SISTEMAS DE SUPERVISIÓN, VIGILANCIA, MONITOREO, REVISIÓN, ALERTAS, VULNERACIONES Y AUDITORÍA EN MATERIA DE DATOS PERSONALES EN LA CASA DE MONEDA DE MÉXICO.

El presente documento, tiene por objeto dar cumplimiento a lo dispuesto en los artículos 30 fracción V, 33 fracción VII y 35 fracción VI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, mismos que establecen entre otros aspectos, las obligaciones y responsabilidades que tienen los sujetos obligados en el tratamiento de datos personales. Para el cumplimiento de estas obligaciones se debe contar con un sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de protección de datos personales.

Derivado de lo anterior, el documento de seguridad de la Entidad contiene entre otros puntos, los mecanismos de monitoreo y revisión de las medidas de seguridad, las cuales deberán de monitorear y revisar de manera periódica los aspectos siguientes:

1. Las medidas de seguridad implementadas en la protección de datos personales.
2. Las amenazas y vulneraciones a que están sujetos los tratamientos o sistemas de datos personales.

En el numeral 63 de Los Lineamientos Generales de Protección de Datos Personales para el Sector Público, establece que los responsables del tratamiento de datos personales, deben realizar el monitoreo y supervisión periódica de las medidas de seguridad, y deberán 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 lo anterior, dicho numeral estipula que se deberá monitorear continuamente lo siguiente:

1. Los nuevos activos que se incluyan en la gestión de riesgos (activo es todo elemento de valor involucrado en el tratamiento de datos personales, como pueden ser una base

de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documentos en papel).

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

3. Las nuevas amenazas que podrían estar activas dentro y fuera del sujeto obligado y que no han sido valoradas.
4. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
5. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
6. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
7. Los incidentes y vulneraciones de seguridad ocurridos.

Derivado de lo anterior, el responsable deberá contar con un programa de auditoría para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

Así, bajo un esquema de mejora continua, a efecto de mantener el monitoreo y revisión de los aspectos en cita, se presentan los mecanismos siguientes:

A. Mecanismo de monitoreo y supervisión en la protección de datos personales. Hipervínculo al portal de la CNDH, sección de casos especiales
B. Mecanismo de actuación ante alertas y vulneraciones a la seguridad de los datos personales.
C. Mecanismo de Auditoría en Materia de Datos Personales.

A. Mecanismo de monitoreo y supervisión en la protección de datos personales.

Se cuenta con la identificación de los Sistemas o Procesos de tratamiento de datos personales de las áreas que manejan datos personales en esta Entidad, los cuales se encuentran detallados en el Documento de Seguridad de Datos Personales en Posesión de Casa de La Moneda de México, el cual contiene las medidas de seguridad administrativas, físicas y técnicas que se

implementan en el tratamiento y protección de datos personales.

Al respecto, se cuenta con un cronograma de trabajo donde se detallan las medidas de seguridad que se deberán implementar por las áreas que cuentan o tienen tratamiento de datos personales en la entidad.

Como un mecanismo de monitoreo de esta Entidad también se solicitará informes semestrales a los responsables de las áreas respectivas de esta entidad, que cuentan con tratamiento de datos personales, en los que dé cuenta del avance de cumplimiento de las medidas de seguridad establecidas para evitar vulneraciones a los sistemas de datos personales.

Así mismo, como parte de las acciones de monitoreo implementadas, la Unidad de Transparencia requerirá a cada unidad administrativa, por cada uno de los tratamientos que realiza en el manejo de datos personales, la elaboración del Reporte de Seguridad de Datos Personales, en el que deberán precisar los elementos siguientes:

1. Se indique si existe la actualización o modificación respecto de las medidas de seguridad y controles implementados en el tratamiento de datos personales que realice. De ser así, deberán incluir una explicación de tal actualización o modificación.

2. Se indique la incorporación de nuevos activos en el tratamiento que realiza, como podrían ser una actualización o modificación en el hardware o software del sistema utilizado, personal de nuevo ingreso a cargo del tratamiento o cualquier otro recurso humano o material que tenga impacto en el tratamiento de los datos personales.

