Seguridad y privacidad en hogares inteligentes: un análisis documental de vulnerabilidades IoT

Rosa Leticia Ibarra Martínez1, Héctor Luis López López 2, Mónica del Carmén Olivarría González3, Rogelio Estrada Lizarraga4

1,2,3,4 Universidad Autónoma de Sinaloa, Facultad de Informática Mazatlán (MEXICO)

Resumen

El Internet de las Cosas (IoT) ha transformado los hogares mediante la incorporación de dispositivos inteligentes como cámaras IP, asistentes virtuales, sensores, cerraduras electrónicas y electrodomésticos conectados. Aunque estos dispositivos ofrecen beneficios en comodidad, automatización y eficiencia energética, su rápida expansión ha incrementado la superficie de exposición a vulnerabilidades que comprometen la seguridad y la privacidad de los usuarios. El presente artículo desarrolla un análisis documental basado en fuentes especializadas de organismos internacionales como OWASP, ENISA y NIST, así como reportes de ciberseguridad emitidos por Cisco, Kaspersky y Fortinet. Los resultados del análisis identifican vulnerabilidades comunes en hogares inteligentes relacionadas con autenticación débil, firmware desactualizado, cifrado insuficiente, puertos expuestos y uso de protocolos inseguros. Estas debilidades facilitan ataques como Man-in-the-Middle, sniffing, secuestro de dispositivos y conformación de botnets, los cuales pueden conducir a vigilancia no autorizada, exposición de datos personales, control remoto indebido e incluso riesgos físicos dentro del hogar. Asimismo, se revisan marcos normativos y estándares internacionales que orientan buenas prácticas de protección, destacando NIST IR 8259, OWASP IoT Top 10 y el GDPR. Finalmente, el artículo presenta recomendaciones basadas en literatura especializada para reducir la superficie de ataque, fortalecer la configuración de dispositivos y promover hábitos de ciberseguridad en usuarios domésticos. El estudio subraya la necesidad de abordar la seguridad IoT de manera integral para garantizar entornos domésticos seguros y resilientes.

Palabras clave: Ciberseguridad, Hogares inteligentes, Internet de las Cosas (IoT), Privacidad, Seguridad digital, Vulnerabilidades IoT.

Abstract

The Internet of Things (IoT) has transformed households through the incorporation of smart devices such as IP cameras, virtual assistants, sensors, electronic locks, and connected appliances. Although these devices provide benefits in comfort, automation, and energy efficiency, their rapid expansion has increased the exposure surface to vulnerabilities that compromise user security and privacy. This article presents a documentary analysis based on specialized sources from international organizations such as OWASP, ENISA, and NIST, as well as cybersecurity reports issued by Cisco, Kaspersky, and Fortinet. The analysis identifies common vulnerabilities in smart homes related to weak authentication, outdated firmware, insufficient encryption, exposed ports, and the use of insecure protocols. These weaknesses facilitate attacks such as Man-in-the-Middle, sniffing, device hijacking, and botnet formation, which can lead to unauthorized surveillance, exposure of personal data, remote control misuse, and even physical risks within the home. Regulatory frameworks and international standards guiding protection practices are also reviewed, highlighting NIST IR 8259, OWASP IoT Top 10, and the GDPR. Finally, the article presents recommendations based on specialized literature to reduce the attack surface, strengthen device configuration, and promote cybersecurity habits among domestic users. The study underscores the need to address IoT security comprehensively in order to ensure safe and resilient smart-home environments.

Keywords: Cybersecurity, Digital security, Internet of Things (IoT), Privacy, Smart homes, IoT vulnerabilities

# INTRODUCción

El Internet de las Cosas (IoT) ha experimentado un crecimiento acelerado en entornos domésticos, favoreciendo la incorporación de cámaras IP, sensores, asistentes virtuales, electrodomésticos conectados y dispositivos de automatización que incrementan la comodidad y la eficiencia energética del hogar [1]. Sin embargo, distintos organismos han advertido que la rápida expansión del IoT ha incrementado también la superficie de exposición a vulnerabilidades, debido a fallas de autenticación, firmware obsoleto, protocolos inseguros y limitada cultura de seguridad entre los usuarios [2], [3].

