Implementación de redes seguras en entornos de IoT: estrategias y mejores prácticas

Jhon Edison Cantor Daza

Asesor

Alfredo Jesús Castro Guzmán

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Ingeniería de Sistemas

Bogotá D.C.

2026

Resumen

El Internet de las Cosas (IoT) se ha consolidado como una de las tecnologías más influyentes en la transformación digital de la sociedad, al integrar dispositivos inteligentes en sectores como la salud, la industria, el comercio y los hogares. Su capacidad para recopilar y procesar datos en tiempo real ha impulsado nuevas oportunidades de eficiencia, automatización e innovación, pero también ha incrementado los riesgos asociados a la ciberseguridad, la privacidad y la resiliencia de infraestructuras críticas. En este contexto, la presente monografía analiza el IoT desde una perspectiva integral, abordando sus beneficios, desafíos y el estado actual de la seguridad en 2025. Se estudian conceptos fundamentales, arquitecturas, protocolos y buenas prácticas de protección, con el fin de ofrecer una visión actualizada del panorama de riesgos. Además, se desarrolla una guía práctica dirigida a usuarios de entornos domésticos y empresariales, orientada a facilitar la implementación de medidas preventivas accesibles y efectivas para dispositivos como cámaras, sensores y alarmas. Finalmente, se incluye un análisis crítico basado en los resultados de una encuesta aplicada a usuarios reales, que evidencia brechas entre las prácticas actuales y las recomendaciones internacionales, destacando la necesidad de fortalecer la concientización y cultura de seguridad digital en ecosistemas cada vez más conectados.

Palabras Clave: Internet de las Cosas (IoT), Seguridad en redes, ciberseguridad, vulnerabilidades IoT, autenticación y cifrado, detección de intrusos, normativas y estándares, diseño seguro (security by design), arquitectura por capas, protocolos seguros.

Abstract

The Internet of Things (IoT) has established itself as one of the most influential technologies in the digital transformation of society, integrating smart devices into sectors such as healthcare, industry, commerce, and homes. Its ability to collect and process data in real time has driven new opportunities for efficiency, automation, and innovation, but it has also increased the risks associated with cybersecurity, privacy, and the resilience of critical infrastructure. In this context, this monograph analyzes the IoT from a comprehensive perspective, addressing its benefits, challenges, and the current state of security in 2025. Fundamental concepts, architectures, protocols, and best practices for protection are examined to provide an up-to-date view of the risk landscape. Furthermore, a practical guide for home and business users has been developed to facilitate the implementation of accessible and effective preventative measures for devices such as cameras, sensors, and alarms. Finally, a critical analysis based on the results of a survey of real users is included, revealing gaps between current practices and international recommendations, and highlighting the need to strengthen awareness and a culture of digital security in increasingly connected ecosystems.

Keywords: Internet of Things (IoT), Network security, cybersecurity, IoT vulnerabilities, authentication and encryption, intrusion detection, regulations and standards, security by design, layered architecture, secure protocols.

Contenido

Lista de Tablas

Lista de Figuras

Introducción

El Internet de las Cosas (IoT) se ha convertido en una de las tecnologías más determinantes en el desarrollo de la transformación digital, al permitir la conexión e interacción continua de dispositivos físicos con Internet y con otros sistemas, por lo que su presencia se ha extendido a sectores como la salud, la educación, el comercio, la industria y los hogares, impulsando nuevos modelos de automatización, optimización de procesos y servicios inteligentes. No obstante, este crecimiento acelerado también ha generado una expansión de la superficie de exposición a ciberataques, evidenciando vulnerabilidades relacionadas con la protección de datos, la gestión de dispositivos, la privacidad de la información y la resiliencia de las infraestructuras digitales.

Frente a este panorama, resulta necesario analizar de manera integral los riesgos y desafíos asociados al IoT, así como las estrategias y buenas prácticas que permitan implementar redes seguras y confiables, de acuerdo con esto, en la presente monografía se aborda los fundamentos conceptuales de la tecnología, su arquitectura, los principales protocolos de comunicación utilizados, los riesgos emergentes y los estándares internacionales que orientan la seguridad en este ecosistema, de la misma manera. se examinan las prácticas actuales de los usuarios mediante una encuesta aplicada en entornos reales, lo que permite identificar brechas entre las recomendaciones técnicas y el uso cotidiano de los dispositivos conectados.