3. Si existe o puede existir el surgimiento de nuevas amenazas en el tratamiento de los datos.

4. La posibilidad de que las nuevas amenazas actualicen una vulnerabilidad en el tratamiento de datos respectivo.

5. Casos en los que una amenaza haya sufrido alguna modificación que derive en el incremento del impacto que

tendría su materialización en la seguridad de los datos personales.

Con la finalidad de que la Unidad de Transparencia, encargada de ejecutar el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales, se implementarán las siguientes etapas:

Monitoreo: Consistirá en el requerimiento por parte de la Unidad de Transparencia del Reporte de Seguridad de Datos Personales, el cual deberá ser desahogado por las instancias que, en el ámbito de sus atribuciones, sean las encargadas de los sistemas de tratamiento de datos personales.

La Unidad de Transparencia requerirá a cada una de las áreas que reportaron tratamientos de datos personales, a través de sus inventarios, la elaboración de un **reporte**, en el que deberán precisarse.

	SI	**NO**
Se realizan y mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de los datos personales.		
Las áreas administrativas que tienen tratamiento de datos personales han revisado el marco normativo que regula en lo particular el tratamiento de datos personales en cuestión, a fin de identificar si éste contempla medidas de seguridad específicas o adicionales a las previstas en la LGPDPPSO y los Lineamientos Generales, y se ha definido la procedencia de su implementación		
Se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.		

Se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.		
Se monitorea y revisa de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, tomando en cuenta lo siguiente: • Los nuevos activos que se incluyan en la gestión de riesgos; • Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras; • Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas; • La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes; • Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir; • El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y • Los incidentes y vulneraciones de seguridad ocurridas.		

Supervisión: Consistirá en el análisis por parte de la Unidad de Transparencia del Reporte de Seguridad de Datos Personales.

Así mismo, la Unidad de Transparencia analizará los reportes de seguridad de datos personales remitidos por las instancias, verificando especialmente lo siguiente:

1. La idoneidad y efectividad de las medidas de seguridad y control respecto del tratamiento.
2. La suficiencia de controles preventivos y correctivos.
3. La gestión interna de nuevas amenazas, vulnerabilidades e incrementos en el impacto de probables daños.
4. Avances generados conforme a lo establecido en el Plan de Trabajo.
5. El cumplimiento de políticas, planes, procesos y procedimientos en materia de seguridad de datos personales.

La Unidad de Transparencia al término de esta revisión elaborará un Dictamen de Seguridad de datos personales en el que se plasmaran las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, notificando al área respectiva

Las recomendaciones y/o requerimientos habrán de ser desahogados, destacando el plazo en que deberán remitirse las evidencias de su cumplimiento a la Unidad de Transparencia.

B. Mecanismos de actuación ante alertas y vulneraciones a la seguridad de los datos personales.

Alerta de Seguridad: Corresponde a una Detección de una amenaza que, de haberse materializado en un daño, hubiera implicado una afectación en la seguridad de los datos personales. Es importante precisar que esta alerta debe contener los siguientes elementos.

- Emisión del reporte de Alerta de Seguridad: Es realizado por la Instancia o área de la entidad que maneja los datos personales y en donde se desarrolló el incidente.

- Registro y análisis por la Unidad de Transparencia, mediante el cual ésta deberá rendir un informe al Comité de Transparencia.

Vulneración de seguridad: Afectación acaecida a los datos personales en cualquier fase de un tratamiento, que haya generado. Cuando se materialice esta vulneración, el titular del área donde se genere debe:

- Realizar el llenado en la bitácora de Vulneraciones.
- Rendir un Informe de Causas y Acciones de una vulneración, informando a la Unidad de Transparencia.
- La Unidad de Transparencia debe notificar la vulneración ocurrida al INAI.
- Notificación de vulneración al particular, por parte de la Instancia.

