Guía para la atención de vulneraciones de Datos Personales INMEGEN

INSTITUTO NACIONAL DE MEDICINA GENÓMICA

2024

Glosario

- Activo: En términos generales, es un bien tangible o intangible que una organización posee y que es requerido para su funcionamiento y el logro de objetivos; es decir, tiene valor para la organización.

- Activo primario: Es la información que contiene datos personales.

- Activo secundario: Todos los elementos físicos (como archivos e instalaciones) y/o tecnológicos (como servidores y sistemas) a través de los cuales se da tratamiento al activo primario.

- Cadena de custodia: Sistema de control y registro que se aplica al indicio, evidencia, objeto, instrumento o producto del hecho delictivo; desde su localización, descubrimiento o aportación, en el lugar de los hechos o hallazgo, hasta que la autoridad competente ordene su conclusión. Con el fin de corroborar los elementos materiales probatorios y la evidencia física, la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: condiciones de recolección, preservación, empaque y traslado.

- Confidencialidad: Deber de seguridad que garantiza que la información no se divulgue a personas no autorizadas.

- Control: Acciones de protección de datos personales resultado de las obligaciones de la normativa en la materia.

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

- Incidente de seguridad: Es un riesgo materializado que afecta de forma negativa la confidencialidad, integridad o disponibilidad de un sistema o la información que procesa, almacena o transmite debido a la explotación de una vulnerabilidad por un agente de amenaza, o que constituye una violación de las políticas y procedimientos de seguridad o políticas de uso aceptable

- INMEGEN: Instituto Nacional de Medicina Genómica.

- LGPDPPSO o Ley: Ley General De Protección de Datos Personales en Posesión de Sujetos Obligados.

- Vulnerabilidad: Debilidad o fallo en un sistema de información, procedimientos de seguridad del sistema, controles internos o de la implementación de un control que podría ser explotada o activada de manera intencional o no por una amenaza.

- Vulneración: Incidente de seguridad que involucra datos personales.

Introducción

Esta guía tiene como finalidad que las áreas responsables de las bases de datos, y quienes intervengan en su tratamiento, como custodios, usuarios y encargados, conozcan las acciones a seguir para gestionar las vulneraciones y, en caso de ser necesario, integrar y/o complementar las actividades necesarias en el proceso relacionado con su atención.

Es así que en cumplimiento a lo dispuesto en el artículo 40 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los responsables del tratamiento de datos personales tienen el deber de informar a los Titulares y al organismo garante, aquellas vulneraciones que afecten de manera significativa los derechos patrimoniales o morales.

Derivado de lo anterior, el presente documento es aplicable a todas las unidades administrativas que integran el Instituto Nacional de Medicina Genómica y Órgano Interno de Control que, por sus funciones, traten datos personales.

¿Qué es una vulneración?

Una vulneración es un incidente de seguridad de la información que afecta los datos personales en cualquier fase de su tratamiento.

Existe una vulneración a la seguridad de las bases de datos personales cuando en cualquier fase de tratamiento tiene lugar alguno de los siguientes acontecimientos:

- Pérdida o destrucción no autorizada de datos personales
    - Pérdida: Sucede cuando los datos existen, pero el área responsable pierde el control o el acceso a ellos.
    - Destrucción: Sucede cuando los datos ya no existen o existen en una forma que es imposible utilizarlos.
- Robo, extravío o copia no autorizada
    - Robo: Sucede cuando una persona se apodera de los datos personales sin derecho y sin consentimiento del área propietaria.
    - Extravío: Sucede cuando el área responsable por descuido desconoce u olvida dónde se encuentra el activo que contiene la información, provocando la pérdida de los datos personales.
    - Copia no autorizada: Sucede cuando el área responsable no
- Uso, acceso o tratamiento no autorizado
- Daño, alteración o modificación no autorizada

Se aconseja revisar y conocer las "Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales" emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y que se encuentran disponibles en https://home.inai.org.mx/wp-content/uploads/Recomendaciones_Manejo_IS_DP.pdf

En dicho documento, se describen los procesos y controles sugeridos por el organismo garante para que los responsables, respondan y mitiguen vulneraciones a la seguridad de la información personal que mantienen.

