Ciudad de México, a 5 de abril de 2020
INAI/110/20

INAI ACONSEJA EXTREMAR PRECAUCIONES AL PROPORCIONAR INFORMACIÓN PARA IDENTIFICACIÓN BIOMÉTRICA

- El Instituto advirtió que, para evitar la comisión de delitos como el robo de identidad por el aumento en el uso de sistemas de identificación biométrica, se debe ser cuidadoso con su utilización

Para prevenir delitos como el robo de identidad, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) recomienda ser cuidadosos con la utilización de sistemas de identificación biométricos.

Un sistema de autenticación biométrico recurre a técnicas como la lectura de huellas dactilares, el reconocimiento de iris, el análisis de retina, el reconocimiento facial y de voz, entre otros.

El INAI señala que se debe tomar en cuenta que diversas instituciones han incorporado sistemas de autenticación biométrica con el objetivo de generar alternativas que garanticen mayor seguridad a sus sistemas de información.

Este tipo de sistemas hacen uso de datos personales, lo que conlleva una alta responsabilidad en el tratamiento de la información.

Los datos personales biométricos no pueden cambiarse, como una contraseña alfanumérica, por ejemplo, que puede renovarse con cierta periodicidad e incluso eliminarse cuando ya no es necesaria, mientras que la información biométrica es inherente a la persona y no existe posibilidad de modificarla.

El INAI emite una serie de recomendaciones para los titulares de los datos personales en la utilización de la autenticación biométrica en la banca móvil:

Primero. Informarse sobre los riesgos relacionados con el tratamiento de datos biométricos para tomar decisiones más informadas respecto del uso de éstos.

Segundo. Estar al tanto de la política y/o aviso de privacidad de las aplicaciones de banca móvil con el objeto de informarse sobre:
a) Los datos personales biométricos que serán recabados. De preferencia, se recomienda que los responsables no conserven los datos biométricos, sino que reciba sólo los datos digitalizados con el fin de autenticar la identidad del usuario.
b) Las finalidades y uso que se dará a dichos datos.
c) Las medidas de seguridad que implementará el responsable para proteger los datos personales biométricos.
d) Los derechos que tiene en relación con el tratamiento de sus datos biométricos.

Tercero. Descargar aplicaciones de banca móvil únicamente en los sitios de aplicaciones autorizados.

Cuarto. Proporcionar el menor número de datos biométricos que sea posible.

Quinto. Utilizar el servicio de autenticación biométrica como método secundario de protección que complemente los otros métodos de seguridad, pero sin reemplazarlos del todo.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) establece que los responsables de los sistemas de información personal deberán informar, de forma inmediata, a los titulares de los datos sobre aquellas vulneraciones de seguridad que afecten de forma significativa sus derechos patrimoniales, señala el Instituto.

Para conocer más sobre estos derechos consultar www.inai.org.mx

-o0o-