciales al tratamiento de los datos personales que deriven en un cambio de nivel de riesgo;
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión con el que se cuente;
- Derivado de un proceso de mejora para mitigar el impacto de vulneración a la seguridad ocurrida;
- Con motivo de la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Con independencia de los supuestos anteriores, el Documento de Seguridad de CMM podrá ser actualizado cada tres años o en el momento que alguna de las áreas administrativas que conforman esta entidad y que tienen tratamiento de datos personales ingrese nuevos activos a los sistemas de datos personales que realizan.

Cuando alguna de las personas titulares de las unidades administrativas de CMM se encuentre en algunos de los supuestos del artículo anterior, la persona enlace presentará por escrito a la Unidad de Transparencia de esta Entidad las actualizaciones conducentes, quien lo someterá al Comité de Transparencia para resolver lo conducente.

En términos de lo previsto en la Ley General, se considera como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

1. La pérdida o destrucción no autorizada;
2. El robo, extravío o copia no autorizada;
3. El uso, acceso o tratamiento no autorizado;

4. El daño, la alteración o modificación no autorizada.

Derivado de lo anterior, como medida de mejora continua, el personal titular de las unidades administrativas responsables del tratamiento de datos personales en CMM deberán llevar una bitácora de las vulneraciones a la seguridad en las que se describa ésta, la fecha en la que ocurrió, el motivo y las acciones correctivas implementadas de forma inmediata y definitiva, mediante el formato de bitácora de vulneraciones y se tomaran las medidas correspondientes de acuerdo a la normatividad jurídica aplicable para evaluar la vulneración.

Informe de vulneración

Cuando las vulneraciones afecten de forma significativa los derechos patrimoniales o morales de las personas titulares de los datos personales, las personas titulares de las unidades administrativas involucradas, deberán generar un informe detallado que contenga al menos lo siguiente:

1. La hora y fecha de la identificación de la vulneración;
2. La hora y fecha del inicio de la investigación sobre la vulneración;
3. La naturaleza del incidente o vulneración ocurrida;
4. La descripción detallada de las circunstancias en torno a la vulneración ocurrida;
5. Las categorías y número aproximado de personas titulares afectadas;
6. Los sistemas de tratamiento y datos personales comprometidos;
7. Las acciones correctivas realizadas de forma inmediata;
8. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;
9. Las recomendaciones dirigidas a las personas titulares;
10. El medio puesto a disposición las personas titulares para que pueda obtener más información sobre la vulneración y cómo proteger sus datos personales;
11. El nombre completo de la o las personas designadas para proporcionar más información, en caso de requerirse;
12. Cualquier otra información y documentación que considere conveniente hacer del conocimiento de la Unidad de Transparencia y demás instancias necesarias.

Para efectos del presente numeral, se entenderá que se afectan los derechos patrimoniales de las personas titulares, cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus bienes, información fiscal, historial crediticio, ingresos o egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados u otros similares.

De la misma manera, se entenderá que se afectan los derechos morales de la persona titular, cuando la vulneración esté relacionada de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, aspecto físico o menoscabe ilegalmente la libertad, integridad física o psíquica de la persona titular de los datos.

Las personas titulares de las unidades administrativas tendrán la obligación de notificar a la(s) persona(s) titular(es) afectada(s) la información descrita en lo incisos anteriores, a través del medio que se establezca para ese fin, marcando copia de conocimiento a la Unidad de Transparencia de CMM.

En aquellos casos en los cuales no sea posible notificar directamente a la(s) personas (s) titular(es) afectada(s) sobre el informe a que hace referencia la presente Política o ello implique esfuerzos desproporcionados, se instrumentarán medidas compensatorias de comunicación para tal efecto, como son: la publicación en sitios de internet, aviso en la página web oficial de CMM, plataformas, tarjetas o cápsulas informativas o cualquier otro similar.

Con independencia de lo anterior, la persona titular de la unidad administrativa, deberá sujetarse a lo señalado en el artículo 37 de la Ley General, que establece que, en caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

El informe de vulneración se deberá remitir a la Unidad de Transparencia (UT) en un plazo no mayor de 48 (cuarenta y ocho horas) hábiles posteriores a que se haya confirmado la vulneración de seguridad, para que ésta la haga del conocimiento al Órgano Garante en tiempo y forma, de conformidad con la Ley General, los Lineamientos Generales y demás normativa aplicable.

En términos de lo previsto en el numeral anterior, la (UT) deberá informar al Comité de Transparencia de lo ocurrido en torno a la vulneración de seguridad de datos personales. El Comité de Transparencia podrá determinar la implementación de acciones adicionales a las realizadas por las personas titulares de las unidades administrativas de CMM para evitar futuras vulneraciones y reforzar las medidas de seguridad existentes.

