REINCISOL
ISSN 2953 - 6421

Seguridad en Hogares Inteligentes: Una Revisión Crítica y Prospectiva Hacia la Agenda 2030

Smart Home Security: A Critical and Prospective Review Towards the 2030 Agenda

Para citar este trabajo:
Cobeña, T., y Zambrano, F., (2025). Seguridad en Hogares Inteligentes: Una Revisión Crítica y Prospectiva Hacia la Agenda 2030. *Reincisol*, 4(8), pp. 3154-3174. https://doi.org/10.59282/reincisol.V4(8)3154-3174

Autores:

Tatiana Elizabeth Cobeña Macias
Universidad Técnica de Manabí (UTM)
Facultad de Ciencias Informáticas
Carrera de Sistemas de Información.
Ciudad: Portoviejo, País: Ecuador
Correo Institucional: tatiana.cobena@utm.edu.ec
Orcid: https://orcid.org/0000-0002-3298-6519

Félix Vicente Zambrano Pico
Universidad Técnica de Manabí (UTM)
Facultad de Ciencias Básicas
Carrera de Estadística
Ciudad: Portoviejo, País: Ecuador
Correo Institucional: felix.zambrano@utm.edu.ec
Orcid: https://orcid.org/0000-0003-1383-658X

RECIBIDO: 17 julio 2025 **ACEPTADO:** 30 agosto 2025 **PUBLICADO:** 11 septiembre 2025

RESUMEN

El objetivo de este documento fue realizar una revisión avanzada sobre la seguridad en el entorno del hogar inteligente mediante el análisis de las debilidades de sus bordes y su influencia en el logro de la Agenda 2030 para el desarrollo sostenible. La evaluación se organizó con base en una revisión exhaustiva de la literatura publicada, incluyendo fundamentos técnicos y tendencias, vectores de ataque prevalentes, impedimentos a nivel de sistema como la obsolescencia planificada y regulaciones en curso. Los resultados principales mostraron que el increíble crecimiento de los dispositivos IoT en el hogar ha resultado en un espacio de ataque grande y frágil como resultado directo de malas prácticas de fabricación, tales como credenciales predeterminadas, falta de capacidades de actualización de firmware, etc. Se descubrieron superficies de ataque que exceden el robo de identidad, como la creación de botnets masivas que pueden llevar a cabo ataques de denegación de servicio distribuidos (DDoS) contra infraestructuras esenciales.

También se mostraron amenazas altamente avanzadas basadas en IA, como el hackeo de voz y ataques de cero clics, que sortean la protección convencional a la cliente basada en el comportamiento del usuario. El eje central del informe encontró una vinculación básica entre la ciberseguridad y los ODS de la Agenda 2030. Descubrieron que la automatización del hogar tiene un potencial significativo para contribuir a EE (ODS 7) y RM (ODS 6,12), pero su inseguridad constituye una amenaza existencial. Botnets de dispositivos ávidos de energía como termostatos o puntos de carga de automóviles pueden desplegarse para desestabilizar la red eléctrica y desencadenar cambios dramáticos en los precios de la energía, echando por tierra décadas de avance hacia redes sostenibles.

Por lo tanto, acordamos que la seguridad no era un complemento a considerar o añadir "más tarde", sino que es un requisito fundamental si la tecnología del hogar inteligente debe cumplir con su visión de un mañana más robusto y sostenible. El informe termina con una agenda de seguridad propuesta para 2030 y recomendaciones para la industria, formuladores de políticas y consumidores sobre lo que pueden hacer para crear un entorno ciberseguro.

Palabras clave: Hogar conectado, ciberseguridad, Internet de las cosas (IoT), Agenda 2030, sostenibilidad.

ABSTRACT

The objective of this paper was to conduct an advanced review of smart home security by analyzing the weaknesses at its edges and their impact on achieving the 2030 Agenda for Sustainable Development. The assessment was organized based on a comprehensive review of published literature, including technical foundations and trends, prevalent attack vectors, system-level impediments such as planned obsolescence, and ongoing regulations. The main findings showed that the incredible growth of IoT devices in the home has resulted in a large and fragile attack space as a direct result of poor manufacturing practices, such as default credentials, lack of firmware update capabilities, etc. Attack surfaces beyond identity theft were discovered, such as the creation of massive botnets capable of carrying out distributed denial-of-service (DDoS) attacks against critical infrastructure.

Highly advanced AI-based threats, such as voice hacking and zero-click attacks, were also demonstrated, which circumvent conventional behavior-based customer protection. The report's central thrust found a fundamental connection between cybersecurity and the SDGs of the 2030 Agenda. They found that home automation has significant potential to contribute to EE (SDG 7) and MR (SDGs 6, 12), but its insecurity constitutes an existential threat. Botnets of energy-hungry devices such as thermostats or car charging stations can be deployed to destabilize the electricity grid and trigger dramatic swings in energy prices, undoing decades of progress toward sustainable grids.

