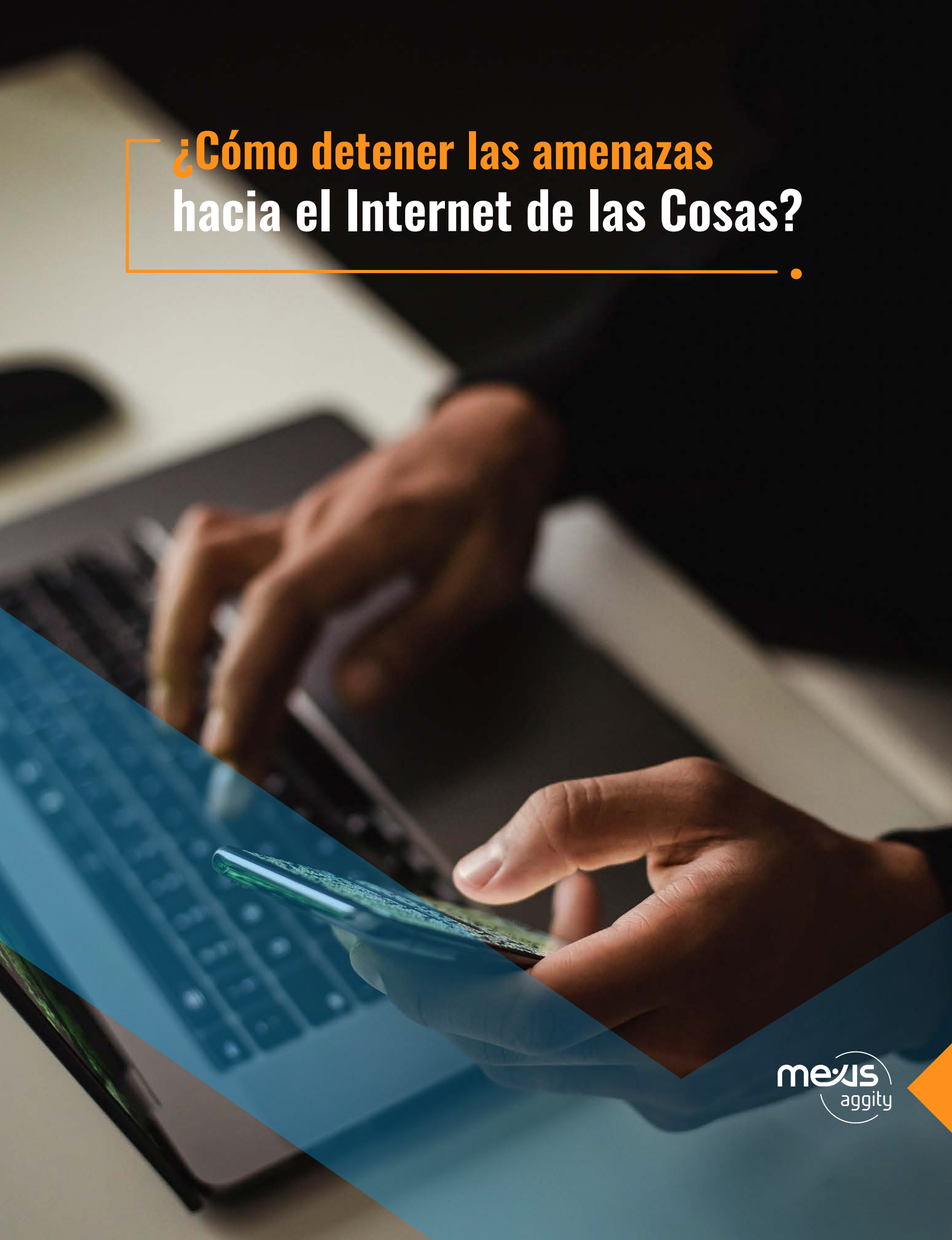
# ¿Cómo detener las amenazas hacia el Internet de las Cosas?



El Internet de las Cosas **(IoT)** implica conectar a la Red una amplia variedad de dispositivos, incluidos productos de consumo, automóviles, componentes industriales y de servicios públicos, sensores y otros objetos cotidianos. Estos han sido equipados con conectividad a Internet para la recopilación, intercambio y procesamiento de datos.