El Comité de Transparencia podrá auxiliarse de la asesoría, orientación o apoyo de las personas titulares de las unidades administrativas, en asuntos de su especialidad, con la finalidad de garantizar la efectiva protección de los datos personales.

Para llevar a cabo lo anterior, el Comité de Transparencia se apoyará de la Unidad de Transparencia para realizar dichas gestiones ante las personas titulares de las unidades de administrativas.

Casa de Moneda de México deberá contar con un Programa de Protección de Datos Personales aprobado por el Comité de Transparencia, cuyo objetivo serán los siguientes:

1. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión de CMM;
2. Cumplir con los principios, deberes y obligaciones de la Ley General, la presente Política y la normatividad que derive de los mismos;

3. Establecer los elementos y las actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua;
4. Promover la adopción de mejores prácticas en la protección de datos personales.

El Programa de Protección de Datos Personales deberá estar actualizado, sin demerito de que podrá ser sometido a su revisión o reajuste por parte del Comité de Transparencia, de conformidad con las facultades y atribuciones que le establece la normativa aplicable, en caso de estimarse necesario.

La Unidad de Transparencia de esta Entidad tendrá las siguientes funciones en relación con el Programa de Protección de Datos Personales:

1. Elaborar y coordinar el Programa en conjunto con las Unidades Administrativas que estime necesario involucrar o consultar;
2. Proponer cambios y mejoras al Programa, a partir de la experiencia de su implementación;
3. Dar a conocer el Programa al interior del sujeto obligado;
4. Coordinar la implementación del Programa en las Unidades Administrativas;
5. Asesorar a las Unidades Administrativas en la implementación del Programa, con el apoyo de las áreas técnicas que estime pertinente;
6. Las demás que de manera expresa señalen el propio Programa.

Como parte de las acciones para cumplir con el principio de información, en CMM se contará con los avisos de privacidad integral y su correlativo aviso de privacidad simplificado, para el tratamiento de datos personales.

Excepcionalmente, cuando dos o más tratamientos de datos personales, atiendan una misma finalidad o función, se podrá contar con un mismo aviso de privacidad, en sus dos modalidades, siempre y cuando sea posible expresar con precisión y claridad las finalidades del tratamiento de datos personales, de tal suerte que no dé lugar a incertidumbre o ambigüedad a sus titulares.

Los formatos para la elaboración de los avisos de privacidad integral y simplificado serán acordes con los elementos que establecen en la Ley General, los Lineamientos Generales y demás normatividad que resulte aplicable.

En la integración y elaboración de los avisos de privacidad, las unidades administrativas preverán un diseño que facilite su entendimiento por parte de las y los titulares
datos. La UT podrá elaborar propuestas de formatos que faciliten su integración o actualización, manteniendo la homogeneidad de los elementos.

En todo momento, las personas titulares de las unidades administrativas deberán asegurarse que los avisos de privacidad se encuentren actualizados.

Las personas titulares de las unidades administrativas se asegurarán de que la información asentada en los avisos de privacidad se encuentre redactada en un lenguaje ciudadano, sencillo, claro y comprensible, considerando en todo momento el perfil de la o el titular al cual vaya dirigido, por lo que se abstendrán de:

1. Usar frases inexactas, ambiguas o vagas;
2. Incluir textos que induzcan a las personas titulares a elegir una opción en específico;
3. Marcar previamente casillas, en caso de que éstas se incluyan, para que las personas titulares otorguen su consentimiento, o bien, incluir declaraciones orientadas a afirmar que las personas titulares ha consentido el tratamiento de sus datos personales sin manifestación alguna de su parte;
4. Remitir a textos o documentos que no estén disponibles para las personas titulares.

CMM contará con un Programa de Capacitación y Actualización en materia de Protección de Datos Personales, como uno de los mecanismos a través de los cuales se cumple con el principio de responsabilidad, el cual considerará los niveles de capacitación atendiendo los roles y las responsabilidades de las personas servidoras públicas que tratan datos personales.

El Comité de Transparencia será el órgano encargado de aprobar el Programa de Capacitación y Actualización en la materia, con base en la propuesta que sea presentada por el enlace de capacitación de CMM en la cual se consideren las necesidades de capacitación de las Unidades Administrativas.

La Unidad de Transparencia coordinará y dará seguimiento a los programas de capacitación continua y especializada en la materia de protección de datos personales a través del enlace de capacitación de CMM

Ejercicio de los Derechos ARCO y la Portabilidad de los Datos Personales

Para efectos de la presente Política, los Derechos ARCOP son aquellos derechos que tiene las personas titulares de los datos personales, para solicitar el Acceso, Rectificación, Cancelación, Oposición y Portabilidad sobre el tratamiento de sus datos personales.