Therefore, we agreed that security was not an add-on or "later" option, but rather a fundamental requirement if smart home technology is to deliver on its vision of a more robust and sustainable tomorrow. The report concludes with a proposed security agenda for 2030 and recommendations for industry, policymakers, and consumers on what they can do to create a cybersecure environment.

Keywords: Connected home, cybersecurity, Internet of Things (IoT), 2030 Agenda, sustainability.

INTRODUCCIÓN

La idea de hogar inteligente se ha transformado rápidamente de una fantasía de ciencia ficción a una experiencia diaria muy práctica gracias a la proliferación del Internet de las cosas (IoT) y los avances en tecnología de convergencia (Lawal, Olaniyi y Gibson, 2024; Ojo-González y Bonilla-Morales, 2021).

Un hogar inteligente es la combinación de sistemas y dispositivos provistos de sensores, software y una conexión de red para permitir dicha automatización (como sistemas de control de iluminación) o tareas más avanzadas como el control de persianas, experiencias multimedia o seguridad, así como muchas otras aplicaciones en inicialización en salud en estos años basados (Ojo-González y Bonilla-Morales, 2021; Agama Chico et al., 2024). La ventaja de esta tecnología es que garantiza confort, ahorro de energía y un nivel de control sobre el ambiente del hogar nunca antes visto (Araque Gallardo, 2024; Romero Macías y Loor Navia, 2025).

La capacidad de monitorear un hogar y controlar sus dispositivos a distancia usando aplicaciones en dispositivos móviles o con altavoces activados por voz ha cambiado las rutinas diarias, y no es sorprendente que el mercado haya reaccionado con grandes tasas de penetración: miles de millones de objetos están conectados alrededor del mundo (Asti Rebatta, 2024; Barik, Misra et al., 2024; Lawal et al., 2024). Tal aumento exponencial se debe a la comprensión de que una casa domótica no solo facilita la vida diaria de los usuarios, sino que también hace que los estilos de vida hogareños de las personas sean más sostenibles y eficientes (Romero Macías y Loor Navia, 2025; Araque Gallardo, 2024).

La conexión muy bien integrada que ofrece el valor del hogar inteligente es, al mismo tiempo, su debilidad. Cada dispositivo inteligente agregado a la red del hogar es un potencial punto de entrada para un adversario, causando que la superficie de ataque aumente (Alshamsi, Shaalan y Butt, 2024; García Pérez, 2025). Un mal enlace puede romper toda la red, llevando a ataques contra datos privados y vigilancia personal o dispositivos siendo controlados remotamente para propósitos nefastos (Alshamsi et al., 2024; Morales-Nava, Sosa Sales, Jiménez-Echeverría, Enríquez Díaz, y Barreto De La Cruz, 2023; Rueda-Panchano, 2023).

La amenaza no es meramente la invasión de la privacidad personal, sino también un peligro de daño físico y económico al hogar, y por virtud de la conexión con sistemas de infraestructura, incluidas las redes eléctricas y servicios municipales (Sianaki y Peiris, 2022; Rosado et al., 2025). Por lo tanto, es necesaria una evaluación crítica de la seguridad del hogar inteligente para desmitificar las fantasías utópicas y considerar los riesgos sistémicos asociados con la adopción masiva no controlada (Araujo Robalino, 2024; Alshamsi et al., 2024). La ciberseguridad en el hogar no es un lujo, sino que se convierte en una de las piedras angulares para el uso y la promesa de la automatización del hogar (García Pérez, 2025).

El objetivo de este artículo es proporcionar una perspectiva avanzada sobre la seguridad en los hogares inteligentes, asociar sus riesgos y oportunidades con la Agenda 2030 e indicar una agenda de seguridad con pautas pragmáticas y evaluables para productores, reguladores y usuarios a fin de extraer eficazmente los beneficios en términos de eficiencia y sostenibilidad como vulnerabilidad reducida al riesgo cibernético (Barik et al., 2024; Rosado et al., 2025; García Pérez, 2025).

METODOLOGÍA DE LA REVISIÓN CRÍTICA

Análisis de Vulnerabilidades y Amenazas en el Ecosistema IoT Doméstico

La mayoría de los usuarios solo quiere completar tareas sencillas y necesarias, y no considera los dispositivos que utilizan en línea que apoyarán estas actividades. Ocultar tantas fallas de tal manera es conveniente para los fabricantes, pero pone en peligro a quienes les confían sus datos comerciales o personales.

Cuando nos referimos a la falsa dicotomía entre seguridad y conveniencia como una de las razones por las que la recuperación ante desastres es difícil. La mayoría de los productos de consumo populares ofrece la conveniencia que genera riesgos de seguridad. Esto sucede en un momento en que crear un sistema informático competente aún no es una opción. Por lo general, aparte de los defectos, el tiempo de espera de entrega difiere en las longitudes de tiempo que tomará llevar el software al mercado.

En la prisa por obtener mayores ganancias, los fabricantes dejan cuestiones como las pruebas de seguridad y la protección de redes hasta demasiado tarde. El precio de su laxitud es que muchos de estos productos contienen fallas. Una falla especialmente significativa es la ausencia de un programa robusto para actualizaciones de firmware, de modo que después de su lanzamiento el software comienza a envejecer y en ganancia es probable que sea explotado en desventaja de uno mismo (Araujo Robalino, 2024; et al., 2025).