Mecanismos específicos que las unidades administrativas de la Casa de Moneda de México (CMM) deberán efectuar cuando:

Se materialice una alerta de seguridad en cualquier fase del tratamiento de datos personales. En este caso, deberán maximizar la protección de los datos personales en posesión de Casa de Moneda de México (CMM), mediante lo siguiente:

- Registrar las amenazas que configuren alertas de seguridad.
- Analizar las alertas de seguridad registradas con la finalidad de definir estrategias para la prevención de una vulneración de seguridad.
- Integrar las estrategias de prevención en el Plan de Trabajo a efecto de que, en los casos conducentes, se implementen como medidas adicionales de seguridad.

Derivado de lo anterior, en caso de advertir una alerta de seguridad se deberá proceder conforme al mecanismo siguiente:

A. Al segundo día hábil siguiente a la fecha en que se detecte la amenaza, la instancia respectiva deberá elaborar un Reporte de Alerta de Seguridad, en los términos que más adelante se abordarán.

B. Al tercer día hábil siguiente a la fecha en que se detecte la anomalía, el reporte deberá ser remitido a la Unidad de

Transparencia quien efectuará el análisis correspondiente.

La unidad administrativa deberá emitir un Reporte de Alerta de Seguridad, en el cual se deberá considerar, como mínimo, el desarrollo de los aspectos siguientes:

Detección.

I. Nombre, cargo y adscripción del servidor público que detectó la amenaza.

II. Fecha, hora y lugar en que se detectó, así como una descripción detallada de cómo fue descubierta.

III. Tratamiento o sistema en que ocurrió.

IV. Nombre, cargo y adscripción del servidor público responsable del tratamiento o sistema.

V. Datos personales involucrados en la amenaza.

Proyección de una posible vulneración.

I. Elementos que permitieron el desarrollo o persistencia de la amenaza.

II. Actuaciones que pueden evitar la reincidencia de la amenaza

III. Descripción de los efectos que hubiera causado la anomalía si hubiere persistido hasta materializar una vulneración.

Medidas de seguridad involucradas

I. Descripción clara de los controles físicos o electrónicos involucrados en la amenaza.

II. Circunstancias que, individual o conjuntamente, permitieron la existencia de la amenaza.

III. Justificar si la amenaza pudo ser prevenida, detallando las herramientas, medios, procedimientos y el personal con que se cuente que efectivamente hubiera podido llevar a cabo tal prevención.

IV. Ante la materialización de la amenaza, justificar si en el futuro puede evitarse su reincidencia, detallando las herramientas, medios, procedimientos y el personal con que se cuente que efectivamente puedan impedirlo.

V. Si la forma de prevenir o evitar la reincidencia de la amenaza, involucran una nueva medida de seguridad, deberá ser claramente descrita.

Concluido lo anterior, al **tercer día hábil siguiente a la detección de la alerta,** el reporte deberá ser remitido a la Unidad de Transparencia.

Recibido el *Reporte de Alerta de Seguridad,* la Unidad de Transparencia procederá a su registro y realizará un análisis de los aspectos siguientes:

a) El impacto que tiene la alerta en la seguridad de los datos personales.
b) Observaciones en materia de seguridad que la instancia debe aplicar en el futuro desarrollo del tratamiento.
c) Medidas de seguridad adicionales que se estime conducente implementar.
d) Si resulta posible, determinar una estrategia de prevención con instancias en las que la alerta de seguridad pueda desencadenarse.

Se materialice una vulneración de seguridad en cualquier fase del tratamiento de datos personales.

Ante una vulneración en la seguridad de los datos personales, de conformidad a la normatividad aplicable, se establecen las obligaciones siguientes:

1. 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 a efecto de evitar que la vulneración se repita.
2. Inscribir la vulneración en la bitácora de las vulneraciones.
3. Informar sin dilación alguna al titular y al Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), las vulneraciones que afecten de forma significativa derechos patrimoniales o morales, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

Para la emisión del informe en mención, necesariamente habrá que considerar, como mínimo, el desarrollo de los aspectos siguientes:

Detección

I. Nombre, cargo y adscripción del servidor público que detectó la vulneración.
II. Fecha, hora y lugar en que se detectó la vulneración.
III. Tratamiento o sistema que fue vulnerado.