La Agencia Europea de Ciberseguridad (ENISA) identifica que los hogares inteligentes son uno de los entornos más vulnerables, ya que muchos dispositivos carecen de prácticas mínimas de protección incorporadas desde fábrica [3]. Asimismo, reportes de empresas como Kaspersky y Fortinet evidencian un incremento sostenido en ataques dirigidos a cámaras IP, asistentes de voz y routers domésticos [4], [5]. Estas condiciones hacen necesario analizar las vulnerabilidades más frecuentes en dispositivos IoT domésticos y sus implicaciones en la privacidad familia.

En consecuencia, este artículo desarrolla un **análisis documental** que reúne evidencia científica, técnica y normativa sobre vulnerabilidades IoT en hogares inteligentes, ataques comunes y medidas de mitigación recomendadas. Este análisis, sustentado en fuentes de OWASP, NIST, ENISA e IEEE, permite comprender el estado actual de la seguridad IoT sin recurrir a métodos empíricos o recolección de datos primaria.

# METODOLOGÍA

## ****Enfoque del estudio****

El presente trabajo adopta un enfoque estrictamente documental basado en el análisis, contrastación y síntesis de literatura científica, normativa y técnica relacionada con la seguridad del Internet de las Cosas (IoT) en entornos domésticos. Este enfoque permite reunir evidencia actualizada sin recurrir a instrumentos empíricos, privilegiando fuentes provenientes de organismos internacionales, reportes técnicos de ciberseguridad y artículos científicos especializados publicados entre 2018 y 2024 [1],[14].

## ****Estrategia de búsqueda de información****

La búsqueda de información se realizó mediante una revisión sistemática de documentos disponibles en bases académicas de alto impacto como IEEE Xplore, Scopus y ScienceDirect, así como en repositorios institucionales y sitios oficiales de organismos normativos. Se emplearon combinaciones de palabras clave como IoT vulnerabilities, smart home security, privacy IoT, router attacks, IoT botnets, home cybersecurity y IoT privacy frameworks. Esta estrategia permitió identificar literatura pertinente en torno a vulnerabilidades frecuentes, tipos de ataques, implicaciones de privacidad y marcos regulatorios aplicables. Adicionalmente, se consultaron reportes especializados de organizaciones reconocidas en ciberseguridad como OWASP, NIST, ENISA, Kaspersky, Fortinet, Cisco Talos y Symantec, así como documentos centrados en riesgos de privacidad elaborados por Mozilla y la Comisión Federal de Comercio de los Estados Unidos [1], [3], [4], [5], [6], [7], [8], [9], [10].

## ****Criterios de selección y análisis****

La selección de documentos se basó en cinco criterios: actualidad (publicaciones de 2018 a 2024), pertinencia temática (IoT doméstico), validez técnica (documentos emitidos por organismos reconocidos), exhaustividad (información sobre vulnerabilidades, ataques o normativas), y disponibilidad pública para su verificación. Los textos seleccionados fueron organizados en categorías analíticas según tipo de vulnerabilidad, naturaleza del ataque, impacto en privacidad y seguridad, y recomendaciones técnicas. Posteriormente, se aplicó un proceso de análisis comparativo que permitió identificar tendencias recurrentes en la literatura técnica y normativas internacionales, así como patrones en el comportamiento de amenazas IoT domésticas documentadas en diferentes regiones [3],[6].

## ****Procedimiento de revisión documental****

El procedimiento metodológico se desarrolló en cuatro etapas: (1) identificación de fuentes primarias y secundarias; (2) revisión crítica del contenido técnico y normativo; (3) clasificación temática; y (4) síntesis argumentativa. En la primera etapa se recopilaron documentos oficiales de organismos de ciberseguridad como OWASP, NIST, ENISA y Symantec, así como informes de empresas de seguridad informática reconocidas. En la segunda etapa se revisaron los elementos clave de cada documento, identificando conceptos, vulnerabilidades, hallazgos técnicos y recomendaciones. En la tercera etapa se organizaron los contenidos en categorías operativas: vulnerabilidades, ataques, impactos, marcos normativos y medidas de mitigación. Finalmente, en la etapa de síntesis se integraron hallazgos de distintas fuentes para elaborar una interpretación crítica que refleja la situación actual de la seguridad IoT en hogares inteligentes.

