PROGRAMA DE PROTECCION DE DATOS PERSONALES DE CASA DE MONEDA DE MÉXICO.

Índice.

Presentación.

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.

Marco Jurídico.

1.- Constitución Política de los Estados Unidos Mexicanos.

2.- Ley Orgánica de la Administración Pública Federal.

3.- Ley General de Archivos.

4.- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

5.- Ley General de Transparencia y Acceso a la Información Pública.

6.- Ley Federal de Transparencia y Acceso a la Información Pública.

7.- Ley de la Casa de Moneda de México.

8.- Estatuto Orgánico de Casa de moneda de México.

9.- Manual de Organización de Casa de Moneda de México.

10.- Lineamientos Generales de Protección de Datos Personales Para el Sector Público.

11.- Acuerdo Mediante el cual se aprueba la adición de un título décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

12.- Guía para cumplir con los principios y deberes de la Ley General de Protección de datos Personales en Posesión de Sujetos Obligados.

Glosario.

Auditoría voluntaria: Proceso sistemático, independiente y documentado mediante el cual el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales obtiene evidencias que le permiten evaluar el grado de cumplimiento en la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en las Leyes y demás normativa que resulte aplicable.

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

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 de la 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.

I. Objetivo General.

Es menester precisas que en cumplimiento de la normatividad jurídica aplicable y como política Interna de esta entidad, para el cumplimiento del Tratamiento de Datos Personales en Posesión de la Casa de Moneda de México y la aplicación de los principios, deberes y obligaciones en materia de protección de datos personales, se debe establecer mejores prácticas y estándares, así como elementos y actividades de dirección, operación, control en los procesos ejercicio de sus funciones en el tratamiento de datos personales.

I.1 Objetivos específicos del Programa

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. Disposiciones Generales y Responsabilidades dentro del Programa

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; 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.

III. 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.

III.1 Listado de unidades administrativas que deben dar cumplimiento al presente programa, considerando la estructura orgánica con la que cuenta Casa de La Moneda de México.

1.- Dirección General

A) Dirección Corporativa de Comercialización.

Gerencia de Ventas Directas

B) Dirección Corporativa de Administración y Finanzas.

Subdirección Corporativa de Recursos Humanos

Gerencia de Personal

Subdirección Corporativa de Recursos Materiales

Gerencia de Adquisiciones y Obra Pública

C) Dirección Corporativa Jurídica y de Seguridad

Subdirección Corporativa Jurídica y de Seguridad
(Unidad de Transparencia)

IV. Política de Gestión de los 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 representar 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 éstos

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.

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.

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.

Es menester precisa que las personas servidoras públicas de Casa de Moneda de México 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.

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 correspondientes 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.

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.

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.

IV.1 Inventario del Tratamiento.

Unidad administrativa	Asentar nombre de la unidad administrativa a cargo o administradora del Sistema, tratamiento o proceso o procedimiento en el que se tratan los datos personales.
Fecha de elaboración o última actualización	Consignar fecha en que concluyó la elaboración del inventario o su última actualización
Nombre del tratamiento (proceso)	Especificar nombre del Sistema, tratamiento, proceso o procedimiento en el que se tratan los datos personales. (Como se tiene registrado el archivo o base de datos).
Fundamento jurídico que habilita el tratamiento	
Atribuciones de la unidad administrativa para realizar el tratamiento	Incluir las atribuciones específicas de la unidad administrativa para llevar a cabo el tratamiento.

PARTE 1 – MEDIOS DE OBTENCIÓN

<table>
<tr><th colspan="11">Medio de obtención de los datos personales

(1)</th></tr>
<tr><td colspan="2">Informar el o los medios a través de los cuales se obtienen los datos personales en este tratamiento. En caso de ser Si es más de un medio, deberá indicarse un medio por fila.

• Marcar con una x el(los) medios, puede ser uno o más.</td><td colspan="3">Tercero que transfiere los datos personales a la Entidad.

