Ciudad de México, a 20 de mayo de 2017
INAI/143/17

LLAMA INAI A TOMAR PRECAUCIONES PARA EVITAR LA VULNERACIÓN DE DATOS PERSONALES

- **Se consideran vulneraciones a la seguridad de los datos personales la pérdida o destrucción de los mismos; el robo, extravío o copia; el uso, acceso o tratamiento no autorizado, y el daño, la alteración o modificación de la información**
- **El Instituto recomienda asumir como prioridad la protección de la información personal**

El Instituto Nacional de Transparencia, Acceso a la Información y de Protección de Datos Personales (INAI) llama a tomar precauciones para evitar la vulneración de datos personales.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) establecen que se consideran vulneraciones a la seguridad de los datos personales la pérdida o destrucción de los mismos; el robo, extravío o copia; el uso, acceso o tratamiento no autorizado, y el daño, la alteración o modificación de la información.

Ante cualquier escenario que pueda vulnerar la información personal bajo el resguardo de instituciones públicas y organizaciones privadas, el INAI hace las siguientes recomendaciones:

1. Asumir como objetivo principal la protección de la información y después la de los equipos de cómputo.

Es importante que a la par de invertir en tecnología para proteger la información, se diseñe un sistema de gestión para cumplir de manera integral con todos los principios y deberes que establece la normatividad en materia de protección de datos personales.

Se debe tomar en cuenta que un alto porcentaje de las vulneraciones no se debe a falta de herramientas tecnológicas adecuadas sino a malas prácticas por parte de los trabajadores.

2. Considerar la privacidad y la seguridad desde el diseño.

Al momento de desarrollar una nueva tecnología, proceso o política pública es importante que desde su diseño se implementen las medidas necesarias para que los datos personales sean protegidos y tratados de manera adecuada.

3. Mantener siempre actualizados los equipos de cómputo y sistemas de información.

Es indispensable actualizar oportunamente el antivirus, las aplicaciones y el sistema operativo de los equipos de cómputo, dispositivos móviles y sistemas de información.

4. Probar y validar las copias y respaldos de información.

No es suficiente contar con copia de los datos personales y de la información crítica, además, hay que validar y hacer pruebas periódicamente para comprobar que los respaldos funcionen.

5. Estar atento a las noticias sobre ciberseguridad y protección de datos personales.

Es necesario mantenerse informado sobre nuevas amenazas, para poder implementar las medidas de seguridad más asertivas.

Finalmente, es importante que las instituciones públicas y organizaciones privadas tomen en cuenta que están obligadas a informar a los titulares y al INAI, en el caso del sector público, sobre las vulneraciones que hayan sufrido los datos personales que tengan bajo su resguardo.

-o0o-