Acceso: Derecho de la persona titular para acceder a sus datos personales y conocer la información relacionada con las condiciones y generalidades del tratamiento.

Rectificación: Derecho de la persona titular para solicitar la corrección de sus datos personales, cuando éstos resulten inexactos, incompletos o no se encuentren actualizados.

Cancelación: Derecho de la persona titular para solicitar que sus datos personales sean bloqueados y ulteriormente suprimidos de los archivos, registros, expedientes y sistemas.

Oposición: Derecho de la persona titular para solicitar que se abstengan de solicitar información personal para ciertos fines o de requerir que se concluya el uso a fin de evitar un daño.

Portabilidad: Prerrogativa de las personas titulares de datos personales que les permite, bajo las condiciones establecidas en la normatividad aplicable, recibir los datos personales que han proporcionado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable del tratamiento sin impedimentos.

La Unidad de Transparencia de CMM será la responsable de turnar las solicitudes de ejercicio de derechos ARCOP que sean presentadas, a aquellas unidades administrativas que conforme a sus atribuciones, competencias o funciones puedan o deban poseer los datos personales, para que se pronuncien y den atención en los plazos y términos establecidos para la atención de solicitudes de acceso a la información y de solicitudes para el ejercicio de los Derechos ARCOP.

Cuando los datos personales se encuentren en un formato estructurado y comúnmente utilizado podrá proceder la portabilidad de los datos personales.

La Portabilidad de los datos personales, tiene por objeto que persona titular solicite, lo siguiente:

- Una copia de sus datos personales que hubiere facilitado directamente a CMM una Unidad Administrativa, en un formato estructurado comúnmente utilizado, que le permita seguir utilizándolos y, en su caso, entregarlos a otro sujeto obligado para su reutilización y aprovechamiento en un nuevo tratamiento;
- La transmisión de sus datos personales a un sujeto obligado receptor, siempre y cuando sea técnicamente posible, que la persona titular hubiere facilitado directamente sus datos personales a CMM y el tratamiento de éstos se base en su consentimiento o en la suscripción de un contrato.

Remisión y transferencias de los Datos Personales

Se le conoce como remisión, a toda comunicación de datos personales realizada por la persona titular de la unidad administrativa y la o el encargado dentro y fuera del territorio mexicano.

La figura de la persona encargada, es una persona prestadora de servicios que trata datos personales a nombre de la persona titular de la unidad administrativa responsable de los datos personales y tiene las siguientes características: puede ser una persona física o

jurídica, de ámbito público o privado, ajeno a CMM, puede ser una sola persona o de manera conjunta con otras personas, no tiene poder de decisión sobre el alcance y contenido del tratamiento de los datos personales y debe delimitar sus actuaciones a lo que diga la persona titular de la unidad administrativa responsable de los datos personales.

La transferencia es toda comunicación de datos personales, dentro o fuera del territorio nacional, a persona distinta de la o el titular, de la persona titular de la unidad administrativa o la o el encargado.

Toda transferencia de datos personales se encontrará sujeta al consentimiento de la persona titular. Para tal efecto, a través del aviso de privacidad correspondiente informarán a la persona titular de los datos personales, las finalidades de la transferencia, así como el tercero receptor.

No se requerirá el consentimiento de la persona titular para llevar a cabo la transferencia de sus datos personales, en los casos previstos en los artículos 22, 66 y 70 de la Ley General.

Políticas para las mejoras Administrativas:

Protocolo para la implementación de confidencialidad, por parte del personal de CMM, que maneja o resguarda datos personales en cualquiera de sus ciclos de vida.

Política de Clasificación de los archivos físicos: Identificar, valorar y, en su caso, incluir en el Catálogo de Disposición Documental los expedientes de archivo que incorporan documentos que reflejan tratamientos de datos personales, con la finalidad de generar certeza sobre el ciclo de vida a que deben estar sujetos.

Política de clasificación de los archivos electrónicos: En cuanto a las bases con las que se cuenta en CMM en (soporte electrónico) relacionadas con tratamientos de datos personales.

Política de Capacitación: Programa de Capacitación de cursos que impartan para el tratamiento, calificación de datos personales.

Política de Bitácora de vulneraciones: Implementación de documentos que permita tener el control si se materializa una vulneración en los sistemas con los que cuenta la CMM.

Política de responsable de seguridad: Que se implemente para el mejor control de las medidas de seguridad que se manejan en los sistemas de datos personales de la CMM.

