PROCEDIMIENTO DE VULNERACIONES EN EL TRATAMIENTO DE DATOS PERSONALES

La Procuraduría de la Defensa del Contribuyente, es un organismo público descentralizado, no sectorizado, con autonomía técnica, funcional y de gestión, que proporciona de forma gratuita, ágil y sencilla servicios de orientación, asesoría, consulta, representación legal y defensa, recepción y trámite de quejas y reclamaciones contra actos u omisiones de las autoridades fiscales federales que vulneren los derechos de los contribuyentes, así como funge como mediadora en los acuerdos conclusivos, los cuales son un medio alternativo para resolver de forma anticipada y consensuada los diferendos que durante el ejercicio de las facultades de comprobación surjan entre las autoridades fiscales y los pagadores de impuestos, o bien, para regularizar la situación fiscal de estos últimos.

En ese sentido, derivado del objeto de su creación y debido a la información (datos personales) a la que tiene acceso por los servicios que presta, esta Procuraduría se encuentra altamente comprometida con la protección de datos personales que trata[1], observando en todo momento, lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como en los Lineamientos Generales de Protección de Datos personales para el Sector Público, a través de la constante supervisión de todos los servidores públicos que la integran, para que cumplan en sus términos con lo dispuesto en dicha normatividad.

De ahí que, si durante el tratamiento de los datos personales a los que se tiene acceso se presentan vulneraciones de seguridad las cuales pueden ser[2], 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.

A través del presente, se dan a conocer las obligaciones que tiene el titular de la Unidad Administrativa en la cual ocurrió la vulneración:

[1] El artículo 3, fracción XXXIII, de la Ley General citada, define a **tratamiento** como 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.

[2] Artículo 38, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Notificación de la vulneración - casos y plazo:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Informar al titular de los datos personales y al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (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 vulneración y que se haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación. El plazo de 72 horas comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad. 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	**1.** Contar con mecanismos que permitan identificar cuándo ocurrió una vulneración a las bases de datos o archivos.	• Dirección de Sistemas Sustantivos; Dirección de Infraestructura Tecnológica y Dirección de Sistemas Administrativos y Gobierno Electrónico, adscritas a la Dirección General Jurídica y de Planeación Institucional, en lo relativo a sistemas electrónicos. • Dirección de Administración y Operación de Servicios adscrita a la Dirección General de Administración y el *"Área Sustantiva competente"* responsable de la base de datos correspondiente, en archivos físicos y/o electrónicos.	• Mecanismos implementados para detectar vulneraciones ocurridas. • Procedimiento para la gestión de vulneraciones de datos personales.
	2. Establecer un procedimiento para notificar las vulneraciones ocurridas al titular y al INAI en el plazo de 72 horas.	• Comité de Transparencia y Dirección de Sistemas Sustantivos; Dirección de Infraestructura Tecnológica y Dirección de Sistemas Administrativos y Gobierno Electrónico, adscritas a la Dirección General Jurídica y de Planeación Institucional.	

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

Contenido de informe para el titular de los datos personales:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Informar al titular lo siguiente con relación a la vulneración ocurrida: o La naturaleza del incidente o vulneración ocurrida; o Los datos personales comprometidos; o Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses. o Las acciones correctivas realizadas de forma inmediata; o Los medios donde puede obtener más información al respecto; o La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y o Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.	**3.** 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.
	4. 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 físico que fue vulnerado, con notificación al Comité de Transparencia.	

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: **I.** La hora y fecha de la identificación de la vulneración; **II.** La hora y fecha del inicio de la investigación sobre la vulneración; **III.** La naturaleza del incidente o vulneración ocurrida; **IV.** La descripción detallada de las circunstancias en torno a la vulneración ocurrida; **V.** Las categorías y número aproximado de titulares afectados; **VI.** Los sistemas de tratamiento y datos personales comprometidos; **VII.** Las acciones correctivas realizadas de forma inmediata; **VIII.** La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida; **IX.** Las recomendaciones dirigidas al titular; **X.** El medio puesto a disposición del titular para que pueda obtener mayor información al respecto; **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 **XII.** Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.	**5.** Elaborar un formato de notificación de las vulneraciones de seguridad ocurridas, donde se incluya la información a la que refiere la columna anterior. **6.** 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 físico que fue vulnerado, con notificación al Comité de Transparencia.	• Formato de notificación al Instituto de la vulneración de seguridad ocurrida. • Constancia de las notificaciones.

Medios de notificación:

Obligaciones	Actividades para su cumplimiento	Unidad administrativa responsable del cumplimiento	Medios para acreditar el cumplimiento
• Determinar los medios por los cual 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.	**7.** Determinar los medios de notificación de las vulneraciones.	• Unidad Administrativa responsable de la base de datos o archivo físico que fue vulnerado.	• 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.

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.	**8.** Elaborar un formato de bitácora de las vulneraciones ocurridas con la información antes señalada. **9.** Llevar una la bitácora de las vulneraciones de seguridad ocurridas.	• Comité de Transparencia.	• Bitácoras.

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.	**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. **11.** Informar al Comité de Transparencia las acciones implementadas para evitar que se repita la vulneración.	• Dirección de Sistemas Sustantivos; Dirección de Infraestructura Tecnológica y Dirección de Sistemas Administrativos y Gobierno Electrónico, adscritas a la Dirección General Jurídica y de Planeación Institucional, en lo relativo a sistemas electrónicos. • Unidades administrativas, en archivos físicos.	• Análisis realizado. • Acciones implementadas. • Informe al Comité de Transparencia.