En caso de que ocurra una vulneración de seguridad, se deberá consultar inmediatamente las recomendaciones del INAI antes señaladas y, seguir los siguientes pasos:

a. Revisar de manera exhaustiva la magnitud de la afectación incluyendo:

   - Causas
   - Sistemas de datos afectados
   - Tipo de vulneración
   - Medidas de seguridad que fueron comprometidas
   - Nivel de afectación (derechos morales, derechos patrimoniales de los usuarios)
   - Actores involucrados en la vulneración (dentro y/o fuera de la organización)

   En caso de que la vulneración ocurra en sistemas administrados por un tercero encargado, éste debe obligarse contractualmente a notificar cualquier vulneración y cooperar durante todo el proceso de revisión y solución correspondiente.

b. De ser el caso, notificar a los titulares la vulneración ocurrida informando cuando menos:
   - Naturaleza del incidente
   - Datos personales comprometidos
   - Recomendaciones a los usuarios de las medidas que éstos pueden adoptar para proteger sus intereses.
   - Acciones correctivas realizadas de manera inmediata
   - Medios en donde pueden obtener más información.

c. Analizar causas por las que se presentó la vulneración e implementar un programa que incluya las acciones preventivas, correctivas y de mejora para actualizar las medidas de seguridad y evitar nuevas vulneraciones.

d. Evaluar la toma de acciones penales, civiles y/o laborales.

Bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales.

Cada unidad administrativa deberá reportar las actividades o sucesos en los que haya ocurrido una vulneración a cualquier sistema de datos personales ya sea físico o electrónico.

La siguiente tabla especifica el rol y funciones debe desempeñar cada área respecto de la atención a vulneraciones.

Áreas, roles y funciones para la atención de vulneraciones

Área / rol	Función
Unidad administrativa	1. Atender vulneraciones 2. Autorizar la implementación de medidas de seguridad para la mitigación de la vulneración, así como las medidas correctivas aplicadas de forma definitiva y medidas preventivas para la atención de la vulneración. 3. Determinar si es procedente la notificación de la vulneración al INAI así como a los titulares. 4. Notificar a los titulares. 5. Llevar una bitácora de vulneraciones.

Unidad de Transparencia	1. Notificar al INAI 2. Proveer el formato para las bitácoras de vulneraciones a las unidades administrativas.
Encargados	1. Notificar a las unidades administrativas cualquier incidente que pueda afectar la seguridad de los datos.

	2. Atender las actividades que las unidades administrativas les indiquen.
Dirección de Desarrollo Tecnológico	En caso de que la vulneración involucre activos informáticos 1. Atender la vulneración de manera conjunta con la unidad administrativa. 2. Contar con un plan de respuesta a incidentes y llevar a cabo las actividades que en él se establezcan. 3. Determinar y diseñar las acciones de mitigación, correctivas definitivas y preventivas de largo plazo junto con la unidad administrativa. 4. Proveer al área propietaria la información acerca de la detección, contención, erradicación de la vulneración y, en su caso, recuperación de los activos secundarios afectados para la toma de decisiones. 5. Proponer a la unidad administrativa las medidas de seguridad para mitigar la vulneración. 6. Implementar medidas correctivas aplicadas de forma definitiva y las medidas preventivas. 7. Disponer de las herramientas y algoritmos para el debido cuidado dela evidencia.

Usuarios	1. Reportar cualquier irregularidad, funcionamiento anormal o evento de seguridad identificado en cualquier fase del tratamiento de los datos personales.

Sanciones

De conformidad con el artículo 163 y 165 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, es responsabilidad de cada unidad administrativa la implementación de medidas de seguridad, por lo que la omisión de contar con las mismas constituye una sanción.

Para tal efecto, las responsabilidades de orden administrativo que resulten de dichos procedimientos son independientes de las que pudiesen implicar una sanción del orden civil o penal.