## ****Limitaciones del estudio****

Al tratarse de un análisis documental, el estudio presenta limitaciones inherentes a la ausencia de trabajo empírico directo. No se realizaron experimentos controlados, pruebas de penetración ni mediciones técnicas en dispositivos reales, por lo que los hallazgos dependen exclusivamente de las fuentes consultadas. Asimismo, la disponibilidad de información reciente varía según la organización; por ejemplo, algunos reportes de Cisco Talos y Symantec no se publican anualmente o no incluyen datos específicos sobre IoT doméstico [6], [8]. Otra limitación es que la normativa mexicana en materia de privacidad (LFPDPPP) aún no aborda de manera explícita escenarios de IoT, lo que deja vacíos normativos que dificultan el análisis local [12]. Finalmente, debido a la rápida evolución de amenazas, es posible que nuevos ataques o vulnerabilidades emergentes no estén reflejados en la literatura disponible al momento de la revisión.

# RESULTADOS

## Vulnerabilidades comunes en dispositivos IoT domésticos

Diversos estudios coinciden en que la mayoría de los dispositivos IoT domésticos presentan debilidades de autenticación, especialmente contraseñas predeterminadas o simples que son fáciles de adivinar o de vulnerar por fuerza bruta [1]. Asimismo, el firmware desactualizado es una de las vulnerabilidades más extendidas: Diversos estudios reportan que una proporción muy elevada de dispositivos IoT en el mercado no recibe actualizaciones regulares de firmware, lo que mantiene expuestas vulnerabilidades conocidas [1], [4].

El cifrado insuficiente también constituye un riesgo recurrente. ENISA advierte que numerosos dispositivos transmiten datos sensibles como imágenes, comandos o información del usuario, sin cifrado TLS adecuado, facilitando ataques de interceptación [3]. Otro elemento crítico es la exposición de puertos y servicios por defecto, muchas veces no documentados, lo que permite accesos remotos no autorizados [2], [6]. Finalmente, el uso de protocolos inseguros como MQTT sin TLS o UPnP mal configurado incrementa la posibilidad de ataques [7].

Tabla 1 Vulnerabilidades frecuentes en IoT doméstico

|  |  |
| --- | --- |
| Vulnerabilidad | Descripción |
| Autenticación débil | Ocurre cuando los dispositivos utilizan contraseñas predeterminadas o fáciles de adivinar, sin mecanismos robustos de autenticación, lo que permite accesos remotos no autorizados. |
| Firmware obsoleto | El dispositivo no recibe actualizaciones de seguridad, por lo que mantiene fallas conocidas que pueden ser explotadas para tomar control o acceder a datos internos. |
| Cifrado insuficiente | Los datos transmitidos (audio, video, comandos o información personal) no están protegidos mediante cifrado fuerte, facilitando su interceptación por atacantes. |
| Puertos expuestos | El dispositivo mantiene abiertos puertos o servicios de red innecesarios o no configurados adecuadamente, permitiendo entradas no autorizadas desde internet. |
| Protocolos inseguros  (MQTT, UPnP) | Algunos dispositivos utilizan protocolos sin cifrado o con configuraciones vulnerables, lo que permite la manipulación de datos o el control del dispositivo desde el exterior |

## Tipos de ataques frecuentes en hogares inteligentes

Las vulnerabilidades descritas permiten diversos tipos de ataques. Los ataques Man-in-the-Middle (MITM) se han vuelto frecuentes, ya que permiten interceptar comunicaciones entre dispositivos y routers domésticos, comprometiendo datos en tránsito [8]. Los ataques de sniffing afectan especialmente a cámaras IP y dispositivos con micrófonos, permitiendo a un atacante visualizar u oír lo que ocurre en el hogar [4].

