



CIBERCONSEJOS PARA PROTEGER TUS DISPOSITIVOS IoT

Si al salir de tu casa utilizas dispositivos inteligentes para protegerla, es importante que sepas que también debes cuidar este tipo de equipos, ya que existen diversos riesgos a los que estamos expuestos, como por ejemplo, secuestro de los dispositivos, robo de información o problemas de privacidad. Tanto las cámaras, relojes, cerraduras, micrófonos, entre otros aparatos, son vulnerables, por lo que es fundamental implementar medidas básicas de seguridad para resguardar los datos y evitar que los ciberdelincuentes accedan a los dispositivos que usamos para vigilar nuestro hogar. Para que en estas vacaciones salgas aún más tranquilo, el CSIRT de Gobierno entrega una serie de recomendaciones que te enseñarán a cómo proteger tus dispositivos IoT.



Peligros del IoT

- **Infección con malware:** Sus consecuencias pueden ser múltiples: robo de datos personales o sensibles, pérdida del control del equipo, encriptación de archivos, entre otras amenazas.
- **Robos:** Toda la información que recopilan los IoT es atractiva para los ciberdelincuentes: conocer nuestros movimientos, almacenar contraseñas, documentos de identidad, datos de tarjetas de crédito, etc.



Peligros del IoT

- **Problemas de privacidad:** Los IoT recopilan muchos datos, los que son enviados al fabricante y, en ocasiones, la información la comparten o se vende a terceros.
- **Secuestro de dispositivos:** Es posible perder el control de las cámaras, altavoces u otro, para causar algún problema de seguridad, espiar a un usuario, dar órdenes a otro dispositivo o pedir un rescate económico.



Recomendaciones de seguridad para dispositivos IoT

- 1.- **REVISA** siempre antes de comprar. Si el dispositivo cuenta con una política de protección de datos personales y léelo detalladamente.
- 2.- **SIEMPRE** compra equipos que cuenten con algún tipo de encriptación de datos.
- 3.- **CREA** contraseñas seguras, robustas y diferentes para cada dispositivo que lo permita.



Recomendaciones de seguridad para dispositivos IoT

- 3.- **ACTIVA** el doble factor de autenticación u opciones de acceso biométrico si el dispositivo cuenta con esa opción.
- 4.- **OCULTA** el nombre de la red inalámbrica a la cual se conectan los dispositivos.
- 5.- **CONFIGURA** los dispositivos en modo privado y desactiva aquellas funciones que no son necesarias para su funcionamiento.



Recomendaciones de seguridad para dispositivos IoT

- 6.- **MANTÉN** actualizados los programas de los dispositivos, en caso de ser posible.
- 7.- **INSTALA** softwares oficiales.
- 8.- **UTILIZA** programas de antivirus y antimalware.