El propósito de este trabajo es aportar una visión actualizada sobre la seguridad en redes IoT y proponer medidas prácticas que contribuyan a fortalecer su adopción responsable en el contexto doméstico y empresarial, promoviendo entornos más seguros, confiables y resilientes.

Planteamiento del problema

La incorporación de dispositivos IoT sin criterios sólidos de seguridad representa un desafío para los usuarios y organizaciones, ya que muchos equipos llegan al mercado con configuraciones predeterminadas inseguras, sin mecanismos de actualización confiables ni protocolos de comunicación robustos y esto se traduce en incidentes frecuentes como accesos no autorizados, secuestro de dispositivos, espionaje digital y ataques a infraestructuras críticas, por lo que de allí surge la necesidad de definir estrategias y buenas prácticas que permitan implementar entornos IoT de manera confiable y resiliente.

Justificación

La adopción masiva de tecnologías relacionadas con el Internet de las Cosas (IoT) ha transformado radicalmente numerosos sectores, permitiendo una mayor automatización, eficiencia y conectividad sin precedentes, sin embargo, este crecimiento exponencial ha generado una paradoja crítica: mientras más dependemos de los dispositivos IoT para optimizar procesos y mejorar la calidad de vida, más expuestos estamos a riesgos de seguridad digital sin precedentes (CyberArk, 2025).

El estudio y análisis de la seguridad en IoT resulta indispensable debido al impacto que tiene en la vida cotidiana y en la continuidad de los servicios esenciales, ya que en un entorno IoT inseguro no solo afecta a usuarios particulares, sino que puede poner en riesgo ecosistemas completos, como redes hospitalarias o sistemas de control industrial. Esta monografía aporta al campo académico y profesional al ofrecer una guía práctica respaldada en estándares internacionales y buenas prácticas, que sirva de base para fortalecer las políticas de ciberseguridad en organizaciones públicas y privadas.

El problema fundamental radica en que una gran parte de los dispositivos IoT actuales presentan vulnerabilidades críticas (Home - OWASP Top 10:2021, n.d.), debido a tres factores clave:

1. Limitaciones técnicas: Debido a los dispositivos con recursos computacionales reducidos que imposibilitan implementar mecanismos robustos de cifrado o autenticación.
2. Diversidad fragmentada: Debido a la ausencia de estándares unificados entre fabricantes, ya que se conocen más de 300 protocolos de comunicación diferentes (Barbara, s.f.).

3. Negligencia en seguridad: Ya que más del 62% de las organizaciones priorizan la funcionalidad sobre la protección (Identity Security Threat Landscape Report, 2024).

Por lo que las consecuencias de esta inseguridad son tangibles y multidimensionales, inicialmente en salud, ya que por ejemplo, los ataques a marcapasos o bombas de insulina conectadas pueden poner en riesgo vidas humanas, así como también en la industria debido a que el costo promedio de un ciberataque exitoso a sistemas IoT industriales puede llegar a superar los $4.5 millones (Panda Security, 2025). Y por último en los hogares ya que los dispositivos domésticos vulnerables son la puerta de entrada para robo de identidades y datos bancarios

Objetivo general

Analizar e implementar estrategias y buenas prácticas para fortalecer la seguridad en redes IoT, garantizando la protección de la información, la integridad de los dispositivos y la confiabilidad de la infraestructura tecnológica.

Objetivos específicos

Identificar las principales vulnerabilidades y riesgos de seguridad presentes en la actualidad en redes IoT.

Analizar los protocolos de comunicación y mecanismos de autenticación utilizados en entornos IoT.

Evaluar las mejores prácticas y estándares existentes para la implementación de redes seguras en IoT.

Proponer un conjunto de estrategias y medidas de seguridad para mitigar las amenazas en redes IoT.

Elaborar un modelo o guía práctica que facilite la implementación segura de infraestructuras IoT.

Marco conceptual y teórico

Internet de las Cosas (IoT)

Definición y Evolución del IoT

El Internet de las Cosas (IoT, por sus siglas en inglés) es un concepto que ha evolucionado con diferentes matices según el enfoque de los autores y organismos internacionales, por lo que de manera general, se entiende como la interconexión de dispositivos físicos que recopilan, procesan y transmiten datos mediante redes de comunicación, normalmente con mínima intervención humana (Ashton, 2009; ITU, 2022).

