

RIESGOS DEL INTERNET DE LAS COSAS EN EL HOGAR

Televisores, juguetes, robots aspiradores, bombillas, alarmas, altavoces o timbres son solo algunos ejemplos de dispositivos que pueden funcionar conectados a Internet.

Cuando utilizamos dispositivos inteligentes en casa podemos incurrir en algunos riesgos para nuestra privacidad y la de quienes conviven con nosotros o nos visitan. Conocerlos es clave para evitarlos.



El dispositivo no distingue quién es su usuario: puede captar y almacenar voces/imágenes/información de personas sin su conocimiento (familiares, invitados...)



Además de los datos que facilitamos directa y conscientemente, los dispositivos incorporan sensores para captar y almacenar otros datos como imágenes y audio.



Muchas empresas que participan en la prestación del servicio (fabricante del dispositivo, desarrolladores de software, prestadores de servicio, etc.) podrían tener acceso a nuestros datos y tratarlos para finalidades ulteriores.



Combinando los datos recogidos con la información de otros usuarios es posible deducir información relativa a nuestros hábitos, comportamiento y/o estado físico.



Algunos dispositivos pueden rastrear nuestros movimientos y como mínimo pueden localizarnos en lugares concretos durante ciertos periodos de tiempo.



El volumen de datos recogido y la combinación de información de varios dispositivos permite elaborar perfiles precisos en función de nuestros hábitos, preferencias y el uso que hacemos de los dispositivos.



Incluso cuando no estamos interactuando directa y conscientemente con el dispositivo, éste puede continuar capturando y tratando datos personales.



Un dispositivo conectado a Internet con configuraciones inseguras, por defecto o vulnerabilidades no solucionadas puede convertirse en la puerta de acceso de ciberdelincuentes a nuestros datos personales.



Los datos personales son tratados por terceros que, en caso de sufrir una brecha de seguridad, pueden ser expuestos.

RECOMENDACIONES PARA EL USO SEGURO DEL INTERNET DE LAS COSAS

Sigue estas recomendaciones para mejorar tu privacidad si utilizas dispositivos inteligentes:

- El derecho fundamental a la protección de datos también depende de ti:
 - Piensa qué datos son necesarios para cada dispositivo; no facilites más datos de los necesarios.
 - Revisa la información que te ofrece el fabricante y si tienes dudas consulta con su delegado de protección de datos.
 - Otorga tu consentimiento solo para las finalidades que se ajusten a tus preferencias y necesidades.
- Elije productos de fabricantes o proveedores que ofrezcan garantías de privacidad y protección de datos, y aquellos que se comprometan a proporcionar actualizaciones de seguridad durante la vida útil del producto.
- Antes** de adquirir el producto infórmate a través de las políticas de privacidad de:
 - Quién va a tratar tus datos personales y cómo puedes contactar con el delegado de protección de datos,
 - Qué tipos de datos van a ser tratados y con qué finalidades,
 - Si se comunicarán tus datos personales a terceros y con qué finalidades,
 - Forma de ejercer **tus derechos** de protección de datos incluido tu **derecho a la portabilidad** de tus datos.
- Durante la puesta en marcha** asegúrate de revisar y configurar tus preferencias y las **opciones de privacidad y seguridad**. Debes poder otorgar tu consentimiento o expresar tu **oposición** a las distintas finalidades. Cambia **usuarios y contraseñas** que vengán establecidas por defecto. Asegúrate de actualizar el dispositivo. Desactiva las funcionalidades que no vayas a usar.
- Mientras tengas el dispositivo** en uso:
 - Comprueba que el dispositivo se puede desconectar cuando no lo estás usando, y utiliza el modo que permite deshabilitar la captura de datos.
 - Revisa periódicamente las opciones de privacidad y seguridad.
 - Instala las actualizaciones de seguridad disponibles.
- Cuando dejes de utilizar** el dispositivo definitivamente:
 - No mantengas conectado a Internet un dispositivo obsoleto, en desuso o sin actualizar.
 - Tienes derecho a solicitar la supresión de tus datos personales y es conveniente eliminar las cuentas de usuario en aquellos proveedores de servicio que no vayas a continuar utilizando.
 - También puedes ejercer tu **derecho a la portabilidad**.
 - Borra los datos que pueda contener el dispositivo **antes de venderlo o reciclarlo**.