En su Caso, (2) *se deberá poner una x en la opción aplicable.</td><td colspan="6">Finalidades de la transferencia recibida, en su caso

(3)</td></tr>
<tr><td>1.</td><td>Directamente del Titular</td><td>x</td><td>Aplica</td><td>x</td><td>No aplica</td><td></td><td>Aplica</td><td></td><td>No aplica</td><td>x</td></tr>
<tr><td>2.</td><td>Modo Personal</td><td></td><td colspan="7" rowspan="8"></td></tr>
<tr><td>3.</td><td>Presencia física del titular de los datos personales</td><td></td></tr>
<tr><td>4.</td><td>Vía telefónica</td><td></td></tr>
<tr><td>5.</td><td>Internet o Medios informáticos</td><td></td></tr>
<tr><td>6.</td><td>Por escrito en las oficinas del sujeto obligado</td><td></td></tr>
<tr><td>7.</td><td>Por mensajería</td><td></td></tr>
<tr><td>8.</td><td>Otro: se debe especificar cual otro medio</td><td></td></tr>
<tr><td colspan="3">* Describir el medio:

Por ejemplo, la fuente de acceso público, URL, domicilio, número telefónico, entre otros.</td></tr>
</table>

PARTE 2 – TIPOS DE DATOS

<table>
<tr><th colspan="2">Listado de datos personales (4)</th><th colspan="4">Sensible (5) (aplica o no aplica)
* Poner una x en el supuesto.</th></tr>
<tr><td colspan="2">Señalar cada uno de los datos personales que se tratan, o sus categorías, uno por fila</td><td>SI</td><td>X</td><td>NO</td><td></td></tr>
<tr><td>Datos Personales</td><td>Datos Personales Sensibles (indicar con una X)</td><td colspan="4" rowspan="8"></td></tr>
<tr><td></td><td>Aplica | No aplica</td></tr>
<tr><td>1. Datos de identificación:</td><td>1. De salud</td></tr>
<tr><td>2. Datos Laborales</td><td>2. Ideológicos</td></tr>
<tr><td>3. Datos Patrimoniales</td><td>3. Vida Sexual</td></tr>
<tr><td>4. Datos de personas que intervienen en procedimientos administrativos convocados por la Entidad</td><td>4. De origen</td></tr>
<tr><td>5. Datos académicos</td><td>5. Biométricos</td></tr>
<tr><td>6. Datos de movimientos migratorios</td><td>6. Electrónicos</td></tr>
<tr><td>7. Otro</td><td>7. Otro</td></tr>
</table>

PARTE 3 – FORMATO Y UBICACIÓN DE LOS DATOS

Formato de la base de datos (6)	**Ubicación base de datos (7)**	**Sección de archivos (8)**	**Serie de archivos (9)**	**Subserie de archivos (10)**
Consignar el o los formatos en los que se encuentra la base de datos del tratamiento. (señalar con una X)	Informar la ubicación del sistema o base de datos. (Si es más de uno, se deberá indicar uno por fila.)	Indicar clave de identificación de la **sección** a la que corresponde el tratamiento.	Asentar clave de identificación de la **serie** a la que corresponde el tratamiento.	Detallar clave de identificación de la **subserie** a la que corresponde el tratamiento

PARTE 4 – FINALIDADES DE TRATAMIENTO

Finalidades del tratamiento (11)	**¿Requiere consentimiento? (12) (aplica o no aplica)** *(si requiere consentimiento, señalar con una X)	**Supuesto del artículo 22 LGPDPPSO que se actualiza, en su caso (13)** **Art. 22 LGPDPPSO Frac. _____**	**Tipo de consentimiento (14)** ***Señalar con una x en el supuesto de aplicar o no aplicar**

PARTE 5 – SERVIDORES PÚBLICOS CON ACCESO A LOS DATOS

Servidores públicos que tienen acceso a la base de datos (15)	Área de adscripción (16)	Finalidad del acceso (17)
Asentar **los puestos o cargos de los servidores públicos** que tienen acceso al sistema o base		Especificar con qué fines tienen acceso los servidores públicos antes identificados. Uno por fila, según

de datos del tratamiento correspondiente. Uno por fila. *** Listado de servidores públicos y área de adscripción. (**ejem. Dirección Corporativa de Administración y Finanzas, etc. Subdirector Corporativo de Recursos Humanos; subdirector Corporativo de Recursos Materiales, Gerente de Personal, jefe de Proyecto, Analista, etc.)	Definir unidad administrativa a la que está adscrito el puesto.	corresponda. **(incluya una X en el supuesto de que se trate))** Acceso o privilegios de los servidores públicos a los datos: acceso de consulta, modificación de los datos, generar copias de los datos, eliminar o actualizar cualquier dato. *** Señalar en cada actividad el área o cargo que la realiza, en los casos que aplique (ejem. Dir. Corp. de Admón. consulta los datos).**	
1.		1. Acceso a los datos	
2.		2. Consulta de los datos	
3.		3. Modificación de los archivos, bases en donde se encuentran los datos	
4.		4. Generar copias de los archivos o bases donde se almacenan los datos.	
5.		5. Bloquea y/o elimina los datos de los archivos o bases donde están almacenados.	
6.		6. Actualizar los datos de los archivos o bases donde están almacenados los datos.	