Esta tecnología ha evolucionado desde su concepción en 1999 (Kevin Ashton, MIT) hasta convertirse en un pilar de la Cuarta Revolución Industrial, permitiendo la automatización de procesos en sectores como:

- Industria 4.0 (monitoreo predictivo de maquinaria).
- Smart Cities (gestión de tráfico, alumbrado público).
- Salud (wearables, telemedicina).
- Domótica (hogares inteligentes con asistencia por voz).

(Universidad Europea, 2023; Panda Security, 2024).

Las aplicaciones del IoT se extienden a numerosos aspectos de la vida cotidiana, incluyendo la domótica, que permite el control automatizado del hogar (iluminación, temperatura, seguridad); los wearables, como relojes inteligentes y pulseras de actividad, que monitorizan la salud y el estado físico; y las ciudades inteligentes, que utilizan sensores y actuadores conectados para optimizar la gestión de recursos y servicios urbanos (Universidad

Europea, 2023). Estos son solo algunos ejemplos del impacto creciente del IoT en nuestra sociedad, no obstante, esta definición tecnológica presenta variaciones según el marco de referencia como por ejemplo, la Unión Internacional de Telecomunicaciones (ITU, 2022) define el IoT desde una perspectiva de interoperabilidad global, priorizando la necesidad de estándares que permitan la comunicación entre dispositivos de distintos fabricantes. En contraste, la Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2024) enfatiza que el IoT debe analizarse principalmente como un ecosistema de riesgos emergentes, en el que las debilidades de firmware, la falta de actualizaciones y el uso de credenciales por defecto representan amenazas constantes.

Por su parte, el National Institute of Standards and Technology (NIST, 2021) concibe el IoT desde un enfoque de gestión de riesgos, subrayando la importancia de integrar mecanismos de seguridad, privacidad y control de accesos durante todo el ciclo de vida de los dispositivos. Esta visión difiere de la ITU, que resalta los beneficios de la conectividad, al enfocarse más en las medidas preventivas necesarias para mitigar las vulnerabilidades.

En síntesis, mientras algunas definiciones privilegian una visión tecnológica (estándares, conectividad, automatización), otras lo hacen desde una perspectiva socioeconómica y de seguridad, considerando la privacidad, la confianza de los usuarios y el impacto de la adopción masiva de estas tecnologías. Esta diversidad de enfoques evidencia tanto el potencial del IoT como la urgencia de abordarlo desde una perspectiva integral que incluya las dimensiones técnicas, sociales y regulatorias.

Arquitectura básica del IoT

La arquitectura de una red IoT típicamente se divide en tres capas que son:

Tabla 1

Capas del modelo de arquitectura IoT y sus funciones principales

Capa	Componentes	Función	Ejemplo
Percepción	Sensores, actuadores, dispositivos	Recopilar datos del entorno (temperatura, movimiento, humedad).	Termostato inteligente (Nest).
Red	Wi-Fi, Bluetooth, Zigbee, LoRaWAN	Transmitir datos a servidores o gateways.	Router con protocolo MQTT.
Aplicación	Plataformas en la nube, software	Procesar datos y generar acciones automatizadas.	Dashboard de análisis en IoT.

Nota. La tabla muestra los componentes más comunes de cada capa del modelo IoT y su función dentro del flujo de operación del sistema. (Adaptado de Barbara, s.f.; Home - OWASP Top 10:2021, n.d.)

Impacto del IoT en la Sociedad

El Internet de las Cosas ha transformado de manera significativa múltiples sectores de la sociedad contemporánea, por ejemplo: en el ámbito doméstico, ha permitido la consolidación de los hogares inteligentes mediante dispositivos como cámaras de seguridad, asistentes virtuales y electrodomésticos conectados. En los negocios, el IoT impulsa procesos de automatización, gestión de inventarios y monitoreo en tiempo real, lo que incrementa la eficiencia y la competitividad empresarial (Statista, 2025).

En el sector salud, la implementación de dispositivos IoT ha facilitado el monitoreo remoto de pacientes, el control de insumos médicos y la detección temprana de emergencias, contribuyendo a mejorar la calidad de vida y a optimizar los recursos sanitarios (WHO, 2023). En paralelo, en el ámbito urbano, el IoT se integra en proyectos de ciudades inteligentes, mejorando la movilidad, el consumo energético y la seguridad pública (ITU, 2022).

