GUÍA PARA REGISTRAR Y REPORTAR VULNERACIONES DE DATOS PERSONALES

I. OBJETIVO.

Establecer los medios y procedimientos para que las áreas que realizan tratamientos de datos personales conozcan las acciones a seguir ante una vulneración de datos personales, así como las acciones correctivas que deben implementar de forma inmediata y definitiva.

II. ÁMBITO DE APLICACIÓN.

Aplica a las áreas del Centro Nacional de Metrología que realizan tratamientos de datos personales.

DEFINICIONES.

Para los efectos del presente documento se entenderá por:

Activo: Todo elemento de valor para una organización, involucrado en el tratamiento de datos personales, entre ellos, las bases de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documentos en papel.

Activos críticos: Activos que un responsable considera como los más valiosos que, si ocurre su pérdida, destrucción, robo, extravío, copia, uso, acceso, tratamiento, daño, alteración o modificación no autorizada, podría provocar una crisis, y comprometer las operaciones, la prestación de servicios o incluso la existencia de la organización.

Alerta de seguridad: Hecho o evento que se detecta y/o registra en los sistemas de tratamiento físico o electrónico, el cual advierte de un posible incidente de seguridad.

Amenaza: Circunstancia o condición externa, con la capacidad de causar daño a los activos explotando una o más de sus vulnerabilidades.

Áreas: Instancias previstas en el Estatuto Orgánico del Centro Nacional de Metrología, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales.

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de

Transparencia y Acceso a la Información Pública.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Derechos ARCOP: Los derechos de acceso, rectificación, cancelación, oposición y portabilidad al tratamiento de datos personales.

Días: Días hábiles.

Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o de manera conjunta con otras trate datos personales a nombre y por cuenta del responsable.

Incidente de seguridad. Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas de un responsable, que afecte la confidencialidad, la integridad o la disponibilidad de la información.

Instituto: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Integridad: Propiedad de la información para salvaguardar la exactitud y completitud de la información.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Plataforma Nacional: La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública.

Revelación: Incidente de seguridad en el cual se expone la información a través de Internet o medios de comunicación masiva.

Riesgo: Potencial o probabilidad de que ocurra un escenario donde una amenaza explote una o varias vulnerabilidades existentes en un activo o grupo de activos, y que éste cause un impacto negativo o daño.

Sistema de tratamiento: Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión,

almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos.

Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Titular: La persona física a quien corresponden los datos personales.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales;

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública;

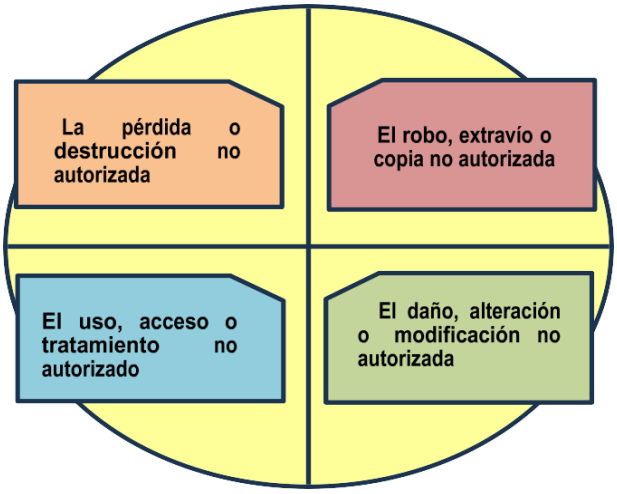
Vulnerabilidad: Circunstancia o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño y,

Vulneración de seguridad: Incidente de seguridad que afecta los datos personales en cualquier fase de su tratamiento, de acuerdo con el artículo 38 de la LGPDPPSO.

ARGUMENTO.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados señala que todo responsable que lleve a cabo tratamiento de datos personales tiene la obligación de establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra vulnerabilidades.

El Artículo 38 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece que las vulneraciones a la seguridad de los datos personales pueden ocurrir en cualquier fase del tratamiento de datos, siendo por lo menos, las siguientes:



Ahora bien, de conformidad con lo dispuesto en los artículos 36 a 41 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los responsables del tratamiento están obligados a notificar las vulneraciones que ocurran en cualquier fase del tratamiento de datos, que afecten de forma significativa los derechos patrimoniales o morales de los titulares, así como tomar medidas preventivas, correctivas y de mejora para evitar nuevas vulneraciones y, realizar las notificaciones al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales como Órgano Garante.