De hecho, los fabricantes envían parches de seguridad para corregir agujeros conocidos (BUTT 49), que, no obstante, aún no corrigen problemas de configuración que causan la no recepción en muchos dispositivos (Alshamsi, & 2024). Muchos agricultores no manejan este proceso manual conscientemente o en absoluto y normaliza el uso de credenciales predeterminadas (Morales-Nava et al., 2023). Todas las combinaciones posibles de estos nombres son bien conocidas por los hackers, y todavía hay casos en que no pueden ser cambiadas por sus usuarios.

La comunicación entre dispositivos de diferentes fabricantes no está estandarizada, hay poca documentación de seguridad sobre estos sistemas operativos ni mecanismos instalados para ese propósito en el lugar; esto hace difícil gestionar y controlar de manera uniforme una red doméstica o empresarial (Méndez, 2024; Rueda-Panchano, 2023). A esto se suman dispositivos que no tienen sistemas operativos ni ninguna documentación escrita. Los puntos vulnerables que surgen de esto pueden ser explotados como entradas no destacadas. La mayoría de las partes que gestionan estas redes no tienen idea de lo que está sucediendo (Araujo Robalino, 2024). Tan derrochador de recursos de red que todo esto es solo demasiado probable, solo una irritación realmente: de todos modos, no se desarrolla nada (He Shimonou, 2024).

Vectores Comunes y Sofisticados de Ataque

Por lo tanto, los atacantes explotan estas vulnerabilidades a través de una variedad de vectores. Especialmente comunes son los ataques en la capa de red que despliegan programas antiparasitarios en dispositivos con contraseñas débiles o cifrado anticuado como el WEP, fácilmente descifrado o violado (Alshamsi et al., 2024).

Una red insegura es un agujero ciego para la interceptación. El atacante aquí está empotrado entre tu hardware y el servidor en la nube. Así pueden ejercer influencia sobre la comunicación no vista, levantar datos, e incluso propagar malware sin que nadie lo note en ninguno de los extremos (García Pérez, 2025; Araujo Robalino, 2024).

El problema más grave y generalmente más subestimado es el de los ataques de botnet de IoT. El firmware obsoleto o las características de credenciales predeterminadas hacen que algunos dispositivos sean inseguros, y pueden ser secuestrados para formar una botnet (Alshamsi et al., 2024). Estos dispositivos, bajo el control de un hacker, se convierten en parte de una red maligna (botnet) que puede causar masivas intrusiones. Un ejemplo destacado es el Botnet Mirai. Cientos de miles de dispositivos, incluidas cámaras de Supervision Net y grabadoras de video digital (DVR), fueron infectados para realizar ataques de Denegación de Servicio Distribuida (DDoS) a gran escala (Alshamsi et al., 2024; Morales-Nava et al., 2023). No solo las máquinas individuales, sino también servicios mundiales como Spotify y Netflix sufren como resultado.

Esto demuestra que la superficie de ataque del hogar inteligente rompe con los peligros respetables para convertirse en una infección de los propios sustratos de las operaciones de Internet (Rosado et al., 2025).

Amenazas Emergentes en la Era de la Inteligencia Artificial

Un panorama de amenazas alimentado por avances en inteligencia artificial (IA) está emergiendo. Por ejemplo, podemos ver que la piratería de voz o la asociación de voz, donde simplemente se graba la voz de una persona y luego se utiliza la grabación como parte de mensajes falsos para que suenen convincentes en evidencia y engañen a quien escucha (Barik et al., 2024). Como resultado, los asistentes de voz y los sistemas de autenticación biométrica se desvían tanto en sus operaciones que esto puede provocar el robo de identidad, la pérdida financiera o el descrédito público.

El uso indebido del lenguaje, o el abuso de la voz, es un ejemplo de delito en el lenguaje. A diferencia de los ataques tradicionales, que requieren la participación activa de la víctima (por ejemplo, hacer clic en un enlace de phishing) o el doble consentimiento en Schwartzsigns (Rosado et al., 2025).

Siempre que no haya oposición activa o, al contrario, la gente esté contigo, la piratería de voz puede comprometer los métodos de confirmación biométrica. Si no se detiene a tiempo, sus efectos, que incluyen pérdidas financieras y descrédito público, pueden experimentarse en segundos (Barik et al., 2024).

El dispositivo que puede demostrar más fácilmente la última revolución social en defectos de seguridad es probablemente el asistente digital. Aquí nuestra historia biométrica personal se registra y prepara su propia trampa (Rosado et al., 2025).

En un nivel más avanzado, tenemos la operación de inyección de audio adversarial. Estos ataques utilizan comandos de voz ultrasónicos, que no son escuchados por el oído humano pero capturados y ejecutados por sistemas de reconocimiento automático de voz (ASR) en asistentes virtuales (Barik et al., 2024). Aquí se aprovechan de las vulnerabilidades inherentes de cualquier máquina que ejecute una red neuronal. ¿Qué podría ser más problemático en cualquier hogar que crear una situación donde un intruso pueda emitir órdenes inaudibles a la red doméstica, por ejemplo, para desbloquear puertas o encender luces?