PARTE 6 – ENCARGADO (Casa de Moneda de México, no tiene contratado encargado de datos personales, por lo que NO APLICA esta sección.)

Nombre del encargado, en su caso (18) (aplica o no aplica)				No. de contrato, pedido o convenio con el encargado o del instrumento jurídico correspondiente (19)
aplica		**No aplica**	**x**	

PARTE 7 – TRANSFERENCIAS DE DATOS

¿Se realizan Transferencias? (20)		Tercero al que se transfie-ren los datos personales, en su caso (21)	Finalidades de la transferencia (22)		¿Requiere consentimiento de la transferencia? (23) (aplica o no)		Supuestos artículos 22, 66 ó 70 que se actualizan, en su caso (24) (especificar el articulo y la fracción)		Tipo de consentimiento que se requiere para la transferencia (25)		¿La transferencia requiere la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico? (26)		Supuesto artículo 66 que se actualiza, en su caso (27) *** Si se elige no aplica elegir la fracción del artículo 66 de la LGPDPPSO**	
aplica	**No aplica**	***si se elige en casilla 20 aplica.**	**aplica**	**No aplica**	**aplica**	**No aplica**	**aplica**	**No aplica**	**aplica**	**No aplica**	**aplica**	**No aplica**	**aplica**	**No aplica**

PARTE 8 – DIFUSIÓN DE LOS DATOS

Difusión de los datos personales (28)					**Fundamento jurídico para la difusión (29)**			
Precisar si en el tratamiento se realiza la difusión de los datos personales**. * Solo en caso de elegir que este supuesto aplica.**					Asentar el fundamento jurídico que ordena la difusión de los datos personales. *** Solo en caso de elegir que este supuesto aplica.**			
aplica		**No aplica**	**x**		**aplica**		**No aplica**	**x**

PARTE 9 – PLAZO DE CONSERVACIÓN Y BLOQUEO

Plazo de conservación (30)	**Bloqueo (31)**	**Observaciones**
Informar el plazo de conservación de los datos personales, según lo	Detallar período en el que estarán	Espacio libre para hacer aclaraciones y precisiones. (si se considera

señalado en los instrumentos de clasificación archivística.	bloqueados los datos personales.	pertinente, de lo contrario, dejar en blanco)

IV.2 Cumplimiento de las obligaciones: Como se ha mencionado, las áreas de esta Entidad, que realicen el tratamiento de datos personales deberán cumplir con los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales; así como con los deberes y obligaciones que prevé la LGPDPPSO, para lo cual este Programa establece el marco de trabajo mínimo que se deberá seguir para alcanzar dicho objetivo. Para ello, se identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las áreas competentes, de acuerdo con lo que establece la LGPDPPSO y los Lineamientos Generales en concordancia con el 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.

- Eliminación: (calidad, seguridad).

Derivado de lo anterior, para cumplir con las obligaciones para el cumplimiento de los principios de 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.

Derivado de lo anterior, las obligaciones para el cumplimiento de los Principios, por parte de la Unidad de Transparencia son:

- 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 recopilen los datos personales que traten, así como los insumos necesarios para que las áreas correspondientes, elaboren el 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 de los Principios 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.

IV.3 Obligaciones Trasversales

Es importante precisar que para el cumplimiento de las obligaciones en materia de 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 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.

IV.4 Obligaciones Relevantes para la obtención de Datos Personales.

La protección de los datos personales prevé tres 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

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;
- En su caso, contar con los contratos en los cuales se establezcan las cláusulas de confidencialidad de datos, respecto de transferencias o remisiones;
- 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.

IV.5 Obligaciones relevantes en la etapa de USO de los datos personales

IV.5.1 Aviso de Privacidad.

De conformidad con los artículos 3, fracción II, 18, 26 y 27 de la LGPDPPSO, 26, 27 y 28 de los Lineamientos Generales; cada sistema de tratamiento de datos personales de la Entidad debe contar con un aviso de privacidad integral y simplificado.

