ANEXO 2
3.T. VULNERACIONES

De acuerdo con los artículos 37, 38, 39, 40 y 41 de la LGPDPPSO y 66, 67, 68 de los Lineamientos Generales, una vulneración de seguridad al debido tratamiento de datos personales se actualiza cuando, en cualquier fase de su tratamiento, ocurra al menos una de las siguientes acciones:

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.

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

Por otro lado, 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, orientación sexual, 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.

En caso de que ocurra alguna vulneración se deberá:

1. Informar al Titular de la **SESNA** y al **INAI**, este informe deberá presentarse a más tardar 72 hrs. a partir de que se confirme la vulneración.
2. Activar el proceso de mitigación de la afectación.
3. Notificar al titular del derecho.
4. Registrar en la bitácora de vulneraciones de seguridad la fecha en la que ocurrió, el motivo o causas que originaron ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

3.1 Plan de acción:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Informar al titular de los datos personales y al **INAI**, en un plazo máximo de 72 horas, a partir de que se confirme que ocurrió la vulneración. El plazo de 72 horas comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad.	Contar con mecanismos que permitan identificar cuándo ocurrió una vulneración a las bases de datos o archivos.	• USTPDN • Dirección General de Administración	• Mecanismos implementados para detectar vulneraciones ocurridas. • Procedimiento para la gestión de vulneraciones de datos personales
	Establecer un procedimiento para notificar las vulneraciones ocurridas al titular de los datos personales y al **INAI** en el plazo máximo de 72 horas.	• Comité de Transparencia • USTPDN • Dirección General de Administración	

3.2 Contenido del informe para el titular de los datos personales vulnerados:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
Informar al titular de los datos personales lo siguiente: • La naturaleza del incidente o vulneración ocurrida; • Los datos personales comprometidos; • Las recomendaciones al titular del derecho 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, y • Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.	Elaborar un formato de notificación de las vulneraciones de seguridad ocurridas, donde se incluya la información a la que refiere la columna anterior.	• Comité de Transparencia.	• Formato de notificación al titular de la vulneración de seguridad ocurrida. • Constancia de las notificaciones.
	Realizar las notificaciones de las vulneraciones cuando éstas ocurran, en el momento y con la información antes señalada.	• Unidad administrativa responsable de la base de datos o archivo que fue vulnerado, con notificación al Comité de Transparencia.	

3.3 Contenido de informe para el INAI:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
Informar al Instituto la siguiente información: ● 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; ● Las acciones correctivas realizadas de forma inmediata; ● La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida; ● Las recomendaciones dirigidas al titular del derecho; ● El medio puesto a disposición del titular del derecho para que pueda obtener mayor información al respecto; ● 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 ● Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.	Elaborar un formato de notificación de las vulneraciones de seguridad ocurridas, donde se incluya la información a la que refiere la columna anterior. Realizar las notificaciones de las vulneraciones cuando éstas ocurran, en el momento y con la información antes señalada.	● Comité de Transparencia. ● Unidad administrativa responsable de la base de datos o archivo que fue vulnerado, con notificación al Comité de Transparencia.	● Formato de notificación al Instituto de la vulneración de seguridad ocurrida. ● Constancia de las notificaciones.

3.4 Medios de notificación:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Determinar los medios por los cuales se notificará a los titulares del derecho las vulneraciones ocurridas, tomando en cuenta: el perfil de los titulares, la forma en que mantiene contacto o comunicación con éstos. Los medios de notificación deben ser gratuitos, de fácil acceso, con la mayor cobertura posible y disponibles en todo momento para dichos titulares.	Determinar los medios de notificación de las vulneraciones.	Unidad administrativa responsable de la base de datos o archivo que fue vulnerado, con notificación al Comité de Transparencia	• Documento en el que se describan los medios que se utilizarán en caso de que sea necesario notificar vulneraciones. • Medio utilizado para notificar la vulneración.

3.5 Bitácora:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• 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.	Elaborar un formato de bitácora de las vulneraciones ocurridas con la información antes señalada. Llevar una bitácora de las vulneraciones de seguridad ocurridas.	• Comité de Transparencia.	• Bitácoras.

3.6 Acciones preventivas y correctivas:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• 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.	Identificar y documentar las posibles causas de la vulneración e implementar las acciones preventivas y correctivas que se requieran para evitar que se repita. Informar al Comité de Transparencia las acciones implementadas para evitar que se repita la vulneración.	• Unidad administrativa responsable de la base de datos o archivo que fue vulnerado, con notificación al Comité de Transparencia	• Análisis realizado. • Acciones implementadas. • Informe al Comité de Transparencia.