Complementando estas amenazas, los ataques 'sin contacto' son una de las realidades más aterradoras del panorama actual de ataque. No necesitan ninguna acción de tu parte, ni siquiera un clic. Explotan vulnerabilidades en el software que procesa datos de fuentes desconocidas (por ejemplo, programas de mensajería o correo electrónico) para inyectar código en tu máquina (Rosado et al., 2025; García Pérez, 2025). La invisibilidad de tales ataques va en contra de toda la educación del usuario en ciberseguridad.

Ahora la ley está en manos de productores y desarrolladores, ya que la seguridad práctica debe integrarse en el software desde el principio (Araujo Robalino, 2024).

Tabla 1. Matriz de Amenazas y Vulnerabilidades en el Hogar Inteligente

Amenaza/Ataque	Descripción	Vulnerabilidad Explotada	Impacto Potencial	Ejemplo Referenciado
Firmware obsoleto	El software interno del dispositivo no se actualiza, dejando fallos de seguridad conocidos sin parchar.	Falta de programas de actualización robustos o automáticos.	Acceso no autorizado, inyección de malware.	Cámaras de seguridad y grabadores de video.18
Credenciales por defecto	Uso de nombres de usuario y contraseñas predeterminados por el fabricante.	Prácticas de diseño inseguras y falta de obligación de cambio inicial.	Control total del dispositivo y entrada a la red doméstica.	Botnet Mirai, que explota contraseñas débiles o predeterminadas.2
Ataque de botnet	Red de dispositivos comprometidos (bots) controlada por un atacante.	Firmware obsoleto, credenciales débiles y la gran cantidad de dispositivos IoT.	Ataques DDoS a gran escala que derriban servicios de internet.	La botnet Mirai, que afectó a servicios como Netflix y PayPal.19
Inyección de audio adversarial	Comandos de voz imperceptibles para humanos que activan sistemas de reconocimiento de voz (ASR).	Vulnerabilidades en el diseño de las redes neuronales de los asistentes de voz.	Ejecución de comandos no autorizados sin el conocimiento del usuario.	Ataques a asistentes de voz como Alexa y Google Home.26
Ataques de "cero clic"	Infiltración en un dispositivo sin que el usuario interactúe (ni clic, ni descarga de archivo).	Fallos no parchados (zero-day) en aplicaciones que procesan datos de fuentes no confiables.	Infección silenciosa del dispositivo con spyware o malware.	Ataques a aplicaciones de mensajería o correo electrónico.6

RESULTADOS

La Obsolescencia Programada: Un Riesgo Ciber de Larga Duración

El Ciclo de Vida de Dispositivos al Final de su Vida Útil (EOL)

La vida media de seguridad de un dispositivo IoT es un requisito olvidado y es algo muy necesario en ese ciclo de vida del producto embebido. Mientras que la persistencia física puede ser duradera, la seguridad del objeto es efímera (García Pérez, 2025).

El bajo soporte de lanzamiento por parte de los fabricantes de dispositivos de consumo acelera el proceso de ventas, termina el soporte y descontinúa el parcheo de seguridad para modelos más antiguos, llevándolos a un estado de Final de Vida Útil (EOL) (Alshamsi et al., 2024). En esta fase es común que se construyan nuevos modelos mientras no se gestiona la seguridad de los dispositivos EOL, convirtiéndose incidentalmente en objetivos claros para los atacantes (Araujo Robalino et al., 2024).

De los 17 mil millones de dispositivos IoT en todo el mundo, un tercio está permanentemente vulnerable durante cinco años, con alrededor de 5.6 mil millones de puntos de ataque potenciales (Rosado et al., 2025). Este enfoque en la alta rotación en los modelos de negocios modernos conduce a una peligrosa "doble brecha" de responsabilidad y contacto.

La empresa está satisfecha con toda la producción y no tiene que preocuparse por la seguridad después de pocas semanas. El usuario final incluso obtiene un producto funcional, que a largo plazo representa una amenaza para la red de ese individuo, así como para la infraestructura global (Sianaki & Peiris, 2022). Esta externalidad es una de las principales razones por las cuales los botnets se propagan en (Morales-Nava et al., 2023).

La ausencia de un marco legal explícito que haga responsables a los fabricantes es responsable de alimentar esta brecha de memoria (Araque Gallardo, 2024).

Efectos de la Obsolescencia de las Redes Domésticas

La obsolescencia puede tener implicaciones inmediatas y peligrosas para la seguridad del hogar. Uno de los ejemplos más preocupantes es que las personas reutilizarán dispositivos antiguos para aplicaciones nuevas, como usar un iPad viejo como controlador de automatización del hogar a pesar de ejecutar software desactualizado lleno de vulnerabilidades (Asti Rebatte, 2024).

