Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

DIRECCIÓN GENERAL DE COMUNICACIÓN SOCIAL Y DIFUSIÓN

COMUNICADO • **INAI/261/21**

INAI ADVIERTE RIESGOS A LA PRIVACIDAD POR CONEXIÓN DE APARATOS DOMÉSTICOS AL INTERNET

Ciudad de México.
28 de julio de 2021

www.inai.org.mx

- **Algunos dispositivos utilizan sensores de red, bluetooth o Wifi y pueden detectar, almacenar, procesar o transmitir información personal**
- **El Instituto emite 10 recomendaciones para proteger datos personales de usuarios del llamado Internet de las Cosas**

INAI ADVIERTE RIESGOS A LA PRIVACIDAD POR CONEXIÓN DE APARATOS DOMÉSTICOS AL INTERNET

Los aparatos electrónicos que usan tecnología denominada Internet de las Cosas (*IoT*, por sus siglas en inglés) y que son dispositivos de uso cotidiano conectados entre sí por medio de la red, tratan datos personales y pueden representar un riesgo a la privacidad, advierte el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Actualmente, existen timbres que permiten hablar con la persona que toca y abrir, sin estar en casa; aspiradoras que comienzan a limpiar cuando el celular se los indica, aun a kilómetros de distancia; también hay cepillos dentales que pueden detectar caries, como ejemplos de la infinidad de dispositivos que utilizan sensores de red, *bluetooth* o *Wifi*, para conectarse en cualquier momento y mantener un monitoreo y control total de los procesos que cada uno realiza.

Al mismo tiempo, estas máquinas pueden detectar, almacenar, procesar o transmitir información personal, a través de una interconexión de internet, como el estado de salud, datos biométricos, hábitos y consumos, entre otros.

Hasta ahora no se encuentran definidos los requisitos mínimos de seguridad que deben cumplir los fabricantes de equipos *IoT*, por ello, la información que almacenen puede ser utilizada para generar patrones de conducta o consumo, pero también puede ser captada por ciberdelincuentes, si no se siguen las medidas de seguridad adecuadas.

En este contexto, el INAI recomienda a los usuarios de aparatos con tecnología *IoT*:

1. Verificar el tipo y cantidad de datos que obtienen los dispositivos inteligentes.

2. Modificar la configuración en función de las necesidades del usuario, conservando siempre las medidas de seguridad instaladas por defecto.

3. Revisar quién o quiénes tienen acceso a la información recabada o si existe la posibilidad de un acceso remoto a ellos, configurando los parámetros de seguridad convenientes.

4. Leer las condiciones de uso y almacenamiento de la información, considerando que pueden recoger datos, procesarlos y compartirlos.

5. Informarse antes de comprar un dispositivo y adquirir los que resulten más seguros, por ejemplo: aquellos que permitan actualizaciones de seguridad, y faciliten el borrado de datos personales cuando sean desechados o transferidos a otro propietario.

6. Cambiar las contraseñas de fábrica y establecer unas seguras, que contengan más de 8 caracteres en letras minúsculas y mayúsculas, dígitos y caracteres especiales.

7. Habilitar el acceso a internet solo cuando sea necesario y en redes que sean seguras.

8. Instalar aplicaciones desde los canales oficiales facilitados por los fabricantes.

9. Mantener actualizado el software del dispositivo, para contar con los parches más recientes, provistos por el fabricante y asegurar que sean remediadas las vulnerabilidades conocidas.

10. Evitar vincular el dispositivo inteligente a otros aparatos de los que se desconoce su nivel de seguridad.

-o0o-

 VER IMAGEN