Asimismo, el device hijacking o secuestro de dispositivos ocurre cuando un atacante toma control de cámaras, focos o sensores mediante credenciales comprometidas. La botnet Mirai demostró la facilidad con la que miles de dispositivos IoT vulnerables pueden integrarse para lanzar ataques DDoS masivos [7]. Finalmente, la suplantación del dispositivo mediante clonación o inyección de comandos constituye una amenaza latente con implicaciones directas en la seguridad física del hogar [6].

A continuación, se presenta una tabla que resume y agrupa los tipos de ataques más comunes dirigidos a dispositivos del Internet de las Cosas en entornos domésticos, junto con sus principales impactos digitales, ejemplos documentados en la literatura especializada y las referencias correspondientes. Esta síntesis permite visualizar de manera clara la relación entre las vulnerabilidades explotadas y las consecuencias que pueden afectar la seguridad y la privacidad del hogar inteligente.

Tabla 2 Tipos de ataques y daños digitales

|  |  |  |
| --- | --- | --- |
| Tipo de ataque | Impacto principal | Ejemplo real |
| Botnets basadas en IoT (ej. Mirai) | Congestión de red, DDoS masivos, control remoto de miles de dispositivos vulnerables. | Variante de Mirai utilizada en ataques globales contra servicios web y cámaras IP vulnerables. |
| Secuestro de cámaras IP (Hijacking) | Acceso no autorizado a video, vigilancia encubierta, violación severa de la privacidad. | Accesos remotos a cámaras mediante credenciales por defecto documentados por Kaspersky. |
| Man-in-the-Middle (MITM) | Interceptación de datos, modificación de tráfico y robo de información personal. | Ataques MITM en asistentes inteligentes y routers domésticos sin cifrado adecuado. |
| Sniffing de tráfico IoT | Captura de audio, video o datos sensibles transmitidos sin cifrado. | Interceptación de transmisiones de cámaras y dispositivos con WiFi inseguro. |
| Explotación de protocolos inseguros (MQTT, UPnP) | Manipulación de dispositivos, inyección de comandos, exposición de servicios internos. | Uso de UPnP mal configurado para comprometer routers domésticos. |
| Acceso por contraseñas débiles o por defecto | Toma de control total del dispositivo, inclusión en botnets o acceso lateral a la red. | Acceso no autorizado a cámaras y smart locks por contraseñas predeterminadas. |
| Ataques a routers domésticos | Compromiso de la red completa, vigilancia, redirección de tráfico y apertura de puertos. | Vulnerabilidades documentadas en routers domésticos por Cisco Talos. |

Ejemplos de estos ataques han sido documentados en los informes de ENISA, Fortinet, Kaspersky y Cisco Talos [3],[6].

La evolución temporal de los ataques dirigidos a dispositivos del Internet de las Cosas evidencia una tendencia ascendente tanto en frecuencia como en sofisticación, lo cual refuerza los patrones identificados en la tabla anterior sobre los tipos de ataques y sus daños digitales asociados. Mientras que en los primeros años predominaban amenazas como las botnets basadas en variantes de Mirai, con el tiempo se han intensificado ataques orientados a vulnerar dispositivos específicos del hogar, como cámaras IP y routers domésticos, así como técnicas más avanzadas como los ataques Man-in-the-Middle y la explotación de protocolos inseguros. A partir de 2023 y proyectándose hacia 2025, la literatura especializada muestra una mayor presencia de intrusiones automatizadas mediante inteligencia artificial, lo que anticipa un incremento significativo en el riesgo para los hogares inteligentes. La figura siguiente sintetiza esta progresión histórica y permite observar cómo los vectores de ataque han evolucionado desde mecanismos relativamente simples hasta técnicas de alto impacto apoyadas en capacidades predictivas y automatizadas.