Entre estos dispositivos, los más utilizados son relojes inteligentes, consolas de videojuegos, televisores inteligentes, dispositivos controlados por voz (como Amazon Alexa), impresoras, cámaras, termostatos y sistemas de alarmas. Menos usados, pero aumentando su popularidad, están los equipos de aptitud física, vehículos y marcos de fotos digitales. Y, finalmente, equipos industriales, que permiten automatizar procesos de minería, manufactura, energía eléctrica, y otras.

"Cualquier dispositivo conectado a internet es propenso a ser atacado. En general, un delincuente puede intervenir, sin autorización, sus funcionalidades 'inteligentes': recopilación, intercambio y procesamiento de datos", dijo Josué Ariza, gerente de Ventas para BeyondTrust. Eventualmente, estas intervenciones podrían permitir a los atacantes moverse a otros sistemas. Esto último es muy común, pues usan estos dispositivos IoT como eslabones más débiles para acceder a otros sistemas más importantes.

Se planteó algunas preguntas y respuestas más importantes que debemos saber con respecto a las amenazas que realizan los delincuentes a dispositivos que comúnmente no creemos que puedan llegar a ser atacados.

## ¿Qué tan difícil es lograr acceder de manera fraudulenta a ellos?

Comparado con otros sistemas más completos, **es más fácil acceder sin autorización a los dispositivos IoT.** Estos dispositivos son generalmente de propósito específico, diseñados y producidos para pocas funciones. Esto incluye el hardware y software, y es común encontrar un enfoque en conveniencia de uso y producción masiva de los mismos, dejando a un lado mejores prácticas de desarrollo de software y de seguridad.

## Qué tipo de ataques pueden recibir?

Concretamente, los atacantes pueden intentar explotar debilidades en el mismo dispositivo físico, en los canales de comunicación utilizados por estos dispositivos, o en el software y las aplicaciones presentes en estos. Podrían acceder a los datos pasivamente (cómo ver lo que está grabando una cámara de seguridad o la ubicación geográfica de un dispositivo), o incluso controlarlo remotamente **(cambiar configuraciones o directamente controlar sus funcionalidades).**

## ¿Cómo se pueden prevenir los ataques?

Como usuarios consumidores finales de estos dispositivos, lo mejor es mantener actualizado el software de los mismos. En este caso, se depende del fabricante del dispositivo para que desarrolle parches de seguridad. “Los usuarios más avanzados, en redes de hogar o empresariales, se deben tomar estrategias de seguridad informática como comenzar con la arquitectura de la red a la que están conectados estos dispositivos, agrupando y aislando diferentes dispositivos, y llegando a incluir controles de red como un IPS (Intrusion Prevention System)”, afirmó Josué Ariza.

Otra acción que se realiza es un inventario centralizado de todos los dispositivos, preferiblemente con un proceso de descubrimiento de dispositivos conectados a las diferentes redes, y de vulnerabilidades en cada uno. En redes empresariales, el programa de seguridad informática debe tomar en consideración los riesgos asociados a los dispositivos IoT requeridos por la organización, siguiendo marcos de trabajos adecuados para la misma.

## ¿Qué tan recurrente es el hackeo de carros?

Cada vez es más común encontrar vulnerabilidades en diferentes tipos de vehículos. Estas podrían permitir rastreo, detección y control remoto sin autorización. También va en aumento la cantidad de software en los vehículos, para diferentes funcionalidades internas o de comunicación con sistemas externos. Se ha encontrado también que algunos fabricantes de vehículos utilizan APIs (Application Programming Interface – o Interfaz de Programación de Aplicaciones) de terceros, en lugar de desarrollar las suyas propias. Todo esto aumenta las probabilidades del hackeo de carros.

La exposición diaria a ciberataques es inminente, sin embargo, se pueden seguir los consejos anteriormente mencionados para prevenirlos. De igual manera, en el mercado existen diversas soluciones como Endpoint Privilege Management de la compañía BeyondTrust que detiene ataques maliciosos como malware y ransomware, ofreciendo seguridad de los datos, uno de los activos más valiosos de las compañías.

Fuente de información: cio.com.mx