Estos avisos deben hacerse del conocimiento de las personas titulares de los datos personales de forma previa a recabar los datos, por lo que las áreas competentes deben contar con ejemplares impresos, con independencia de que en el portal de internet de la CCM se encuentren disponibles para garantizar que cualquier persona pueda consultarlos.

Los avisos de privacidad integrales deberán contar, cuando menos, con los elementos siguientes:

1. El domicilio del responsable.

2. Los datos personales que serán sometidos a tratamiento, identificando aquellos que son sensibles.

3. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento.

4. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieren el consentimiento de la persona titular.

5. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO.

6. El domicilio de la Unidad de Transparencia; y

7. Los medios a través de los cuales el responsable comunicará a las personas titulares de los cambios al aviso de privacidad.

Los avisos de privacidad simplificados deberán contar con, al menos, los elementos siguientes:

1. La denominación del responsable.

2. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquellas que requieran el consentimiento de la persona titular.

3. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar.

4. Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales.

5. Las finalidades de estas transferencias.

6. Los mecanismos y medios disponibles para que la persona titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular; y

7. El sitio donde se podrá consultar el aviso de privacidad integral.

Así mismo el personal de las áreas administrativas que integran esta Entidad deberán 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;

- Incluir en el inventario contenido en el aviso de privacidad los lugares y medios en los que se difunden y colocan los avisos de privacidad;

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

VI.5.2 Documento de Seguridad

En cumplimiento de las obligaciones de seguridad, el Comité de Transparencia deberá aprobar el Documento de Seguridad de Casa de Moneda de México; el cual, en cumplimiento al artículo 35 de la LGPDPPSO, contiene los apartados y anexos siguientes:

I. Objetivo.

II. II. Marco normativo.

III. Glosario.

IV. Inventarios de datos personales y de los sistemas de tratamiento.

V. Funciones y obligaciones del personal que trate datos personales.

VI. Análisis de riesgo.

VII. Análisis de brecha.

VIII. Programa general de capacitación

IX. Actualización del documento de seguridad

X. Anexo

IV.5.3 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 la persona titular para acceder a sus datos personales y conocer la información relacionada con las condiciones y generalidades del tratamiento.

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

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

Oposición: Derecho 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 transmitir los 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.

V. Revisión y Auditoria

Para el debido cumplimiento de los principios, deberes y obligaciones que establecen la Ley General, los Lineamientos Generales y la normativa aplicable en materia de protección de datos personales, el Comité de Transparencia a través de la UT supervisará a las unidades administrativas para garantizar el derecho a la protección de datos personales en CMM de conformidad con lo dispuesto en el artículo 30 fracción V de la Ley General.

La supervisión en materia de protección de datos personales se sustanciará mediante requerimientos de información sobre el tratamiento de datos personales, así como de sugerencias a las unidades administrativas para prevenir algún incumplimiento a las disposiciones en materia de protección de datos personales y realizando auditorias para verificar los procedimientos, tratamientos y medidas de seguridad que se realizan para el tratamiento los sistemas de datos personales de esta Entidad.

De conformidad a la normatividad jurídica aplicable la auditoria en materia de datos personales tiene las siguientes etapas.

La etapa de apertura tendrá la finalidad de definir el personal de la instancia auditada ante el cual la Unidad de Transparencia substanciará la auditoría, así como los tratamientos de datos personales que serán auditados, el tipo de revisión que ameritará (documental, presencial o virtual), y los requerimientos específicos necesarios para su realización.

En la **etapa de revisión** se realizará el escrutinio de la forma en que la instancia acredite el cumplimiento de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como los deberes de seguridad y confidencialidad, de conformidad con lo previsto en la normativa aplicable, así como en el Programa de Protección de Datos Personales y el Documento de Seguridad.

En la **etapa conclusiva,** la Unidad de Transparencia puntualizará a la instancia auditada las consideraciones efectuadas, abundará en los puntos de mejora y las cuestiones que se estimen de atención prioritaria y señalará la forma en que las observaciones y requerimientos deberán ser cumplimentados, destacando el plazo en que las instancias deberán remitir las evidencias correspondientes.

Etapa de apertura

Notificación de auditoría: De conformidad con el calendario de auditorías en materia de datos personales, la Unidad de Transparencia comunicará a la instancia correspondiente, lo siguiente:

I. La fecha en que dará inicio la auditoría, la cual deberá realizarse con un mínimo de 5 días hábiles entre la notificación del oficio y su celebración.