No obstante, diferentes organismos subrayan visiones contrastantes, por ejemplo para ITU (2022), el IoT representa principalmente una oportunidad tecnológica que habilita innovación y desarrollo sostenible, en cambio, la ENISA (2024) enfatiza que esta misma expansión introduce riesgos sociales y de seguridad, como la exposición de datos personales, la vulnerabilidad de infraestructuras críticas y el aumento de ataques masivos mediante botnets. De manera similar, la OMS (2023) reconoce los beneficios del IoT en la atención sanitaria, pero advierte que un mal manejo de la información clínica puede comprometer la privacidad y la confianza en los servicios de salud.

De acuerdo con la Universidad Europea (2023), el IoT ha transformado la vida cotidiana mediante:

- Eficiencia energética a través de edificios inteligentes que regulan el consumo.
- Medicina preventiva como pulseras que monitorean ritmo cardíaco.
- Movilidad urbana como semáforos adaptativos basados en flujo vehicular.

Sin embargo, su adopción masiva también ha generado desafíos críticos como:

- Falta de estandarización debido a dispositivos con protocolos incompatibles.
- Ciberseguridad ya que el 70% de los dispositivos IoT tienen vulnerabilidades (Home - OWASP Top 10:2021, n.d.).

- Privacidad debido al riesgo de filtración de datos personales (CyberArk, 2024).

De acuerdo con estas posturas, se refleja un contraste entre una visión optimista centrada en la eficiencia y la modernización, y una visión crítica que advierte sobre la dependencia tecnológica, la exclusión digital en comunidades con menor acceso y los riesgos de vigilancia masiva, por lo que el impacto del IoT en la sociedad no debe analizarse únicamente desde sus beneficios técnicos, sino también desde sus implicaciones éticas, sociales y de seguridad.

Ejemplos Prácticos de IoT

Tabla 2.

Ejemplos de aplicaciones IoT y vulnerabilidades asociadas

Ámbito	Aplicación	Vulnerabilidad Asociada
Salud	Marcapasos conectados	Ataques que alteran ritmos cardíacos
Hogar	Cerraduras inteligentes	Hackeo por contraseñas predeterminadas (ESET, s.f.)
Industria	Robots autónomos en fábricas	Interceptación de datos de producción

Nota. La tabla presenta ejemplos comunes de aplicaciones de IoT en distintos sectores y las vulnerabilidades más frecuentes asociadas a su uso.

El Internet de las Cosas se manifiesta en aplicaciones concretas que permiten visualizar su impacto en distintos sectores. Estos ejemplos ilustran tanto los beneficios de la tecnología como los desafíos asociados a su implementación:

- **Sector salud.** Los hospitales incorporan dispositivos IoT para monitoreo remoto, rastreo de insumos y digitalización de historiales médicos, por ejemplo para la OMS (2023), estas tecnologías contribuyen a mejorar la calidad de vida y optimizar recursos sanitarios, pero la manipulación indebida de dispositivos médicos conectados o la filtración de datos sensibles puede tener consecuencias graves, desde violaciones a la privacidad hasta la afectación directa de la vida de los pacientes.
- **Hogares inteligentes.** La integración de cámaras de vigilancia, sensores de movimiento y electrodomésticos conectados aporta comodidad, eficiencia energética y seguridad doméstica, sin embargo, diversos estudios han demostrado que muchos de estos dispositivos son desplegados con configuraciones predeterminadas inseguras, lo que los convierte en objetivos frecuentes para ciberataques, por lo que para la ITU (2022) representa una innovación en calidad de vida, para ENISA (2024) implica un aumento en la superficie de ataque.
- **Entornos empresariales e industriales.** El IoT se utiliza en procesos de automatización, gestión de inventarios y mantenimiento predictivo, lo cual incrementa la competitividad y reduce costos. Según Statista (2025), el sector industrial concentra una de las mayores cuotas de adopción de IoT a nivel global, sin embargo, el NIST (2021) advierte que en este tipo de entornos el riesgo de intrusiones puede afectar directamente la continuidad de operaciones críticas, como ocurre en sistemas SCADA o de control industrial.

Importancia de la Seguridad en IoT

La seguridad en el Internet de las Cosas no constituye únicamente un aspecto técnico, sino un elemento esencial para garantizar la confiabilidad y sostenibilidad de los entornos

digitales actuales es por esto que a medida que los dispositivos conectados se integran en hogares, negocios y servicios públicos, se amplían las oportunidades de innovación, pero también los riesgos asociados a accesos no autorizados, filtración de datos y fallos en infraestructuras críticas (ENISA, 2024).