Como se señaló en las definiciones, un activo es todo elemento de valor para una organización, involucrado en el tratamiento de datos personales. Estos activos son susceptibles a amenazas, es decir, a factores externos que tienen el potencial de dañarlos.

En términos del Sistema de Gestión de Seguridad de Datos Personales los activos deberán ser aquéllos que estén relacionados con el ciclo de vida de los datos personales previamente identificados y sus distintos tratamientos.

Se pueden identificar dos tipos de activos:

Activos de información, corresponden a la información relativa a los datos personales o información de procesos en los que interviene el flujo de datos personales y actividades involucradas en el tratamiento de éstos.

Activos de apoyo, en los cuales residen los activos de información, como son: o Hardware o Software o Redes y Telecomunicaciones o Personal o Estructura organizacional o Infraestructura adicional.

Para que una amenaza tenga efecto, requiere explotar una vulnerabilidad, debilidad o falla propia de un activo. Los activos, las amenazas y las vulnerabilidades se combinan para generar riesgos. Cuando un riesgo se materializa, ocurre un incidente de seguridad, el cual se traduce en una violación a las medidas de seguridad.

Una amenaza tiene el potencial de dañar un activo y causar una vulneración a la seguridad. Las amenazas pueden ser de origen natural o humano, y pueden ser accidentales o deliberadas y además provenir de adentro o desde afuera de la

organización. Las amenazas deben ser identificadas considerando que algunas pueden afectar a más de un activo al mismo tiempo.

Para identificar un incidente de seguridad, se requiere de la detección y/o registro de alertas de seguridad, los cuales son advertencias respecto a cambios en los sistemas de tratamiento.

Las vulnerabilidades son debilidades en la seguridad de los activos y pueden ser identificadas en los siguientes ámbitos:

Organizacionales

- De procesos y procedimientos
- De personal
- Del ambiente físico
- De la configuración de sistemas de información
- Del hardware, software o equipo de comunicación
- De la relación con prestadores de servicios
- De la relación con terceros

La presencia de vulnerabilidades no causa daño por sí misma, se requiere de una amenaza que la explote. Una vulnerabilidad que no se encuentre expuesta a una amenaza identificada posiblemente no requiera la implementación de un control, pero debe ser reconocida y monitoreada constantemente, o bien, cuando surja algún cambio.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados especifica como obligaciones ante la presentación de vulneraciones:

- ✓ Analizar las causas por las cuales se presentó la vulneración e implementar en su plan de trabajo - del Documento de Seguridad- las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales para evitar que la vulneración se repita.

- ✓ Llevar una bitácora de vulneraciones en la que se describa la fecha en que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

- ✓ Informar al titular de los datos personales y al Instituto las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales de la persona titular.

A mayor abundamiento, el artículo 41 de la Ley de la materia dispone que, ante una vulneración, el responsable deberá informar al titular de los datos personales lo siguiente:

- La naturaleza del incidente.
- 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.

PROCEDIMIENTO PARA REGISTRO DE VULNERACIONES Y PLAN DE ACCIÓN

Con objeto de dar cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y tomando como referencia las mejores prácticas en materia de protección de datos personales, para reportar vulneraciones en el tratamiento de datos personales cuando se presente y evitar que se repita, se deberán seguir los siguientes pasos:

La persona servidora pública que tenga conocimiento sobre una vulneración de datos personales deberá informar, inmediatamente, a la Unidad de Transparencia del CENAM.

La Unidad de Transparencia deberá informar inmediatamente sobre la vulneración a la persona titular del área o unidad administrativa de su adscripción para informar el hecho. La Unidad de Transparencia brindará el acompañamiento necesario en las gestiones que deban documentarse, las cuales deben realizarse con celeridad para garantizar la eficacia de las medidas adoptadas.

La persona titular del área coordinará las acciones preventivas que se estimen convenientes al interior del área de su adscripción para asegurar el cese inmediato de la vulneración.

Una vez implementadas las acciones preventivas, el titular del área o unidad administrativa deberá documentar, a través de la BITÁCORA DE VULNERACIONES, la siguiente información:

- Tratamiento(s) de datos personales afectado(s).
- El nombre y la clave de identificación registradas en el Inventario de Tratamientos de Datos Personales.
- Nombre y cargo de quien reporta la vulneración dentro del área.
- Fecha y hora aproximada de la vulneración.
- Tipo de vulneración.
- Motivos (posibles o identificados) de la vulneración.
- Motivo se relaciona con identificar las acciones u omisiones de cualquier persona -incluso ajena a la institución- que pudieran haber provocado la vulneración y sea posible distinguirlas en ese momento.
- Acciones preventivas realizadas por el área responsable.
- Fecha y hora aproximada en que se hizo del conocimiento a la Unidad de Transparencia. Para tener registro de ello, dicha comunicación podrá realizarse a través del correo electrónico pnt-tut@cenam.mx
- Firma del titular del área.

