Ciudad de México, a 20 de julio de 2017
INAI/226/17

EMITE INAI RECOMENDACIONES PARA USO DE DISPOSITIVOS CON TECNOLOGÍAS DEL INTERNET DE LAS COSAS

- **El Instituto afirmó que la información generada o utilizada a través de la interacción de los usuarios con los diversos dispositivos *IoT*, puede resultar atractiva para ciberdelincuentes y derivar en cibercrímenes, como robo de identidad o ciberacoso**

Un bajo nivel de seguridad en la utilización de dispositivos favorecidos con las tecnologías del Internet de las cosas puede representar un riesgo inminente a la privacidad de los usuarios, advirtió el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Se ha definido al internet de las cosas, *Internet of Things* o *IoT*, por sus siglas en inglés, como la infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos físicos y virtuales, gracias a la interoperabilidad de tecnologías de la información y la comunicación presentes y futuras.

En otras palabras, se apuntó, el Internet de las cosas es un concepto que hace alusión a la conexión digital existente entre los objetos de uso diario y cotidiano con el Internet.

El objetivo del internet de las cosas es lograr que todo artefacto, mediante el uso de sensores de red, bluetooth, wi-fi, entre otros, pueda conectarse en cualquier momento y lugar para mantener un monitoreo y control total de los procesos que cada uno de estos aparatos realice.

Estos objetos de uso diario pueden detectar, almacenar, procesar y transmitir información personal a través de una interconexión de Internet, como estado de salud, datos biométricos, hábitos y consumos, entre otros.

Por ejemplo, existen refrigeradores que advierten a los consumidores la fecha de caducidad de los alimentos; zapatos para correr que registran en la nube datos estadísticos relacionados con la actividad física semanal; televisores que permiten manipular el encendido o apagado de luces, cerraduras o termostatos en el hogar; cepillos dentales que pueden detectar caries; cámaras de seguridad con reconocimiento facial orientadas a la protección del domicilio; y automóviles que pueden conectarse a la red, a través de aplicaciones móviles, para realizar múltiples funciones, entre otros.

Sin embargo, el Instituto destacó que en la actualidad no se encuentran definidos los requisitos mínimos de seguridad que deben cumplir los fabricantes de equipos *IoT,* aunado a que los mismos no se encuentran exentos de ser objeto de algún tipo de vulneración.

De acuerdo con un estudio realizado por Hewlett Packard en 2015, se reportó que el 70 por ciento de los dispositivos más comúnmente utilizados en el Internet de las cosas tienen vulnerabilidades de seguridad en las contraseñas, cifrado o permisos de acceso, y que el 50 por ciento de las aplicaciones de dispositivos no encriptan las comunicaciones, lo cual puede derivar en un hackeo o acceso no autorizado a la información que éstos utilizan para su funcionamiento.

Asimismo, el órgano garante de la protección de datos personales, pidió no pasar desapercibido que la información generada o utilizada a través de la interacción de los usuarios con los diversos dispositivos *IoT* puede resultar atractiva para los ciberdelincuentes y propiciar así su obtención ilícita para la comisión de cibercrímenes, como robo de identidad o ciberacoso.

Por lo tanto, apuntó, es necesario que desarrolladores de software, fabricantes de dispositivos, proveedores de conectividad y compañías de análisis de datos hagan del conocimiento de los titulares de los datos todas las características concernientes a la información personal que será objeto de tratamiento.

El INAI emitió las siguientes recomendaciones para los usuarios de aparatos con tecnología *IoT*:

- Encriptar los dispositivos, en caso de contar con esa posibilidad en su configuración.
- Evitar guardar información personal que identifique o haga identificable al usuario a través del equipo. Por ejemplo, generar un nombre de usuario sin revelar su nombre verdadero.
- Crear una contraseña segura y distinta para todos y cada uno de los dispositivos *IoT*, la cual deberá ser lo más compleja posible.
- Desactivar las redes inalámbricas del dispositivo bluetooth, wi-fi, etc. cuando no sean necesarias o cuando no se esté utilizando el equipo.
- Indagar sobre los datos personales que los equipos *IoT* obtienen, así como revisar las políticas de privacidad correspondientes, en caso de existir.

- Moderar la utilización de aparatos vinculados al internet de las cosas, aminorando su uso para actividades que realmente lo ameriten.
- Actualizar el software de los diversos aparatos puede prevenir que los hackers tomen el control de un dispositivo.
- Cubrir las cámaras de cualquier dispositivo cuando no se esté utilizando.

-o0o-