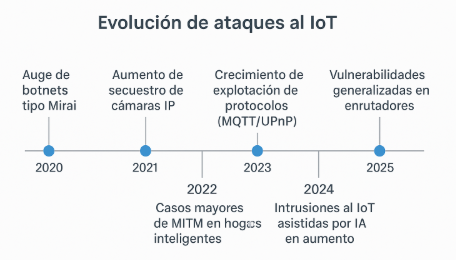


Figura 1 Evolución de ataques al IoT.

## Impacto en la privacidad y seguridad del hogar

La explotación de dispositivos IoT vulnerables puede generar consecuencias significativas tanto en el ámbito digital como en la esfera personal de los usuarios. La exposición de datos sensibles, como imágenes, audios, historiales de uso o patrones de comportamiento, constituye uno de los riesgos más documentados por organismos internacionales, dado que permite la elaboración de perfiles detallados e invasivos sobre la vida cotidiana de los habitantes [9], [10]. Asimismo, la manipulación remota no autorizada de cerraduras electrónicas, asistentes virtuales, cámaras o sistemas de alarma puede derivar en riesgos físicos directos, incrementando la posibilidad de allanamientos, extorsión o vigilancia encubierta dentro del hogar [13].



Figura 2 Privacidad y seguridad del Hogar.

El riesgo se intensifica debido a la interconexión inherente del ecosistema doméstico, ya que numerosos dispositivos comparten la misma red local. Esta condición facilita el movimiento lateral del atacante, permitiendo comprometer computadoras, teléfonos móviles o equipos de almacenamiento personal, aunque el ataque inicial haya ocurrido en un sensor, cámara o electrodoméstico inteligente [5]. Informes recientes muestran que las botnets que operan sobre dispositivos IoT continúan creciendo, favorecidas por credenciales débiles, firmware obsoleto y configuraciones por defecto, lo que incrementa la probabilidad de secuestro de dispositivos, espionaje en tiempo real y uso ilícito de recursos computacionales [14].

Adicionalmente, la falta de transparencia en los modelos de tratamiento de datos, políticas poco claras sobre retención de información y transferencias a terceros representan riesgos jurídicos y éticos relevantes, especialmente cuando los usuarios desconocen qué información recopilan sus dispositivos, con qué fines y durante cuánto tiempo será almacenada [13]. En este sentido, la protección de la privacidad en hogares inteligentes no solo depende de medidas técnicas, sino también de prácticas regulatorias y de alfabetización digital que permitan a los usuarios comprender y gestionar de manera informada los riesgos asociados.

## Marcos normativos y estándares internacionales

El marco normativo internacional proporciona fundamentos esenciales para comprender el alcance y las obligaciones en materia de seguridad del Internet de las Cosas (IoT), orientando tanto a fabricantes como a usuarios finales en la adopción de medidas preventivas. El documento NIST IR 8259 establece un conjunto de actividades básicas de ciberseguridad que deben considerarse desde la fabricación del dispositivo, tales como la gestión de identidades, actualizaciones seguras, protección del software embebido y documentación transparente sobre configuraciones recomendadas [2]. Este estándar es particularmente relevante porque define responsabilidades mínimas para los desarrolladores, reduciendo así el riesgo de vulnerabilidades heredadas.

Por su parte, el OWASP IoT Top 10 constituye una de las clasificaciones más influyentes sobre vulnerabilidades críticas en el ecosistema IoT, destacando riesgos como la autenticación débil, la falta de cifrado, las actualizaciones inseguras y la exposición de servicios de red [1]. De forma complementaria, la ENISA, a través de su *Threat Landscape for IoT*, presenta un análisis exhaustivo de amenazas emergentes y tendencias en ciberataques que afectan a dispositivos domésticos, industriales y urbanos, subrayando la rápida evolución de botnets, fallas en protocolos y explotación de configuraciones predeterminadas [3].

En cuanto al ámbito de protección de datos, el GDPR establece principios de transparencia, minimización de datos y responsabilidad proactiva, lo cual afecta directamente a los dispositivos que recopilan información sensible en el hogar inteligente [11]. En el caso de México, [12] la LFPDPPP determina obligaciones para el tratamiento de datos personales, aunque aún no incorpora de manera específica lineamientos orientados al IoT doméstico, lo que deja un vacío normativo que se vuelve relevante ante el crecimiento acelerado de estos dispositivos. No obstante, la aplicación de sus principios generales sigue siendo fundamental para asegurar prácticas adecuadas de manejo de datos personales.

