

## ANEXO 6.1

### 3.T. VULNERACIONES

#### 1. ¿Qué es una vulneración de datos personales?

Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

- I. La pérdida o destrucción no autorizada;
- II. El robo, extravío o copia no autorizada;
- III. El uso, acceso o tratamiento no autorizado, o
- IV. El daño, la alteración o modificación no autorizada.

#### 2. ¿En qué artículos de la Ley General y de los Lineamientos se prevé lo relativo a las vulneraciones?

37 al 41 de la LGPDPSO y 66 a 68 de los Lineamientos Generales.

#### 3. ¿Cuáles son las obligaciones vinculadas con las vulneraciones?

##### 3.1 Notificación de la vulneración: casos y plazo:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> <li>Informar al titular y al INAI, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en un plazo máximo de 72 horas, a partir de que se confirme que ocurrió la</li> </ul>	<ol style="list-style-type: none"> <li>Contar con mecanismos que permitan identificar cuándo ocurrió una vulneración a las bases de datos o archivos.</li> </ol>	<ul style="list-style-type: none"> <li>Gerencia de Tecnologías de la Información, en lo relativo a sistemas electrónicos.</li> <li>Subdirección General de Administración y Finanzas y unidad administrativa responsable de la</li> </ul>	<ul style="list-style-type: none"> <li>Mecanismos implementados para detectar vulneraciones ocurridas.</li> <li>Procedimiento para la gestión de vulneraciones de datos personales.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<p>vulneración y que se haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación.</p> <p>El plazo de 72 horas comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad.</p> <p>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.</p> <p>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,</p>	<p>2. Establecer un procedimiento para notificar las vulneraciones ocurridas al titular y al INAI en el plazo de 72 horas.</p>	<p>base de datos correspondiente, en archivos físicos.</p> <ul style="list-style-type: none"> <li>Comité de Transparencia y Gerencia de Tecnologías de la Información.</li> </ul>	

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
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.			

### 3.2 Contenido de informe para el titular:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> <li>• Informar al titular lo siguiente con relación a la vulneración ocurrida:               <ul style="list-style-type: none"> <li>○ La naturaleza del incidente o vulneración ocurrida;</li> <li>○ Los datos personales comprometidos;</li> <li>○ Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;</li> <li>○ Las acciones correctivas realizadas de forma inmediata;</li> <li>○ Los medios donde puede obtener más información al respecto;</li> <li>○ La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y</li> <li>○ Cualquier otra información y documentación que considere</li> </ul> </li> </ul>	3. Elaborar un formato de notificación de las vulneraciones de seguridad ocurridas, donde se incluya la información a la que refiere la columna anterior.	<ul style="list-style-type: none"> <li>• Comité de Transparencia.</li> </ul>	<ul style="list-style-type: none"> <li>• Formato de notificación al titular de la vulneración de seguridad ocurrida.</li> <li>• Constancia de las notificaciones.</li> </ul>
	4. Realizar las notificaciones de las vulneraciones cuando éstas ocurran, en el momento y con la información antes señalada.	<ul style="list-style-type: none"> <li>• Unidad administrativa responsable de la base de datos o archivo que fue vulnerado, con notificación al Comité de Transparencia.</li> </ul>	

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
conveniente para apoyar a los titulares.			

### 3.3 Contenido de informe para el INAI:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> <li>Informar al Instituto la siguiente información: <ul style="list-style-type: none"> <li>I. La hora y fecha de la identificación de la vulneración;</li> <li>II. La hora y fecha del inicio de la investigación sobre la vulneración;</li> <li>III. La naturaleza del incidente o vulneración ocurrida;</li> <li>IV. La descripción detallada de las circunstancias en torno a la vulneración ocurrida;</li> <li>V. Las categorías y número aproximado de titulares afectados;</li> <li>VI. Los sistemas de tratamiento y datos personales comprometidos;</li> <li>VII. Las acciones correctivas realizadas de forma inmediata;</li> </ul> </li> </ul>	<p>5. Elaborar un formato de notificación de las vulneraciones de seguridad ocurridas, donde se incluya la información a la que refiere la columna anterior.</p>	<ul style="list-style-type: none"> <li>Comité de Transparencia.</li> </ul>	<ul style="list-style-type: none"> <li>Formato de notificación al Instituto de la vulneración de seguridad ocurrida.</li> <li>Constancia de las notificaciones.</li> </ul>