Del mismo modo, una gestión inadecuada del final de la vida útil de dispositivos antiguos representa una amenaza significativa (Méndez, 2024). Muchos dispositivos IoT contienen información personal y confidencial en un almacenamiento interno. Si se descarta tal cual, sin un borrado seguro, se convierte en una amenaza masiva para la identidad de una persona.

En tales casos, la colección de dispositivos EOL ya usados puede llegar al mercado negro, donde algunos ciberdelincuentes pueden hacerse con ellos y recuperar información sensible en su lugar (Rueda-Panchano, 2023).

Esto muestra que la seguridad debe garantizarse a lo largo de todo el ciclo de vida desde el momento de la producción hasta el final de la vida (Rosado et al., 2025).

Estrategias de Mitigación y Buenas Prácticas

La primera firewall doméstica: Medidas a nivel de usuario

Con los usuarios reconociendo esto, de hecho, se convierten en el primer firewall para su red. Luego, asumen parte del control que debería estar en manos de otras personas y examinan problemas de seguridad directos o de alto nivel (Agama Chico et al., 2024).

Una medida esencial es que la red WiFi esté encriptada cambiando las credenciales de administración predeterminadas del router, utilizando una contraseña fuerte y habilitando una mejor encriptación WPA3 (Alshamsi et al., 2024). Al mismo tiempo, se recomienda segmentar tu red doméstica en una red de invitados separada para dispositivos IoT, de modo que no se mezclen con equipos sensibles del hogar o móviles como portátiles y teléfonos inteligentes (Romero Macías & Loor Navia, 2025).

Las medidas del usuario incluyen instar a la gestión a establecer contraseñas únicas y activar la autenticación de dos pasos (2FA) al manejar el dispositivo, que es vital (García Pérez, 2015). También se recomienda apagar aquellas funciones que realmente no necesitas, como el control de voz o la capacidad para que otros accedan remotamente a tu computadora en casa, ya que esto minimiza la superficie de ataque (Rosado et al., 2025).

Sin embargo, todavía existen grandes obstáculos para el usuario, debido a la complejidad de la configuración y la falta de confianza en la seguridad del producto (Araque Gallardo, 2024).

Soluciones Técnicas y de la Industria

En la industria, "Seguridad desde el Diseño" es una necesidad que incluirá todas las medidas desde la concepción del producto (Barik, Misra, Mohan, & Mishra, 2024). Entre ellas, la encriptación de extremo a extremo y la autenticación sólida son necesarias (Lawal, Olaniyi, & Gibson, 2024). Los servicios de actualización de firmware y software están entre los antídotos más importantes para las debilidades de seguridad de IoT. Esto permite a los fabricantes parchear agujeros sin necesidad de intervención del usuario (Araujo Robalino, 2024; Alshamsi et al., 2024).

Sin embargo, este modelo se verá presionado con la interfaz de consumidor plug-and-play. Las necesidades de simplicidad y rapidez son primordiales (Ojo-Gonzalez & Bonilla-Morales, 2021). Si la seguridad resulta en cosas como 2FA o redes segregadas que no pueden ser consumidas sin problemas, entonces la gente sentirá que no son fácilmente accesibles y difíciles de usar. Por tanto, es importante que la industria produzca soluciones robustas que, no obstante, sean fáciles de usar y no socaven la accesibilidad y confianza del usuario final (Rosado et al., 2025).

La Seguridad como Catalizador o Barrera para la Agenda 2030

Potencial de Sostenibilidad en los Hogares Inteligentes

Los hogares inteligentes, además de ser divertidos y placenteros, tienen un papel central en el logro de varios de los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas (Romero Macías & Loor Navia, 2025).

Los hogares que son "inteligentes" (controlados electrónicamente) pueden provocar un cambio radical en el consumo de energía y agua, aliviando el ODS 7 (energía asequible y no contaminante) y el ODS 12 (producción y consumo responsables) (Araque Gallardo, 2024).

Se estima que los sistemas inteligentes pueden reducir hasta un 30% el consumo energético. El entorno de realidad virtual, cada vez más entendido como "Naturaleza", es un tema para luminarias como el consultor Kevin Kelly, y se basa en un suministro constante de captura de video (Agama Chico et al., 2024). Al igual que los circuitos de materia y energía anteriores, los sistemas que se integran con fuentes renovables, como la eólica o solar, hacen posible el almacenamiento de producción neta (Sianaki & Peiris, 2022). El ODS 6 también apoya sensores para agua y gas que previenen fugas o desperdicios (Araujo Robalino, 2024).

La Barrera de Seguridad: Un Obstáculo para los ODS

Por un lado, esta interconexión, que proporciona sus razones funcionales de ser, ayuda a que los objetivos de sostenibilidad entren en vigor. Por otro lado, abre la puerta a riesgos que podrían neutralizar esos mismos objetivos (Alshamsi et al., 2024).

Dispositivos como cargadores de vehículos eléctricos, aires acondicionados o termostatos pueden ser utilizados en la realidad como botnets de alto impacto: no solo pueden derribar su propia red eléctrica, sino la de todo un país. Y hasta mercados de energía enteros ya han sido comprometidos durante un tiempo considerable (Rosado et al., 2025).