Identificada y registrada esta información, se deberán implementar y/o planear las acciones correctivas de corto plazo, en coordinación con la Unidad de Transparencia y las áreas competentes para subsanar la vulneración y evitar posteriores incidentes.

En caso de que se deba informar a los titulares de los datos personales y/o al INAI como Órgano Garante sobre una vulneración que ponga en riesgo sus derechos patrimoniales o morales, el titular del área o unidad administrativa responsable de la base de datos o archivo que fue vulnerado deberá informar al titular, en un plazo máximo de 72 horas, a partir de que se confirme que ocurrió la vulneración y que se haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación, lo siguiente:

- La naturaleza del incidente o vulneración ocurrida.

- 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 ayuden al titular a entender el impacto del incidente.
- Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

Se entenderá que se afectan los derechos patrimoniales del titular cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular.

Se entenderá que se afectan los derechos morales del titular cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica de éste.

El titular del área o unidad administrativa responsable de la base de datos o archivo que fue vulnerado deberá determinar los medios por los cuales se notificará a los titulares las vulneraciones ocurridas, tomando en cuenta lo siguiente: el perfil de los titulares, la forma en que mantiene contacto o comunicación con éstos, que sean gratuitos; de fácil acceso; con la mayor cobertura posible y que estén debidamente habilitados y disponibles en todo momento para el titular

La Unidad de Transparencia realizará los requerimientos internos necesarios para recabar información suficiente y emitirá las comunicaciones correspondientes, debiendo informar al Instituto lo siguiente:

- La hora y fecha de la identificación de la vulneración.
- La hora y fecha del inicio de la investigación sobre la vulneración.
- La naturaleza del incidente o vulneración ocurrida.
- La descripción detallada de las circunstancias en torno a la vulneración ocurrida.
- Las categorías y número aproximado de titulares afectados.
- Los sistemas de tratamiento y datos personales comprometidos.

El titular del área o unidad administrativa responsable de la base de datos o archivo que fue vulnerado deberá identificar y documentar las posibles causas de la vulneración e implementar las acciones preventivas y correctivas que se requieran para evitar que se repita. De igual forma, deberá informar al Comité de Transparencia las acciones implementadas para evitar que se repita la vulneración.

Al final de este proceso, deberá concluirse la información de la bitácora de vulneraciones, incluyendo las acciones correctivas implementadas y/o planeadas en el corto plazo, así como las áreas involucradas en su consecución. La versión original de la bitácora de vulneraciones deberá firmarse por el titular del área o unidad administrativa y permanecerá bajo resguardo del área involucrada. Además, se remitirá un ejemplar en copia simple a la Unidad de Transparencia para el seguimiento respectivo.

FORMATO DE BITÁCORA DE VULNERACIONES DE DATOS PERSONALES

Fecha	Día	Mes	Año

ÁREA O UNIDAD ADMINISTRATIVA RESPONSABLE DE LA BASE DE DATOS O ARCHIVO QUEFUE VULNERADO

Denominación del área	
Titular	

DATOS DE LA VULNERACIÓN Tratamiento (s) de datos personales afectado (s)

Nombre del sistema de tratamiento de datos personales (inventario)	
Clave de inventario	
Fecha y hora aproximada de la vulneración	
Nombre y cargo de la persona servidora pública que reportó la vulneración dentro del área	

Tipo de vulneración

Marque con una X el tipo de vulneración:

- ○ Pérdida o destrucción
- ○ Robo, extravío o copia no autorizada
- ○ Uso, acceso o tratamiento no autorizado
- ○ Daño, alteración o modificación.

Motivos (posibles o identificados) de la vulneración	
Acciones preventivas realizadas	
Fecha y hora de notificación a la Unidad de Transparencia	
Nombre y cargo de la persona servidora pública que reportó la vulneración dentro del área	
Acciones correctivas implementadas definitivamente	
Acciones correctivas planeadas a corto plazo	
Observaciones	
Firma el titular del área	

Fecha de elaboración 09 diciembre de 2024