Procedimiento y Notificación de Vulneraciones

Preparación	I. Disponer de un Plan de Respuesta. La unidad administrativa deberá establecer la forma para detectar alertas de seguridad así como las herramientas y equipo para su atención II. Identificación de contactos. La unidad administrativa deberá designar un enlace con la Unidad de Transparencia así como elabora un directorio para la atención del incidente. III. Acuerdos de confidencialidad para las personas que atiendan las vulneraciones. Se sugiere incluir nombre, puesto, área de adscripción, función en la atención a la vulneración y el acuerdo de confidencialidad. IV. Determinar los medios para la atención a vulneraciones. Así como la manera en que realizarán el envío de información digital e impresa, se deberá establecer la manera en la que se comunicarán las brechas o debilidades encontradas.

Respuesta	I. Confirmar si un incidente vulneró la seguridad de los datos. i. Identificar la cantidad de datos personales y número de titulares afectados. ii. Categorizar los datos personales afectados, iii. Identificar si hubo activos secundarios afectados, mediante la detección de los sitios y medios de almacenamiento y el tipo de soporte documental donde están contenidos los datos personales. iv. Identificar el tipo de vulneración ocurrida. II. Implementar acciones de mitigación a) Disponer o definir un área de trabajo asignada para el análisis de las vulneraciones. b) Recolectar la evidencia que permita investigar las causas. c) Analizar las evidencias obtenidas. d) Generar el informe de resultados del análisis de la evidencia. e) Determinar la causa de la vulneración y proponer las medidas temporales para contenerla. f) En el caso de que aplique, disponer de ambientes de pruebas para verificar el correcto funcionamiento y compatibilidad de las acciones de mitigación que se pretenden implementar. g) Implementar/ejecutar las medidas temporales de mitigación III. Informar a la Unidad de Transparencia

	Notificar a la Unidad de Transparencia inmediatamente al momento de confirmar la vulneración y previa a la notificación de las y los titulares y al INAI para que, junto con la unidad administrativa, determinen si procede la notificación, a través del formato para ello. IV. Determinar si se notifica la vulneración al Titular y al INAI. La condición para determinar la afectación incide en si la vulneración afectó derechos patrimoniales o morales del titular. El plazo máximo para la notificación a la Unidad de Transparencia es de 36 horas que comenzará a correr el mismo día natural en que la unidad administrativa confirme la vulneración, para que la Unidad notifique al INAI dentro de las 72 horas que la Ley señala. V. Definir acciones correctivas definitivas Es necesario que dichas medidas sean incluidas en el plan de trabajo del documento de seguridad. VI. Definir acciones Preventivas. VII. Registrar la vulneración en la bitácora.

Anexo 1. Formato de Acuerdo de Confidencialidad

El/La que suscribe *nombre completo*, en mi calidad de *puesto que desempeña* de la *Dirección de área*, identificándome con el número *señalar número de empleado*, como empleado/empleada del Instituto Nacional de Medicina Genómica, en relación con la gestión de vulneraciones que pudieran presentarse en el *sistema/proceso de negocio/servicio*, donde desempeño la función de *señalar la función que desempeñará*.

Atendiendo a mis obligaciones y responsabilidades reconozco que tendré acceso a información susceptible de ser clasificada como confidencial o temporalmente reservada.

Además, entiendo que el acceso a tal información, sin importar su fuente, sea verbal, escrita, impresa, virtual o cualquier otra, tendrá el único propósito de cumplir con actividades requeridas en la gestión de vulneraciones, por lo que me comprometo a:

1. Desempeñar las actividades que me correspondan, bajo los principios de legalidad, profesionalismo, honradez, lealtad, integridad y eficiencia.

2. Facilitar las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes que correspondan.

3. Guardar cabal y absoluta secrecía y discreción durante y aún concluida mi relación laboral con el Instituto.

Por lo anterior, no podré utilizarla, difundirla, divulgarla, reproducirla, publicarla, cederla, transferirla, alterarla, falsificarla, destruirla, enajenarla de manera personal o por conducto de terceros, por cualquier medio a persona alguna y/o usarla con fines personales, lucrativos, comerciales u otro, en beneficio propio o de terceros y, en general, realizar cualquier acción no autorizada por escrito o contraria a los intereses del Inmegen, que pueda poner en riesgo la ejecución de las funciones y atribuciones del Instituto.