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<p>VIII. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;</p> <p>IX. Las recomendaciones dirigidas al titular;</p> <p>X. El medio puesto a disposición del titular para que pueda obtener mayor información al respecto;</p> <p>XI. El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar mayor información al Instituto, en caso de requerirse, y</p> <p>XII. Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.</p>	<p>6. Realizar las notificaciones de las vulneraciones cuando éstas ocurran, en el momento y con la información antes señalada.</p>	<ul style="list-style-type: none"> <li>Unidad administrativa responsable de la base de datos o archivo que fue vulnerado, con notificación al Comité de Transparencia.</li> </ul>	

### 3.4 Medios de notificación:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> <li>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.</li> </ul>	<p>7. Determinar los medios de notificación de las vulneraciones.</p>	<ul style="list-style-type: none"> <li>Unidad administrativa responsable de la base de datos o archivo que fue vulnerado.</li> </ul>	<ul style="list-style-type: none"> <li>Documento en el que se describan los medios que se utilizarán en caso de que sea necesario notificar vulneraciones.</li> <li>Medio utilizado para notificar la vulneración.</li> </ul>



### 3.5 Bitácora:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> <li>Llevar una bitácora de las vulneraciones de seguridad ocurridas, en la que se describa la vulneración, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.</li> </ul>	<p>8. Elaborar un formato de bitácora de las vulneraciones ocurridas con la información antes señalada.</p> <p>9. Llevar una la bitácora de las vulneraciones de seguridad ocurridas.</p>	<ul style="list-style-type: none"> <li>Comité de Transparencia.</li> </ul>	<ul style="list-style-type: none"> <li>Bitácoras.</li> </ul>

### 3.6 Acciones preventivas y correctivas:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
<ul style="list-style-type: none"> <li>Analizar las causas por las cuales se presentó la vulneración e implementar en el plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales, a fin de evitar que la vulneración se repita.</li> </ul>	<p>10. Identificar y documentar las posibles causas de la vulneración e implementar las acciones preventivas y correctivas que se requieran para evitar que se repita.</p> <p>11. Informar al Comité de Transparencia las acciones implementadas para evitar que se repita la vulneración.</p>	<ul style="list-style-type: none"> <li>Gerencia de Tecnologías de la Información, en lo relativo a sistemas electrónicos.</li> <li>Unidades administrativas, en archivos físicos.</li> </ul>	<ul style="list-style-type: none"> <li>Análisis realizado.</li> <li>Acciones implementadas.</li> <li>Informe al Comité de Transparencia.</li> </ul>

#### 4. Lista de comprobación

	Sí	No
Se cuenta con mecanismos que permitan identificar las vulneraciones ocurridas a las distintas bases de datos y archivos del sujeto obligado.	<input type="checkbox"/>	<input type="checkbox"/>
Se cuenta con el procedimiento para realizar notificaciones de vulneraciones tanto a los titulares como al INAI.	<input type="checkbox"/>	<input type="checkbox"/>
Se han elaborado los formatos para notificar las vulneraciones a los titulares y al INAI, respectivamente.	<input type="checkbox"/>	<input type="checkbox"/>
Se han determinado los medios para notificar las vulneraciones.	<input type="checkbox"/>	<input type="checkbox"/>
Se han realizado las notificaciones de las vulneraciones en el momento y con la información establecida por la LGPDPPSO y los Lineamientos Generales.	<input type="checkbox"/>	<input type="checkbox"/>
Se cuenta con una bitácora de las vulneraciones ocurridas.	<input type="checkbox"/>	<input type="checkbox"/>
Se han identificado las causas de las vulneraciones e implementado las acciones preventivas y correctivas que se requieran para evitar que se repita.	<input type="checkbox"/>	<input type="checkbox"/>
Se ha informado al Comité de Transparencia sobre las acciones preventivas y correctivas implementadas para evitar que se repita la vulneración.	<input type="checkbox"/>	<input type="checkbox"/>