II. La necesidad de que la instancia auditada designe al personal con el que la Unidad de Transparencia substanciará la auditoría.

III. La convocatoria a una reunión previa al inicio de la auditoría, entre el personal de la Unidad de Transparencia y el personal designado por la instancia auditada.

Reunión previa

En el día señalado para la reunión previa, se informarán los tratamientos de datos personales que serán auditados, el tipo de revisión que ameritará (documental, presencial, virtual o mixta), así como los requerimientos específicos necesarios para la realización de la propia auditoría.

Efectuada la reunión previa, la referida Unidad de Transparencia elaborará una minuta en la que se precisará el desarrollo de la propia reunión, la cual deberá ser signada por los involucrados.

Acuerdo de inicio

En el día estipulado para el comienzo de la auditoría, la Unidad de Transparencia emitirá un acuerdo de inicio en el que deberá asentar lo siguiente:

I. El día en que comenzará y finalizará la auditoría.

II. El servidor público designado por la Unidad de Transparencia para sustanciar la auditoría.

III. El servidor público designado por la instancia auditada para sustanciar la auditoría.

IV. Identificación del tratamiento o tratamientos de datos personales materia de la auditoría.

V. El tipo de revisión que amerite el tratamiento (documental, presencial, virtual o mixta).

VI. La documentación, sistema o espacio físico que deberá estar plenamente disponible para ser examinado.

VII. Los datos de contacto de la Unidad de Transparencia ante los cuales podrán solventarse dudas relacionadas con el desarrollo de la auditoría

Etapa de revisión: El acuerdo de inicio deberá ser notificado a la instancia respectiva y deberá obrar en el expediente que para esos efectos integre la Unidad de Transparencia.

Examinación: En el marco de lo estipulado en el acuerdo de inicio, la Unidad de transparencia procederá a la revisión del tratamiento o tratamientos de datos personales, a efecto de corroborar que se encuentren apegados a los principios y deberes siguientes:

A. Principio de licitud: el tratamiento de datos personales deberá tener sustento o estar relacionado con las facultades o atribuciones que la normatividad aplicable confiera a la instancia auditada.

B. Principio de finalidad: el tratamiento de datos personales deberá estar justificado por finalidades concretas, lícitas, explícitas y
legítimas, relacionadas con las atribuciones que la normatividad aplicable le confiera a la instancia auditada.

C. Principio de lealtad: que los datos personales no se hayan obtenido a través de medios engañosos o fraudulentos.

D. Principio de consentimiento: cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la Ley General, la instancia auditada deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales.

E. Principio de calidad: que la instancia auditada haya adoptado las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

F. **Principio de proporcionalidad**: que la instancia auditada sólo haya tratado los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad para la cual fueron recabados.

G. Principio de información: que la instancia auditada haya informado al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales.

H. **Principio de responsabilidad**: que la instancia auditada haya adoptado la políticas y mecanismos necesarios para asegurar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General que establece las disposiciones en materia de protección de datos personales.

I. Deber de seguridad: que la instancia auditada haya establecido y mantenido medidas de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión.

J. **Deber de confidencialidad**: la instancia auditada deberá demostrar la existencia de controles o mecanismos que tengan por objeto que todas aquellas personas que

intervengan en cualquier fase del tratamiento de los datos personales guarden confidencialidad respecto de éstos.

VI. Proceso de revisión y Mejora Continua

El proceso de revisión y mejora continua permitirá verificar que los parámetros establecidos en la LGPDPPSO, en los Lineamientos Generales, en este Programa de Protección de Datos Personales y en el Documento de Seguridad se cumplan cabalmente o permitan realizar los ajustes necesarios para su cumplimiento. La finalidad de la implementación cíclica de estas etapas permitirá garantizar el tratamiento óptimo de los datos personales en posesión de Cada de Moneda.

ETAPA 1. En esta etapa, se realizará una revisión de inventarios de datos personales y avisos de privacidad. Con la finalidad de cumplir con la política de gestión de datos personales, las obligaciones y las verificaciones del Programa se llevará a cabo un análisis de los inventarios de datos personales y avisos de privacidad. Esta revisión permitirá verificar que se cumplen con las obligaciones normativas.

Formato de revisión de Inventario.