Políticas de mejoras físicas: Cuidado de los bienes informáticos: Implementación de rol para que se verifique el estado que guardan de manera cotidiana los equipos que almacenan los datos personales, en la CMM

Protocolo de zona de confidencialidad: Controles de accesos en la CMM.

políticas de mejoras técnicas:

Políticas de cuidado de la contraseña personal: Protocolo de revisión periódica de estas para el acceso a los datos personales, del personal de la CMM.

Fallas en los equipos: Protocolo de revisión periódica de los equipos que almacenan datos personales, del personal de la CMM.

No instalar softwares: Protocolo periódico de vigilancia de estos elementos dentro de los equipos que almacén datos personales en la CMM.

V. Roles y Responsabilidad de los encargados de Redactar las políticas.

Con relación a lo dispuesto en el artículo 33, fracción II de la LGPDPPSO, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.

En el caso del personal de Casa de Moneda de México las funciones y obligaciones de las personas que tratan datos personales se han identificado en dos niveles:

I. A nivel estructura, a través del Programa de Protección de Datos Personales de esta Entidad, en el cual se describen todas las obligaciones que establece la Ley General y los Lineamientos Generales y su asociación con el área responsable de su cumplimiento,

II. A nivel de servidor público, a través de los inventarios que se desarrollaron por cada uno de los tratamientos, en los cuales se identificó el personal que realiza el tratamiento, el área al que está adscrito y la finalidad de dicho tratamiento.

En el Documento de Seguridad de la CMM se tiene acceso a los roles y responsabilidades de las personas que realizan tratamientos de datos personales y las obligaciones inherentes a dicho tratamiento.

VI. Sanciones

Serán causas de sanción por incumplimiento a las obligaciones en materia de protección de datos personales, las establecidas en el artículo 163 de la LGPDPPSO:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;

II. Incumplir los plazos de atención para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGPDPPSO;

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la LGPDPPSO; y, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;

VII. Incumplir el deber de confidencialidad;

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad;

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;

XI. Obstruir los actos de verificación de la autoridad;

XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO;

XIII. No acatar las resoluciones emitidas por el Instituto y los Organismos garantes; y

XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea;

VII. Revisión, Evaluación y Mejora de las Políticas de Gestión y Tratamiento

Revisión de las medidas de seguridad: El artículo 33, fracción VII de la LGPDPPSO establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

De acuerdo con la fracción VI del artículo 35 de la LGPDPPSO, los mecanismos de monitoreo y revisión forman parte del documento de seguridad. Así, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

Monitoreo y supervisión periódica de las medidas de seguridad implementadas: Artículo 63. Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:

I. Los nuevos activos que se incluyan en la gestión de riesgos;

II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;

III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;

IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;

V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y

VII. Los incidentes y vulneraciones de seguridad ocurridas.

Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

De lo anterior es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer, a través de un ciclo de mejora continua, la protección de los datos personales que resguarda este Instituto.

A continuación, se desarrollan las acciones de monitoreo y supervisión periódica para las medidas de seguridad de la CMM:

Mecanismos de Monitoreo

1) Revisión de cumplimiento de las políticas internas de la CMM, relacionadas con el tratamiento de datos personales. Tiene el objetivo de asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en concordancia con lo dispuesto en la LGPDPPSO, los Lineamientos Generales, y demás normatividad que resulte aplicable.

Para ello, cuando se identifica algún cambio en los instrumentos antes mencionados, se deberán realizar las siguientes actividades:

a) Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.

b) Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.

c) Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.

d) Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

2) Revisión del riesgo. Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ello, se implementarán los siguientes monitoreos:

a) Monitoreo del entorno físico. Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con:

- Personal de vigilancia en los accesos al edificio de la CMM
- Control de acceso a través de bitácoras para visitantes y personal de la CMM, que olvidó su credencial.
- Circuito cerrado de cámaras de vigilancia en el corporativo y planta de San Luis de la CMM.

b) Monitoreo del entorno electrónico. Para la detección continua de amenazas y vulnerabilidades.

c) Actualización del plan de trabajo. Derivado del monitoreo del entorno físico o electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos

identificados. Estos cambios se pondrán a consideración del área que apoya en el análisis de riesgos.

d) Revisión de avances del plan de trabajo. A través de los mecanismos que determine el área que apoya en el análisis de riesgos y la Unidad de Transparencia, se hará una revisión de los avances en el plan de trabajo, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo el plan de trabajo, para hacer los ajustes correspondientes al mismo.

e) Vulneraciones a la seguridad de los datos personales. En caso de identificar un incidente de seguridad que involucre datos personales, el área que apoya en el análisis de riesgos y la Unidad de Transparencia se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente.

El presente documento, fue aprobado por unanimidad de votos de los integrantes del Comité de Transparencia de la Casa de Moneda de México, en su Segunda Sesión Ordinaria celebrada el 15 de mayo de 2024.