Un ciberdelincuente puede manipular la demanda de energía en tiempo real, provocando la pérdida de millones de dólares o incluso apagones completos, como si se librara una guerra a través de computadoras (Sianaki & Peiris, 2022).

Los hogares inteligentes no pueden ser una fuente de desarrollo sostenible. Esto se ilustra bastante bien en la historia anterior. Los hogares inteligentes que no estén protegidos contra amenazas como esta se convertirán de catalizadores de los ODS a ser solo otro riesgo sistémico (Barik et al., 2024; García Pérez, 2025).

Tabla 2. Vínculo Crítico entre Riesgos de Seguridad y los ODS de la ONU

Objetivo de Desarrollo Sostenible (ODS)	**Beneficio Potencial de la Domótica**	**Riesgo de Seguridad Asociado**	**Conclusión: Impacto en la Agenda 2030**
ODS 7: Energía asequible y no contaminante	Optimización del consumo energético y reducción de la huella de carbono.	Ataques de botnets de alta potencia que manipulan la demanda energética para desestabilizar la red eléctrica.	La inseguridad del IoT doméstico podría revertir los avances en eficiencia energética, comprometiendo la transición hacia energías renovables.
ODS 9: Industria, innovación e infraestructura	Creación de redes eléctricas inteligentes y mejora de la resiliencia de la infraestructura.	Los ciberataques contra los dispositivos de los hogares inteligentes son un vector de ataque para acceder a infraestructuras críticas.	La falta de seguridad en la capa del usuario podría exponer y comprometer la resiliencia de la red eléctrica, socavando los pilares de la infraestructura crítica.
ODS 12: Producción y consumo responsables	Uso eficiente de los recursos hídricos mediante sensores y sistemas de riego inteligentes.	Ataques de inyección de código malicioso o toma de control de dispositivos para malgastar recursos (ej. dejar llaves de agua abiertas).	La inseguridad no solo afecta la privacidad, sino que podría utilizarse para sabotear la eficiencia de los recursos, lo que iría en contra del consumo responsable.
ODS 11: Ciudades y comunidades sostenibles	Fomento de la resiliencia comunitaria y la eficiencia urbana a través de redes inteligentes interconectadas.	La interconexión de miles de dispositivos vulnerables en una comunidad crea un riesgo sistémico de ataque coordinado a gran escala.	Un ataque a la escala del hogar inteligente podría tener un efecto dominó, afectando la estabilidad y la sostenibilidad de comunidades enteras, en lugar de ser un problema aislado.

Marco Regulatorio y la Búsqueda de Estandarización

La Brecha entre la Innovación y la Regulación

Así que la industria del IoT ha superado con creces a los sistemas regulatorios en términos de aplicación, investigación y desarrollo (Barik, Misra, Mohan, & Mishra, 2024). No hay estándares para los protocolos de seguridad entre diferentes fabricantes, lo que ha hecho que el entorno esté fragmentado, con muchos puntos de entrada vulnerables (Ojo-Gonzalez & Bonilla-Morales, 2021). Esto ha llevado a una situación en la que la ciberseguridad es manejada por los consumidores (históricamente) y, aun ahora, deben navegar a través de mares de dispositivos inseguros (García Pérez, 2025). El resultado ha sido la aparición de amenazas sistémicas como botnets y ataques de cero clic, haciendo este modelo insostenible (Alshamsi, Shaalan, & Butt, 2024; Rosado et al., 2025). Debido a que el problema es demasiado grande para que los individuos puedan manejarlo por sí solos, la sociedad ha asumido la responsabilidad por un modelo de negocio que en su esencia valora la rapidez y el bajo costo sobre la seguridad a largo plazo (Araque Gallardo, 2024).

Las comunidades y los jugadores de la industria han respondido creando foros en línea para que los profesionales compartan información o discutan lo que pueden hacer para ayudar a las empresas. En el Reino Unido, el bloguero de marketing digital Giovanni Pasqual de Staff Digital ha lanzado una cuenta de WeChat que está disponible las 24 horas del día: más de 500 especialistas en marketing digital se han unido ahora con un promedio de 9 a 10 conversaciones en tiempo real por día entre ellos (Staff Digital, Comunicado de Prensa 2021). La última semana de noviembre, por su parte, fue la Semana de la Tecnología en West Yorkshire (Reino Unido). Incluyó diversas actividades destinadas a promover aplicaciones para pequeñas y medianas empresas en el ámbito digital, así como sistemas controlados por voz (Base de datos multimedia, Gestión de archivos de texto y Comunicaciones directas 2021).

El papel de los organismos de normalización

En respuesta a esta brecha, los organismos de normalización y los gobiernos han asumido un papel cada vez más activo. En los Estados Unidos, la Ley de Mejora de la Ciberseguridad del IoT de 2020 (IoT CIA) constituye la primera ley federal que regula la seguridad de los dispositivos IoT para agencias gubernamentales. Esta ley otorga al Instituto Nacional de Estándares y Tecnología (NIST) el mandato de desarrollar estándares mínimos de seguridad que las agencias federales deben cumplir cuando compran dispositivos conectados (Rosado et al., 2025). Aunque la ley no regula directamente los dispositivos de consumo, su objetivo es utilizar el poder adquisitivo del gobierno para exigir a los fabricantes la aplicación de buenas prácticas en toda su gama de productos. Los estándares del NIST se centran en identidades únicas, métodos para alterar credenciales y formas de proporcionar actualizaciones de firmware, entre otras cosas (García Pérez, 2025).