Nombre de la Unidad Administrativa		**Cumplimiento**
objetivo	Actualización de inventarios y avisos de privacidad	SI
		NO
meta	Todas las áreas que realizan tratamiento de datos personales deberán contar con el inventario de datos personales y avisos de privacidad	SI
		NO
Medios de Verificación	Correo electrónico institucionales, que sirva de de información de integración de nuevos activos por parte de las unidades que manejan datos personales.	SI
		NO
		SI

	Oficios de información y cumplimiento de requerimientos.	NO
	Actualización de Avisos de Privacidad en la página de Transparencia (Apartado "Protección de datos personales, verificados por el área respectiva.	SI
		NO
	Cumplimiento del cronograma de trabajo trimestral.	SI
		NO

ETAPA 2. Cumplimiento del Programa de Capacitación. Que todo el Personal de Casa de Moneda este capacitado en el tema de tratamiento de Datos Personales, de todos los cursos que imparte del INAI, la implementación de talleres y asesorías especializadas dirigidas a las personas servidoras públicas que realizan algún tratamiento de datos personales.

Formato de Cumplimiento de Capacitación

Nombre de la Unidad Administrativa		**Cumplimiento**
objetivo	Que todas las personas servidoras públicas que tratan datos personales se encuentren capacitados en materia de protección de datos personales.	SI
		NO
meta	Todo el personal que realice atención a solicitudes ARCO, tratamiento de datos personales en cualquiera de sus etapas, personal de nuevo ingreso, deberá estar capacitado	SI
		NO
Medios de Verificación	Constancias de capacitación de los cursos impartidos	

Numero de Servidores capacitados por área	Número de personas.	Total:

ETAPA 3. Revisión y, en su caso, actualización del Documento de Seguridad. Cada que se detecte la creación o modificación de un inventario de tratamiento, se deberá actualizar dicho documento.

Se realizará una revisión de los siguientes puntos:

- Revisión de Inventario de Datos Personales
- Revisión de Avisos de Privacidad
- Cumplimiento del Programa anual de Capacitación
- Revisión y en su caso la actualización del documento de seguridad de Casa de Moneda de México.

La supervisión en materia de protección de datos personales se sustanciará mediante requerimientos de información sobre el tratamiento de datos personales, así como de sugerencias a las unidades administrativas para prevenir algún incumplimiento a las disposiciones en materia de protección de datos personales. Se deben implementar los diferentes formatos como lo es la bitácora de reporte de incidentes en caso de que se dé una vulneración de datos.

Bitácora de reporte de incidentes

Elaborado por:	Fecha elaboración:	Aprobado por:	Fecha de aprobación:

Naturaleza del Incidente o vulneración ocurrida:

_____
_____
_____
_____

Fecha y hora en que se produjo:

_____
_____
_____

Datos Personales Comprometidos:

_____
_____
_____

Nombre y cargo de quién recibe la notificación:

_____
_____
_____

Las recomendaciones dirigidas al titular sobre las medidas que éste pueda adoptar para proteger sus intereses:

_____
_____
_____
_____

Las acciones correctivas realizadas de manera inmediata

_____
_____
_____
_____

Los medios puestos a disposición del titular para que pueda obtener más información al Respecto.

_____
_____
_____
_____

La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente:

_____
_____
_____
_____
_____

VII. Sanciones

Cuando el Comité de Transparencia tenga conocimiento del incumplimiento de alguna obligación prevista en este Programa, deberá realizar un exhorto al área correspondiente para que lleve a cabo las acciones que resulten pertinentes con objeto de modificar dicha situación y evitar incumplimientos

futuros o situaciones de riesgo que los pudieran ocasionar. De manera adicional, es importante que las personas servidoras públicas que están a cargo del tratamiento de datos personales tengan presente que de conformidad con el artículo 163 de la LGPDPPSO serán causas de sanción por incumplimiento, las siguientes:

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 previstos en la LGPDPPSO 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, 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. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales.

VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la LGPDPPSO.

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 según los artículos 31, 32 y 33 de la LGPDPPSO.

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. Programa de Protección de Datos Personales

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

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.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones, serán consideradas como graves.

Asimismo, de conformidad con el artículo 105 de los Lineamientos Generales, cuando algún área competente se niegue a colaborar con la Unidad de Transparencia en la atención de las solicitudes para el ejercicio de los derechos ARCO, ésta dará aviso al superior jerárquico para que le ordene realizar sin demora las acciones conducentes.

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.