En el marco de todo lo observado acepto:

a) La posibilidad de ser sujeto de responsabilidades administrativas, civiles y penales en caso de incurrir en alguna de las acciones, omisiones o violaciones estipuladas en el presente acuerdo,
b) Abstenerme de participar en cualquier acto u omisión en el que exista la posibilidad de tener un conflicto de interés,

c) Estar obligado a notificar de forma inmediata a mi superior jerárquico y al área administrativa pertinente, en caso de tener conocimiento de algún hecho hipotético similar a los señalados en los incisos anteriores.

Lo anterior con fundamento en lo dispuesto por los Artículos 3, 110 fracción VI, 113, 174 y 186, fracción IV de la Ley Federal de Transparencia y Acceso a la Información Pública; 4, 113, fracción VI, 116, 201 y 206 fracción IV de la Ley General de Transparencia y Acceso a la Información Pública; 6, 7, 153, 163 y 165 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 75 de la Ley General de Responsabilidades Administrativas.

Leído el presente acuerdo de confidencialidad y con conocimiento de los derechos y obligaciones que de ella emanan, manifiesto mi conformidad con sus términos y asumo sin restricción alguna, las condiciones y responsabilidades que me correspondan, así como las consecuencias que deriven del incumplimiento de los compromisos establecidos por el Inmegen, en las leyes mexicanas y en las normas institucionales.

Ciudad de México a día de mes de año.

Nombre y firma del empleado

Anexo 2. Tipos de datos personales de acuerdo a su riesgo

Tipo de Dato	Riesgo inherente
Identificación y contacto, laborales y académicos. Como nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, domicilio, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo, experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cédula profesional, entre otros.	Bajo
De Ubicación física de la persona, la relativa al tránsito de las personas dentro y fuera del país (geolocalización) y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más (dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etc.).	Medio
De patrimonio. Todos aquellos que permitan inferir el patrimonio de una persona, incluye entre otros, saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados, número de tarjeta bancaria de crédito y/o débito.	Medio

De autenticación. Información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, identificaciones oficiales, inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona.	Medio
Jurídicos, como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.	Medio
Sensibles. Todos aquellos que afecten la esfera más íntima de su titular, es decir, los que puedan dar origen a discriminación o conlleven un riesgo grave a la integridad del titular, como revelar aspectos del origen racial o étnico, estado de salud, pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales, entre otros, según el caso en concreto.	Alto

Anexo 3. Formato de Aviso de Vulneraciones a la Unidad de Transparencia

Descripción de la Vulneración	
Fecha de identificación de la vulneración:	dd/mm/aaaa
Naturaleza de la vulneración:	
Descripción de las circunstancias de la vulneración ocurrida:	
Acciones correctivas inmediatas:	
Acciones implementadas para corregir los daños ocasionados:	
Posibles Consecuencias de la Vulneración	
Activos secundarios comprometidos	
Bases de datos:	
Sistema de tratamiento:	
Datos Personales comprometidos	
Categoría	Listado de datos
Tipo de riesgo	Número de titulares afectados

Anexo 4. Formato de Aviso Notificación de Vulneraciones al INAI

Datos de la Vulneración	
Fecha de identificación	
Hora de identificación	
Fecha de inicio de la investigación	
Hora de inicio de la investigación	
Descripción de la Vulneración	
Naturaleza	
Circunstancias de tiempo, modo y lugar.	
Acciones correctivas inmediatas	
Información comprometida	
Bases de datos	
Sistemas de tratamiento	
Datos Personales Comprometidos	
Categoría	Listado de datos personales

Tipo de riesgo	Número de titulares afectados
Recomendaciones dirigidas al titular	
Medio para que el titular obtenga más información	
Nombre completo de las personas designadas y datos de contacto	
Comentarios	

Anexo 5. Formato de Bitácora de registro de Vulneraciones

Bitácora de Vulneraciones:

Vulneración	Fecha	Motivo	Acciones Correctivas inmediatas	Acciones Correctivas Definitivas

Elaboró: _____