Ciudad de México, a 25 de junio de 2018
INAI/190/18

EMITE INAI RECOMENDACIONES PARA EL MANEJO DE INCIDENTES DE SEGURIDAD DE DATOS PERSONALES

- **El documento facilita a los responsables del manejo de datos personales, la atención a las vulneraciones que pudieran registrarse en su organización y, por ende, coadyuva en el cumplimiento de las obligaciones normativas**
- **De acuerdo con LFPDPPP y LGPDPPSO, los responsables del tratamiento están obligados a notificar las vulneraciones a la seguridad de los datos personales que afecten de forma significativa los derechos patrimoniales o morales de los titulares**

Con el fin de facilitar a los responsables del manejo de datos personales la atención de las vulneraciones que pudieran ocurrir en su organización y, por ende, coadyuvar en el cumplimiento de sus obligaciones normativas, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), elaboró las *Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales*.

El documento, que puede ser consultado en www.inai.org.mx, desarrolla una serie de sugerencias para orientar a los responsables del tratamiento de datos personales sobre cómo atender incidentes de seguridad que pongan en riesgo los datos personales.

Asimismo, ofrece los procedimientos mínimos para mitigar el impacto negativo a los titulares y a la organización del responsable, como consecuencia de un incidente de seguridad.

De este modo, si un incidente resulta en una vulneración a la seguridad de los datos personales, también se proporcionan formatos de referencia para documentarlos, así como el procedimiento de notificación de vulneraciones a los titulares.

De acuerdo con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los responsables del tratamiento están obligados a notificar las vulneraciones a la seguridad de los datos personales que ocurran en cualquier fase de su tratamiento, 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.

En ese sentido, el documento contiene un apartado con un *Plan de Respuesta a Incidentes de Seguridad*, en el que se desarrollan los conceptos y la metodología para su elaboración, en tres secciones:

1.- *Alertas e incidentes de seguridad*. Se explica la estructura de los riesgos, su relación con las alertas y los incidentes de seguridad, así como las condiciones en las que este último se convierte en una vulneración o revelación.

2.- *Incidentes de seguridad que afectan datos personales.* Se indica que las vulneraciones son un tipo particular de incidente de seguridad, y se describen las acciones que deben realizar los sujetos obligados para notificar y atender una vulneración, dependiendo de si son de sector público o de sector privado, y

3.- *Etapas del plan de respuesta a incidentes de seguridad.* Se desarrollan las etapas mínimas para generar y documentar un plan de respuesta a incidentes.

De igual forma, contiene una serie de recomendaciones orientadas a los usuarios en el entorno digital, para protegerse de amenazas informáticas como el *malware*.

-o0o-