IV. Nombre, cargo y adscripción del servidor público responsable del tratamiento o sistema.
V. Datos personales involucrados en la vulneración.
VI. Descripción detallada de la forma en que se detectó la vulneración.

Investigación

I. Fecha y hora en que se inició la investigación de la vulneración
II. Nombre y cargo del servidor público designado para la investigación de la vulneración
III. Naturaleza de la vulneración.
IV. Fecha y hora de la vulneración.
V. Descripción detallada de la forma en que se desarrolló la vulneración.
VI. Tipo y número aproximado de titulares afectados
VII. Posibles consecuencias de la vulneración.

Medidas de seguridad vulneradas e impacto causado.

a. Descripción clara de cada uno de los controles físicos o electrónicos que operan en el tratamiento o sistema, incluyendo el servidor público responsable de su implementación.

b. Identificación de la totalidad de las personas que cuentan con acceso a cualquiera de las fases del tratamiento, incluyendo servidores públicos o personas ajenas a la CMM.

c. Identificación y descripción de la vulneración materializada.

d. Determinación del nivel de impacto causado por la vulneración en relación con el tratamiento o sistema (alto, medio, bajo), considerando el número de titulares afectados, así como el tipo y naturaleza de los datos personales involucrados en la vulneración.

e. Determinación relativa a si la vulneración generó una afectación significativa a los derechos patrimoniales y/o morales de los titulares de los datos personales.

Acciones preventivas y correctivas.

a. Justificar si la vulneración pudo ser prevenida, es decir si hubiera sido posible eliminar las causas del riesgo que fue materializado, detallando las herramientas, medios, procedimientos y el personal con que se cuente que efectivamente hubiera podido llevar a cabo tal prevención.

b. Si la vulneración no pudo ser prevenida, describir de manera detallada la herramienta, medida o procedimiento con la que se estaría en oportunidad de prevenir futuras vulneraciones del mismo tipo.

c. Analizar las medidas que, de acuerdo con la magnitud de la vulneración ocurrida, permitan el restablecimiento del tratamiento o sistema de datos personales.

d. Analizar las medidas correctivas que permitan evitar la reincidencia de las acciones que propiciaron la vulneración.

e. Recomendaciones para el titular afectado.

f. Medio puesto a través del cual pueda obtenerse más información respecto de la vulneración.

g. Datos de contacto de los servidores públicos designados para la gestión de la vulneración.

h. Cualquier información y/o documentación que se considere conveniente.

Análisis de la vulneración de seguridad.

Recibido el Informe de Causas y Acciones de una Vulneración, la Unidad de Transparencia procederá a su registro y realizará un análisis que deberá dilucidar los aspectos siguientes:

a) El impacto que tiene la vulneración de seguridad en la protección de los datos personales.

b) Observaciones en materia de seguridad que la instancia debe aplicar en el futuro desarrollo del tratamiento.

c) Medidas de seguridad adicionales que se estime conducente implementar.

d) Si resulta posible determinar una estrategia de prevención en diversos tratamientos en los que la vulneración de seguridad pueda desencadenarse.

Si del análisis de la vulneración, la Unidad de Transparencia advierte la posibilidad de generar una estrategia de prevención procederá a su integración en el Plan de Trabajo de la CMM.

La Unidad de Transparencia integrará la Bitácora de Vulneraciones a la Seguridad de los Datos Personales, en la que se concentrarán las vulneraciones acaecidas en la totalidad de las unidades administrativas de la CMM; de conformidad con el formato que se aplique.

Por lo que, dentro del plazo de 24 horas siguientes al en que la instancia notifique la vulneración, se deberá proceder a su registro.

La inscripción realizada, deberá ser informada por la Unidad de Transparencia y al Comité de Transparencia, para su conocimiento y efectos conducentes.

Posterior a la inscripción deberá remitirse una copia de dicho registro a la instancia respectiva, a efecto de que sea integrada a su bitácora interna de incidentes y vulneraciones a la seguridad.

Informe de la vulneración al INAI y al titular de los datos personales.