## Recomendaciones de mitigación basadas en literatura

La literatura revisada coincide en que la mitigación efectiva de riesgos en entornos IoT domésticos requiere una combinación de medidas técnicas, organizativas y de configuración. Una de las acciones más recurrentes es cambiar inmediatamente las contraseñas predeterminadas por credenciales robustas y únicas, ya que dichas contraseñas representan uno de los vectores de ataque más frecuentemente explotados por botnets y actores maliciosos [2], [3]. También se destaca la importancia de mantener actualizado el firmware, dado que muchos dispositivos dejan de recibir soporte y actualizaciones, lo que expone vulnerabilidades conocidas que pueden ser aprovechadas durante largos periodos.

Otra medida ampliamente recomendada es la segmentación de la red doméstica, separando los dispositivos IoT del resto de equipos principales (computadoras, teléfonos, servidores personales). Esto limita el impacto de un ataque y reduce la probabilidad de movimientos laterales dentro de la red [5]. Asimismo, se recomienda verificar que las comunicaciones estén protegidas mediante cifrado TLS u otros protocolos seguros, ya que la falta de cifrado continúa siendo una de las debilidades más comunes identificadas por estudios internacionales [2], [3].

Organizaciones como OWASP resaltan la necesidad de revisar continuamente las configuraciones del dispositivo, permisos, puertos abiertos y servicios habilitados, ya que muchos productos incluyen funcionalidades innecesarias que amplían la superficie de ataque [1]. Finalmente, tanto Kaspersky como Fortinet subrayan el papel central del router doméstico como punto crítico de seguridad, recomendando su actualización frecuente, la desactivación de interfaces de administración remota no utilizadas y la adopción de configuraciones seguras de red [4], [5]. En conjunto, estas acciones conforman una estrategia integral que contribuye a fortalecer la seguridad general del ecosistema IoT.

Con el fin de integrar de manera estructurada las medidas de mitigación más relevantes, se incluye a continuación una tabla comparativa que agrupa las acciones recomendadas en función de su propósito, alcance y nivel de impacto. Esta síntesis facilita la comprensión de cómo cada medida contribuye a reducir riesgos específicos dentro del ecosistema IoT doméstico, ofreciendo una visión clara y ordenada de las estrategias que la literatura especializada considera fundamentales para mejorar la seguridad y privacidad en los hogares inteligentes.

Tabla 3 Medidas de mitigación IoT y su propósito

|  |  |  |  |
| --- | --- | --- | --- |
| Medida de mitigación | Descripción técnica | Propósito principal | Riesgo mitigado |
| Cambio de contraseñas predeterminadas | Sustitución de contraseñas por credenciales robustas y únicas. | Reducir accesos no autorizados derivados de credenciales débiles. | Fuerza bruta, hijacking. |
| Actualización periódica de firmware | Instalación de parches y mejoras del fabricante. | Corregir vulnerabilidades conocidas y mejorar estabilidad del sistema. | Explotación de fallas, malware IoT. |
| Segmentación de la red doméstica | Separación de red principal y red IoT en diferentes VLAN o SSID. | Limitar el movimiento lateral del atacante. | Compromiso global de la red. |
| Activación de cifrado TLS/HTTPS | Asegurar que las transmisiones del dispositivo estén cifradas. | Proteger datos en tránsito contra interceptación. | MITM, sniffing. |
| Revisión de puertos abiertos y servicios | Auditoría de configuraciones, protocolos y permisos habilitados. | Reducir superficie de ataque y accesos no documentados. | Exposición de puertos, explotación remota. |
| Configuración segura del router | Ajustes de seguridad, desactivar administración remota, cambiar claves. | Fortalecer el punto crítico de entrada a la red doméstica. | Secuestro del router, control total de red. |

En conjunto, las medidas descritas reflejan un consenso sólido en la literatura especializada respecto a la necesidad de adoptar estrategias preventivas, continuas y contextualizadas para fortalecer la seguridad de los hogares inteligentes. Su aplicación sistemática permite reducir la superficie de ataque, limitar posibles afectaciones a la privacidad y garantizar entornos domésticos más resilientes frente a amenazas emergentes del ecosistema IoT.