En Europa, la Directiva de Sistemas de Redes e Información (NIS2) representa un esfuerzo similar para mejorar la resiliencia cibernética y armonizar leyes en todo el continente (Rosado et al. en los años que resulten pertinentes). Desde su introducción, las ventas de equipos de TI que no cumplan con las regulaciones de ciberseguridad no pueden continuar: la responsabilidad recae directamente sobre los fabricantes (Araque Gallardo 2024). De manera similar, las directrices de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) apoyan este enfoque. Se proporcionan recomendaciones a los fabricantes y desarrolladores a lo largo de toda la cadena de suministro de IoT: desde la fase de diseño, hasta el soporte y mantenimiento (Sianaki & Peiris 2022). Estas leyes anuncian un cambio fundamental. La ciberseguridad pasa de ser una tarea individual a formar parte de la cadena de suministro y diseño, impulsando un enfoque de "seguridad desde el diseño" (Rosado et al. en los años que resulten pertinentes).

Investigación sobre Propuestas para una Agenda de Seguridad 2030

Siguiendo los hallazgos del estudio, se sugiere que la agenda de seguridad en hogares inteligentes se desarrolle hacia 2030 de la siguiente manera:

Para los Fabricantes:

- Adoptar un enfoque de "Seguridad desde el Diseño": Desde el mismo inicio de la conceptualización y proceso de diseño del producto, la seguridad debería ser una prioridad, no algo añadido posteriormente.
- Comprometerse con el Soporte a Largo Plazo: Los fabricantes deben asegurar que las actualizaciones de seguridad y los parches de vulnerabilidad estén disponibles durante la vida útil de un producto, incluso después de declarar su "fin de vida". La responsabilidad no cesa en el punto de venta.
- Usar Certificaciones Transparentes: Los productos deberían tener certificaciones de seguridad claras y reconocibles, permitiendo a los consumidores decidir por sí mismos sobre las medidas de protección, así como proporcionar la participación abierta del fabricante.

Para Legisladores y Reguladores:

- Armonizar Regulaciones Globales: Los gobiernos deberían cooperar entre sí para establecer estándares globales de ciberseguridad IoT, evitando la fragmentación regulatoria resultante al implementar medidas uniformes.
- Establecer Responsabilidad Legal: Se deben crear leyes que responsabilicen legalmente a los fabricantes en casos donde los defectos de seguridad puedan ser explotados, dando una motivación económica para enfatizar la protección.
- Incentivar la Investigación en Seguridad: Los gobiernos deberían promover la investigación en ciberseguridad, especialmente en el desarrollo de contramedidas para amenazas novedosas como ataques de cero clic e inyecciones de audio adversariales.

Para los Consumidores:

- Fomentar la Alfabetización Digital: Se deben promover campañas que eduquen a los usuarios sobre los riesgos del IoT e informen de algunas medidas de protección básicas, como la gestión de contraseñas o la activación de autenticación de dos factores.

- Los usuarios deberían tomar un papel más activo y, al menos ocasionalmente, realizar una auditoría de red doméstica que verifique qué dispositivos están conectados a sus propias redes. Esto puede incluir deshabilitar funciones innecesarias y, siempre que sea posible, actualizar el software.
- Conozca a los fabricantes de cualquier cosa nueva que compre y asegúrese de que sean una empresa comprometida con la seguridad, así como en proporcionar actualizaciones oportunamente.

CONCLUSIONES

El análisis realizado confirma que la seguridad en los hogares inteligentes es un tema multidimensional que abarca vulnerabilidades técnicas, vectores de ataque sofisticados y desafíos regulatorios y de modelo de negocio. La revisión crítica de la literatura revela que la rápida proliferación de dispositivos IoT, sin las salvaguardas adecuadas, ha creado un riesgo sistémico que va más allá de la mera pérdida de datos personales. Las botnets de dispositivos domésticos representan una amenaza tangible para la estabilidad de infraestructuras críticas como las redes eléctricas, lo que demuestra que la ciberseguridad es un pilar fundamental para la sostenibilidad de la sociedad moderna y no un simple complemento.

La dicotomía entre la promesa de eficiencia y la realidad de la inseguridad pone de relieve una verdad fundamental: la tecnología que busca hacernos más sostenibles es, por su naturaleza interconectada, vulnerable a ser utilizada para fines que socavan los Objetivos de Desarrollo Sostenible. El problema se agrava por la brecha de soporte de seguridad que resulta de la obsolescencia programada y la falta de confianza del consumidor.4 En consecuencia, la seguridad no debe ser vista como un costo adicional o una barrera para la conveniencia, sino como una inversión fundamental para la viabilidad a largo plazo del ecosistema del hogar inteligente y un requisito previo para alcanzar un futuro verdaderamente sostenible y resiliente.