El artículo 40 de la Ley General dispone que, ante una vulneración que afecte de forma significativa derechos patrimoniales o morales, se deberá informar sin dilación alguna al titular y al INAI.

Dicho informe, deberá realizarse en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

Al respecto, el artículo 66 de los Lineamientos Generales estipula que la notificación del informe al titular y al Instituto referido deberá realizarse dentro en un plazo máximo de 72 horas, a partir de que se confirme la ocurrencia de la vulneración y el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación de afectación.

Bajo ese panorama, ocurrida una vulneración, la Unidad de Transparencia deberá realizar lo siguiente:

A. Notificar la vulneración al INAI.
B. Verificar que la instancia respectiva notifique al particular o particulares afectados por la vulneración identificada.

Notificación de la vulneración a los particulares.

De haberse considerado la actualización de una afectación significativa al patrimonio o a la moral del titular o titulares de los

datos personales, la instancia respectiva deberá realizar un informe que considere los aspectos siguientes:

- La naturaleza de la vulneración.
- Los datos personales comprometidos.
- Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses.
- Las acciones correctivas realizadas de forma inmediata.
- Los medios donde puede obtener más información al respecto.
- La descripción de las circunstancias generales en torno a la vulneración ocurrida, que le ayuden a entender el impacto de la vulneración.
- Cualquier otra información y documentación que se considere conveniente para apoyar a los titulares de los datos personales afectados.

La Unidad de Transparencia podrá auxiliar a la instancia en la elaboración del informe, el cual deberá notificarse por la instancia respectiva al particular o los particulares afectados dentro de las 72 horas siguientes a la detección de la vulneración

Auditoria: Ley General de Datos Personales en Posesión de Sujetos Obligados (Ley General), establece que se deberá mantener un sistema de supervisión y vigilancia, incluyendo auditorías, que permita comprobar el cumplimiento de las políticas de datos personales.

Las auditorías en materia de datos personales tendrán las finalidades siguientes:

- ✓ Determinar que los tratamientos de datos personales se encuentren apegados a la normativa aplicable.
- ✓ Supervisar la adopción y cumplimiento de las políticas, procedimientos y mecanismos determinados en el Sistema de Gestión y el Documento de Seguridad.
- ✓ Verificar la eficiencia de las medidas de seguridad físicas, administrativas y técnicas instauradas.
- ✓ Validar el avance de los objetivos planteados en el Plan de Trabajo.

- ✓ Prevenir la materialización de vulneraciones a la seguridad de los datos personales.

- ✓ Promover la implementación de mejoras en el tratamiento de los datos personales, que permitan elevar su grado de protección.

En ese sentido, el Mecanismo de Auditoría en Materia de Datos personales tiene como objetivos principales los siguientes:

1. Establecer los aspectos a examinar.

2. Puntualizar los documentos a través de los cuales se asentará el desarrollo de las etapas respectivas, las observaciones advertidas y las aclaraciones conducentes.

3. Precisar el proceso a través del cual se seleccionarán las instancias auditables.

Es importante referir que el alcance que tendrán las auditorías practicadas se concentrará exclusivamente en el análisis de la forma en que cada instancia, en el ámbito de su competencia, implementa las políticas que les resulten aplicables en materia de datos personales, así como la evaluación del estado de seguridad en que se encuentran los datos personales bajo su tratamiento; lo anterior, con la finalidad de implementar mejoras que de manera progresiva permitan a la CMM perfeccionar el manejo y protección de los datos personales.

El Programa de Auditoría en materia de Datos Personales será ejecutado por la Unidad de Transparencia; con el informe respectivo al Comité de Transparencia.

Por lo que se refiere al ámbito de aplicación, se indica que las instancias que en el ejercicio de sus funciones realicen el tratamiento de datos personales, serán los sujetos auditables materia del programa, de modo que se encuentran obligadas a coadyuvar activamente con la Unidad de Transparencia para el desarrollo de las auditorías respectivas.

Etapas de la auditoria en materia de datos personales.

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.

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, en el Programa de Protección de Datos Personales y en el Documento de Seguridad.

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.

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.