En el ámbito de la salud, la protección de los dispositivos IoT resulta indispensable para resguardar la privacidad de los pacientes y asegurar la continuidad de tratamientos que dependen de monitores remotos o bombas de insulina inteligentes (WHO, 2023). De igual manera, en entornos urbanos, la seguridad de los sistemas de transporte, alumbrado público o gestión energética se convierte en un factor clave para la resiliencia de las ciudades inteligentes.

Más allá de los sectores específicos, la seguridad en IoT se justifica desde la necesidad de proteger los principios fundamentales de la información como: la confidencialidad, integridad y disponibilidad (NIST, 2021), por lo que el compromiso de cualquiera de estos pilares puede tener impactos sociales y económicos de gran alcance, desde pérdidas financieras hasta riesgos para la misma vida humana. Adicionalmente, la importancia de fortalecer la seguridad en IoT radica en la creación de confianza entre los usuarios, empresas y gobiernos, y sin medidas adecuadas, la percepción de vulnerabilidad puede frenar la adopción de estas tecnologías, de tal manera que, organismos internacionales como ISO/IEC y NIST recomiendan que la seguridad se integre desde la fase de diseño y se mantenga de manera continua durante todo el ciclo de vida de los dispositivos (ISO/IEC, 2023).

Modelos y marcos de seguridad aplicables al IoT

Para mitigar los riesgos, resulta esencial aplicar marcos de seguridad reconocidos internacionalmente:

- **Modelo CIA (Confidencialidad, Integridad y Disponibilidad).** En el contexto de IoT, la confidencialidad se logra mediante cifrado de extremo a extremo y autenticación robusta; la integridad con firmas digitales y validación de firmware; y la disponibilidad con planes de redundancia y mecanismos de recuperación ante incidentes (ISO/IEC, 2023).
- **Zero Trust.** Este enfoque parte de la premisa de que ningún dispositivo ni red es confiable por defecto y en IoT, esto se traduce en segmentación de redes, autenticación continua, monitoreo permanente y restricciones basadas en roles y contexto (Microsoft, 2023).
- **Defense in Depth (Defensa en profundidad).** Este modelo recomienda implementar múltiples capas de seguridad en toda la arquitectura IoT, así, incluso si un atacante compromete un sensor o cámara, todavía deberá superar firewalls, sistemas de detección de intrusos y controles en la capa de aplicación (NIST, 2021).
- **Security by Design.** Este modelo plantea que la seguridad debe incorporarse desde la concepción del dispositivo y mantenerse durante todo su ciclo de vida. Lo cual implica limitar funciones innecesarias, habilitar solo los servicios esenciales, y ofrecer actualizaciones automáticas y firmadas digitalmente (ENISA, 2024).

Arquitectura de Redes IoT: Componentes y Seguridad por Capas

Modelo de Capas en IoT y sus Riesgos de Seguridad

Tabla 3.

Riesgos y Capas de IoT

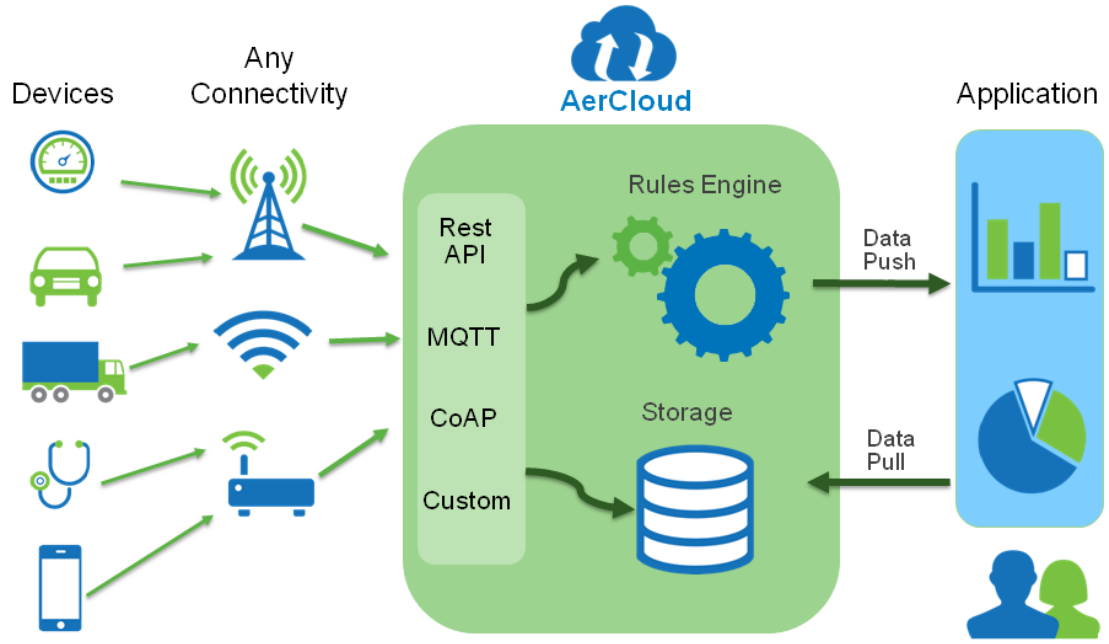
Capa	Componentes	Amenazas Comunes	Medidas de Protección
Percepción	Sensores, RFID, cámaras IoT	Spoofing, manipulación física, datos no cifrados	Autenticación TPM, cifrado AES-128, sellado antifraude
Red	Wi-Fi, Zigbee, LoRaWAN, MQTT	Man-in-the-Middle, DDoS, explotación de protocolos inseguros	Segmentación de red, VPN/IPSec, IDS/IPS
Procesamiento	Gateways, servidores locales (Edge), plataformas cloud	Alteración de algoritmos, acceso no autorizado, ejecución de código malicioso	Aislamiento de procesos, actualización de firmware segura, uso de entornos confiables
Almacenamiento	Bases de datos (SQL, NoSQL), servicios cloud (AWS, Azure)	Acceso no autorizado, pérdida de datos, ransomware	Cifrado en reposo, copias de seguridad, control de acceso basado en roles (RBAC)
Aplicación	APIs, plataformas cloud (AWS IoT)	Inyección SQL, APIs no autorizadas, filtración de datos	OAuth 2.0, WAF (firewall de aplicaciones web), cifrado de extremo a extremo (E2E)

Nota. Referencia de Home - OWASP Top 10:2021, n.d., s.f.; Barbara, s.f.; CyberArk (2024)

Diagrama de arquitectura IoT

Figura 1

Ejemplo de arquitectura general de una solución de IoT basada en la nube



Nota. La imagen muestra un ejemplo de la arquitectura general de una solución de IoT basada en la nube. Referencia tomada de Jecrespom. (2024).

En resumen, respecto a la *Figura 1*, los dispositivos IoT miden datos (por ejemplo: ritmo cardíaco, velocidad, temperatura), se conecta mediante una red (Wi-Fi, LTE, etc.), se realiza envío de datos usando protocolos (MQTT, REST API), AerCloud los procesa (a través de reglas) y los almacena. La aplicación final muestra gráficos, alertas o toma decisiones automáticas y adiciona pasa nuevamente a capa de almacenamiento.

Técnicas de Seguridad por Capa

En un sistema IoT, la seguridad debe implementarse de forma segmentada en cada capa de la arquitectura para mitigar riesgos específicos según el tipo de componentes y comunicaciones involucradas, ya que esto se conoce como un enfoque de seguridad por capas o defensa en profundidad, y se divide en:

A. Capa de Percepción. Esta capa incluye sensores, actuadores, etiquetas RFID y dispositivos embebidos.

Técnicas de seguridad recomendadas:

- Cifrado de datos en el dispositivo (por ejemplo, AES).
- Autenticación mutua entre sensores y gateways.
- Firmas digitales para validar firmware.
- Detección de manipulación física (tamper detection).

Ejemplo práctico: En 2023, se identificaron múltiples vulnerabilidades en termostatos inteligentes de marcas comerciales (como el modelo ficticio XYZ), los cuales fueron explotados por atacantes debido a la ausencia de autenticación en el firmware del dispositivo. Según ESET (s.f.), los atacantes aprovecharon que el firmware podía ser reemplazado o modificado sin verificación criptográfica, lo que permitió la instalación de software malicioso. Este ataque permitió el control remoto del termostato, la modificación de temperaturas sin autorización e incluso el uso del dispositivo como punto de entrada para movimientos laterales en redes domésticas. Este incidente evidenció la necesidad crítica de firmar y validar el firmware antes de

su ejecución, y de implementar controles de acceso incluso en dispositivos considerados "menores".

B. Capa de Red. Esta capa es responsable de la transmisión de datos entre los dispositivos IoT y otros nodos, como gateways, servidores o la nube. Utiliza diversos protocolos y tecnologías como Wi-Fi, ZigBee, LoRa, 5G, entre otros.

Técnicas de seguridad recomendadas:

- Segmentación VLAN: Aislar dispositivos IoT en redes separadas.
- VPN entre nodos críticos.
- Control de acceso mediante firewalls IoT.
    - Protocolos seguros como: over TLS (no usar MQTT sin cifrado). CoAP + DTLS para entornos con baja potencia.

Ejemplo real: El ataque de Mirai en 2016 es uno de los incidentes más emblemáticos que afectó a la capa de red en el ecosistema IoT. Este malware escaneaba Internet en busca de dispositivos IoT (como cámaras IP, grabadoras de video, routers domésticos) que todavía usaban credenciales predeterminadas o débiles. Una vez infectados, estos dispositivos eran reclutados en una botnet masiva para ejecutar ataques DDoS (Denegación de Servicio Distribuida) contra sitios web y servicios DNS.

Según Panda Security (2024), el ataque llegó a generar un tráfico de más de 1 Tbps, afectando plataformas globales como Twitter, Netflix, Reddit y Spotify, dejando en evidencia la falta de medidas de autenticación y segmentación en la capa de red.

C. Capa de Procesamiento. Esta capa se encarga de analizar, procesar y tomar decisiones a partir de los datos generados por los dispositivos IoT. Puede incluir gateways inteligentes, edge computing y plataformas de análisis en tiempo real.

Técnicas de seguridad recomendadas:

- Ejecución en entornos de confianza (Trusted Execution Environments, TEE).
- Aislamiento de procesos y uso de contenedores seguros.
- Validación y actualización segura del firmware/software.
- Registro y auditoría de procesos automáticos (logs firmados).
- Protección contra ejecución de código malicioso mediante listas blancas (*whitelisting*).

Ejemplo Practico: En junio de 2023, se identificaron múltiples vulnerabilidades críticas en routers celulares industriales utilizados en entornos de manufactura y energía. Estas fallas permitían a atacantes remotos ejecutar código arbitrario y manipular procesos industriales al explotar debilidades en la conexión entre dispositivos IIoT y plataformas de gestión en la nube. La explotación de estas vulnerabilidades evidenció la necesidad de fortalecer la seguridad en la capa de procesamiento, especialmente en entornos industriales donde las consecuencias pueden ser significativas Dark Reading. (2024, junio 10).

D. Capa de Almacenamiento. Es la encargada de guardar los datos generados por los dispositivos, procesados o no, ya sea localmente (on-premise) o en la nube. Involucra bases de datos, servicios de almacenamiento distribuido y sistemas de respaldo.

Técnicas de seguridad recomendadas:

- Cifrado de datos en reposo (ej. AES-256).

- Control de acceso basado en roles (RBAC).
- Mecanismos de respaldo y recuperación (backup y disaster recovery).
- Auditoría de accesos y trazabilidad (*logging* seguro).
- Almacenamiento redundante para garantizar disponibilidad (RAID, replicación).

Ejemplo práctico: En 2024, la plataforma de almacenamiento en la nube Snowflake sufrió una brecha de seguridad que afectó a más de 160 organizaciones, incluyendo empresas de telecomunicaciones, bancos y servicios de salud. Los atacantes explotaron configuraciones incorrectas en los entornos de los clientes, accediendo a datos sensibles como información personal identificable y registros de llamadas. Este incidente resaltó la importancia de implementar medidas de seguridad robustas en la capa de almacenamiento, especialmente en plataformas en la nube utilizadas por múltiples organizaciones Wikipedia contributors 2024. (n.d.).

E. Capa de Aplicación. La capa de aplicación es la encargada de permitir la interacción del usuario con el sistema IoT, ya sea mediante interfaces gráficas (apps móviles, dashboards web) o APIs que facilitan el control, monitoreo y análisis de los dispositivos conectados.

Técnicas de seguridad recomendadas:

- Validación de entradas del usuario (prevención de ataques XSS, SQLi).
- Gestión segura de sesiones (tokens, expiración, cookies seguras).
- Uso de HTTPS en todas las comunicaciones.
- Autenticación fuerte (2FA).

- Registro y auditoría de acciones del usuario.