# CONCLUSIONes

El análisis documental demuestra que los hogares inteligentes presentan vulnerabilidades significativas debido a fallas técnicas de los dispositivos, configuraciones inseguras y limitada cultura de ciberseguridad. Estas debilidades facilitan ataques como interceptación de comunicaciones, secuestro de dispositivos y conformación de botnets, con impactos que comprometen tanto la privacidad como la seguridad física del hogar.

Asimismo, los marcos normativos internacionales y las buenas prácticas propuestas por OWASP, NIST y ENISA ofrecen referencias esenciales para fortalecer la protección de los hogares conectados. La adopción de medidas preventivas, junto con la concientización del usuario, constituye un elemento clave para reducir la superficie de ataque en entornos domésticos.

La seguridad en hogares inteligentes depende de la colaboración entre fabricantes, usuarios y reguladores. Las vulnerabilidades más críticas surgen de la falta de actualizaciones, autenticación débil y desconocimiento del usuario. La adopción de tecnologías como cifrado avanzado, detección de intrusos y blockchain, junto con la educación del usuario, es esencial para mitigar riesgos y proteger la privacidad y seguridad en el entorno doméstico conectado.

referencias

1. OWASP Foundation, “OWASP IoT Top 10,” 2023. [Online]. Available: https://owasp.org/www-project-internet-of-things/
2. NIST, “Foundational Cybersecurity Activities for IoT Device Manufacturers”, NIST Internal Report 8259, 2020. [Online]. Available: <https://doi.org/10.6028/NIST.IR.8259>
3. ENISA, “Threat Landscape for IoT and Smart Devices”, European Union Agency for Cybersecurity, 2022. [Online]. Available: <https://www.enisa.europa.eu>
4. Kaspersky, “Kaspersky unveils an overview of IoT-related threats in 2023”, 2023. [Online]. Available: https://www.kaspersky.com/about/press-releases/kaspersky-releases-overview-of-iot-related-threats-in-2023
5. Fortinet Labs, “2022 IoT Threat Review,” FortiGuard Labs, 2023. [Online]. Available: https://www.fortinet.com/blog/threat-research/2022-iot-threat-review.
6. Cisco Talos, “*The Internet of Vulnerable Things”*, 2017.
7. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M., “*A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security*”, IEEE Commun. Surv. Tutor., vol. 22, no. 3, pp. 1646-1685, 2020. doi: 10.1109/COMST.2020.2988293.
8. Symantec Corporation, *Internet Security Threat Report, vol. 23*, Broadcom Inc., 2018. [Online]. Available: [https://docs.broadcom.com/doc/istr-23-executive-summary-en](https://docs.broadcom.com/doc/istr-23-executive-summary-en?utm_source=chatgpt.com)
9. Mozilla Foundation, *Privacy Not Included*, 2023.
10. U.S. Federal Trade Commission (FTC), “*Internet of Things: Privacy & Security in a Connected World*”, 2015
11. European Union, “General Data Protection Regulation (GDPR),” 2018.

[12] Cámara de Diputados del H. Congreso de la Unión, “Ley Federal de Protección de Datos Personales en Posesión de los Particulares,” México, 2010. [Online]. Available: <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

[13] Information Commissioner’s Office (ICO), *Consumer IoT Guidance – Impact Assessment*, June 25, 2024. [Online]. Available: https://ico.org.uk/media/for-organisations/consumer-iot-guidance-impact-assessment-june-25.pdf

[14] Bitdefender, *2023 IoT Security Landscape Report*, Apr. 25, 2023. [Online]. Available: [https://www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf](https://www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf?utm_source=chatgpt.com)