REFERENCIAS BIBLIOGRÁFICAS

Agama Chico, A. J., Oviedo Galarza, J. E., García Paredes, R. V., & Maliza Cruz, W. I. (2024). Prototipo electrónico para internet de las cosas en viviendas inteligentes. Journal of Science and Research, 9(2), 157–172. Recuperado a partir de https://revistas.utb.edu.ec/index.php/sr/article/view/3093

Alshamsi, O., Shaalan, K., & Butt, U. (2024). Towards Securing Smart Homes: A Systematic Literature Review of Malware Detection Techniques and Recommended Prevention Approach. Information, 15(10), 631. https://doi.org/10.3390/info15100631

Araque Gallardo, J. (2024). Análisis Exhaustivo de los Sistemas de Gestión de la Energía en Hogares Inteligentes. CESTA, 4(2). https://doi.org/10.17981/cesta.04.02.2023.03

Araujo Robalino, M. I. (2024). Soluciones de seguridad en sistemas iot de hogares inteligentes para mitigar riesgos y vulnerabilidades mediante la realización de pruebas de penetración.

Asti Rebatta, S. A. (2024). Adopción de domótica en hogares de Lima: explorando la integración de productos inteligentes.

Barik, K., Misra, S., Mohan, R., Mishra, B. (2024). AIoT and Its Trust Models to Enhance Societal Applications Using Intelligent Technologies. In: Misra, S., Siakas, K., Lampropoulos, G. (eds) Artificial Intelligence of Things for Achieving Sustainable Development Goals. Lecture Notes on Data Engineering and Communications Technologies, vol 192. Springer, Cham. https://doi.org/10.1007/978-3-031-53433-1_16

García Pérez, K. A. (2025). Estrategias proactivas para mitigar los riesgos emergentes de ciberseguridad en dispositivos IOT para hogares inteligentes (Master's thesis, La Libertad, Universidad Estatal Península de Santa Elena, 2025).

Lawal, K. N., Olaniyi, T. K., & Gibson, R. M. (2024). Leveraging Real-World Data from IoT Devices in a Fog–Cloud Architecture for Resource Optimisation within a Smart Building. Applied Sciences, 14(1), 316. https://doi.org/10.3390/app14010316

Méndez, P. G. P. (2024). Diseño de una antena para aplicaciones IoT en hogares inteligentes (Doctoral dissertation, Instituto Nacional de Astrofísica, Óptica y Electrónica).

Morales-Nava, R., Sosa Sales, A., Jiménez-Echeverría, J. R., Enríquez Díaz , J. M., & Barreto De La Cruz , J. L. (2023). Implementación de un control de acceso en cerradura eléctrica con base al reconocimiento facial y huella dactilar para elevar el nivel de seguridad en los hogares . Ciencia Latina Revista Científica Multidisciplinar, 7(3), 5976-5991. https://doi.org/10.37811/cl_rcm.v7i3.6602

Ojo-Gonzalez, K., & Bonilla-Morales, B. (2021). Requerimientos no funcionales para sistemas basados en el Internet de las cosas (IoT): Una revisión. I+D Tecnológico, 17(2), 30-40. https://doi.org/10.33412/idt.v17.2.3303

Romero Macías, J. V., & Loor Navia, E. A. (2025). Aplicaciones de internet de las cosas (IoT) en la optimización de la eficiencia energética en entornos residenciales.: Internet of things (IoT) applications in energy efficiency optimization in residential environments. Revista Científica Multidisciplinar G-Nerando, 6(1), Pág. 281 –. https://doi.org/10.60100/rcmg.v6i1.406

Rosado, D.G., Sánchez, L.E., Martínez, F., Blanco, C., Serrano, M.A., Fernández Medina, E. (2025). Hacia un marco de gobierno de la seguridad para ciudades inteligentes. En Suárez Corona, A. (ed.) (2025). XVIII Reunión Española sobre Criptología y Seguridad de la Información: XVIII RECSI, León 23-25 octubre 2024. (p. 307-312). Universidad de León, Servicio de Publicaciones.

Rueda-Panchano, C. I. (2023). Investigación sobre la Aplicación de la Automatización Residencial con el Objetivo de Reducir el Riesgo de Robo en una Vivienda Común. Ibero-American Journal of Engineering & Technology Studies, 3(1), 478-485.

Sianaki, O.A., Peiris, S. (2022). The Impact of the Blockchain Technology on the Smart Grid Customer Domain: Toward the Achievement of the Sustainable Development Goals (SDGs) of the United Nations. In: Barolli, L., Hussain, F., Enokido, T. (eds) Advanced Information Networking and Applications. AINA 2022. Lecture Notes in Networks and Systems, vol 451. Springer, Cham. https://doi.org/10.1007/978-3-030-99619-2_49

Conflicto de intereses

Los autores indican que esta investigación no tiene conflicto de intereses y, por tanto, acepta las normativas de la publicación en esta revista.

Con certificación de: