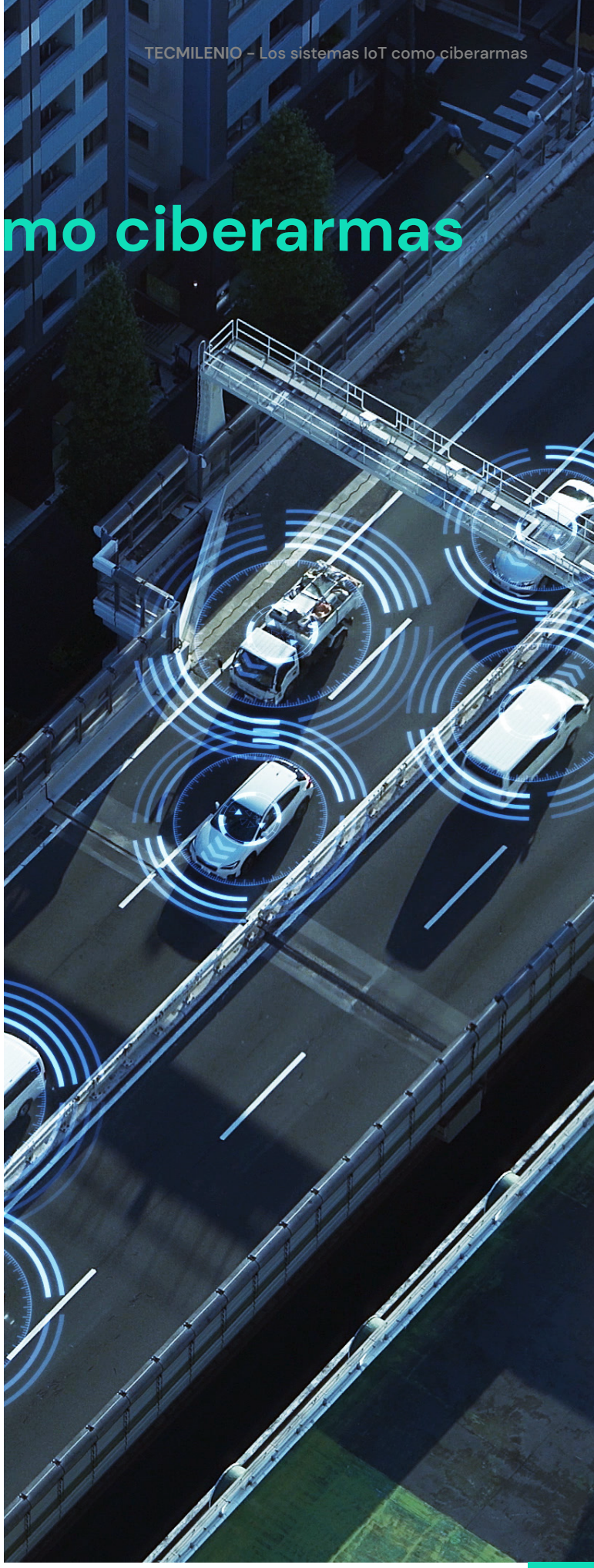
CENTRO
DE COMPETENCIAS
TECMILENIO

# Los sistemas IoT como ciberarmas

# Los sistemas IoT como ciberarmas



La idea de utilizar sistemas IoT como ciberarmas se ha vuelto cada vez más común en el mundo de la seguridad cibernética.

Fisher (2019): "El Internet de las cosas (IoT) está creciendo exponencialmente, pero mucha gente sigue sin ser consciente de los riesgos que suponen los dispositivos inteligentes".

A medida que los dispositivos IoT se vuelven cada vez más comunes en nuestra vida diaria, también se están convirtiendo en un objetivo atractivo para los ciberdelincuentes. Los dispositivos IoT a menudo tienen una seguridad más débil en comparación con otros dispositivos conectados a Internet, lo que los hace vulnerables a los ataques. Debido a que los dispositivos IoT son en su mayoría remotos, actualizar el software y firmware es un gran desafío, según Días (2023).

Además, muchos dispositivos IoT son fabricados por empresas que no tienen experiencia en seguridad cibernética, lo que resulta en dispositivos con vulnerabilidades conocidas que los ciberdelincuentes pueden explotar.

El número de dispositivos IoT crece de forma muy rápida, todo dispositivo IoT debe protegerse y sujetarse a mantenimiento constante, debido a que día a día se detectan nuevas vulnerabilidades en los sistemas IoT. Muchos de estos dispositivos no incluyen funciones de seguridad, por lo que son más susceptibles a algún ataque. E incluso cuando cuentan con funciones de seguridad, los usuarios no dedican el tiempo necesario para configurar dichos dispositivos y darles el mantenimiento adecuado, dejando abierta una puerta fácil de vulnerar a sus dispositivos IoT, según Fisher (2019).

Para prevenir estos ataques es importante que los fabricantes de dispositivos IoT mejoren la seguridad de sus productos y que los

usuarios tomen medidas para asegurar sus dispositivos, como cambiar las contraseñas predeterminadas y mantener sus dispositivos actualizados con los últimos parches de seguridad. También es importante que las empresas adopten políticas de seguridad sólidas para proteger sus redes y sistemas de los ataques que utilizan dispositivos IoT comprometidos.

También existe la posibilidad de que estos dispositivos sean utilizados para realizar acciones maliciosas en el mundo físico.

Por ejemplo, un atacante podría tomar el control de un dispositivo IoT en una fábrica y manipular sus ajustes para causar un mal funcionamiento en una máquina, lo que podría resultar en daños materiales y riesgos para la seguridad de los trabajadores.

Otro ejemplo podría ser el uso de dispositivos IoT en sistemas de transporte, como los sistemas de control de tráfico o los sistemas de control de semáforos, para causar accidentes o interrupciones en el tráfico.

Fisher (2019) señala: “La cámara de seguridad Nest es un objetivo frecuente para los hackers que quieren secuestrar dispositivos IoT. En una ocasión, alguien recibió una advertencia falsa sobre misiles balísticos y, en otra, se amenazó a una pareja con secuestrar a su bebé. En un tercer incidente, una voz surgió de la cámara, el hacker se hizo también con el control del termostato y elevó la temperatura de la casa por encima de los 30 °C”.

La mayoría de estas situaciones son debido al mal comportamiento del usuario con respecto a su seguridad. Al no utilizar contraseñas seguras, los hackers obtuvieron acceso al dispositivo IoT aprovechando las vulnerabilidades para causar daños.

Varios dispositivos IoT ofrecen autenticación de varios factores ( lo que supone una capa extra de seguridad), sin embargo los propietarios no siempre conocen esta posibilidad o no saben cómo se usa.

Dentro del hogar, una vez comprometido un dispositivo IoT, los hackers pueden recopilar datos y venderlos. Puesto que algunos dispositivos almacenan datos como claves de cifrado de números de tarjetas de crédito, contraseñas y mucha más información confidencial. Además de esto un hacker puede recopilar los movimientos de la fami-

lia y venderlos a alguien que quiera saber que hay dentro de su casa o en qué momentos está se queda vacía, según Fisher (2019).

Aunque las empresas también ignoran los riesgos de seguridad de IoT algunas veces. El sector de fabricación y sanitario son principalmente vulnerables al riesgo de pirateo y esto es muy grave debido a que cualquier ataque podría poner vidas en riesgo.

Para prevenir estos riesgos, es importante que los fabricantes de dispositivos IoT implementen medidas de seguridad robustas en sus productos y que los usuarios tomen medidas para proteger sus dispositivos, como cambiar las contraseñas predeterminadas y mantener sus dispositivos actualizados con los últimos parches de seguridad. Además, es importante que las empresas adopten políticas de seguridad sólidas y capaciten a sus empleados sobre las mejores prácticas de seguridad cibernética para garantizar la protección de sus sistemas y redes contra los ataques que utilizan dispositivos IoT comprometidos.

# Referencias bibliográficas


- Dias, L. (2023). *Proteger los dispositivos conectados a IoT hace que Internet sea más seguro*. Recuperado de https://technocio.com/proteger-los-dispositivos-conectados-a-iot-hace-que-internet-sea-mas-seguro/

- Fisher, S. (2019). *Riesgos de seguridad en el Internet de las cosas*. Recuperado de https://www.avast.com/es-es/c-iot-security-risks