Ejemplo práctico: En 2021, de acuerdo con The Hacker News. (2021, 13 de enero) se descubrió una vulnerabilidad crítica en la aplicación móvil de control de cámaras Ring de Amazon, que permitía a un atacante interceptar las credenciales del usuario mediante un ataque Man-in-the-Middle (MitM) si el usuario accedía a la app desde una red Wi-Fi no segura. La app, en versiones anteriores, no validaba adecuadamente los certificados SSL, lo que permitió a investigadores de seguridad simular un servidor falso y capturar datos de acceso, incluyendo tokens de sesión. Con esos datos, un atacante podía visualizar transmisiones de video en vivo, acceder a grabaciones almacenadas en la nube e incluso activar el micrófono y el altavoz de las cámaras.

Este caso evidenció la necesidad de implementar validaciones estrictas de certificados, obligar el uso de conexiones seguras (HTTPS) y alertar a los usuarios cuando se conectan a redes públicas o abiertas. El incidente fue corregido posteriormente por Amazon, pero demostró que una falla en la capa de aplicación puede comprometer completamente la privacidad del usuario final.

Seguridad en redes IoT

La seguridad en redes IoT hace referencia al conjunto de políticas, prácticas y tecnologías destinadas a proteger la integridad, confidencialidad y disponibilidad de los dispositivos, la infraestructura y los datos, por ejemplo: Newman, S. (2025, April 8) destaca la importancia de abordar los desafíos de seguridad en el IoT para proteger la privacidad de los usuarios y la integridad de los sistemas, a diferencia de las redes tradicionales, donde los dispositivos suelen

seguir estándares consolidados, en IoT conviven equipos con distintos niveles de madurez en ciberseguridad, lo que incrementa las vulnerabilidades (ENISA, 2024).

Aunque organismos como NIST (2021) proponen un enfoque estructurado basado en control de acceso, autenticación y gestión de vulnerabilidades, su aplicación práctica en entornos domésticos y pequeñas empresas enfrenta limitaciones. ENISA (2024) advierte que la mayoría de los dispositivos IoT de consumo no incluyen soporte para actualizaciones seguras, lo que dificulta el cumplimiento de los estándares propuestos. Esto sugiere que la seguridad en IoT no solo es un desafío técnico, sino también económico y regulatorio.

Principales Vulnerabilidades

De acuerdo con OWASP Foundation (s.f.) identifica las siguientes vulnerabilidades críticas en dispositivos IoT:

Tabla 4.

Ranking de vulnerabilidades IoT

Ranking	Vulnerabilidad	Impacto	Ejemplo
1	Contraseñas débiles/ predeterminadas	Acceso no autorizado a dispositivos	Ataque a cámaras IP con credenciales admin:admin (ESET, s.f.)
2	Interfaces de red inseguras	Exposición de APIs o puertos sin autenticación	Hackeo a cerraduras inteligentes via API expuesta (Panda Security, 2024)
3	Falta de actualizaciones	Explotación de vulnerabilidades conocidas	Botnet Mirai que infectó routers obsoletos
4	Cifrado ausente o débil	Interceptación de datos sensibles	Filtración de datos médicos de wearables (CyberArk, 2024)
5	Mala gestión de permisos	Escalación de privilegios	Manipulación remota de sistemas industriales

Nota. La tabla muestra las principales vulnerabilidades presentes en el ecosistema IoT, ordenadas según su frecuencia e impacto identificado en reportes de seguridad recientes.

Estas amenazas han sido ampliamente documentadas en incidentes como la botnet Mirai, que explotó dispositivos IoT inseguros para ejecutar ataques masivos de denegación de servicio (NIST, 2021).

Estadísticas Clave

El crecimiento exponencial de los dispositivos IoT ha traído consigo un incremento proporcional en los riesgos de seguridad. A continuación, se presentan estadísticas recientes que evidencian la urgencia de implementar mecanismos de protección robustos en cada capa de la arquitectura IoT:

Crecimiento de dispositivos IoT. Según Statista (2025), se estima que para el año 2025 habrá más de 30 mil millones de dispositivos IoT conectados en el mundo, lo que representa un aumento de más del 300% respecto a 2015, por lo que esta expansión no solo ocurre en hogares inteligentes, sino también en sectores críticos como salud, industria, agricultura y ciudades inteligentes.

Aumento de ataques dirigidos a IoT. El informe de Kaspersky (2023) reveló que los ataques a dispositivos IoT aumentaron un 41% respecto al año anterior, detectando más de 1.600 millones de intentos de intrusión solo en el primer semestre y las formas más comunes de ataque incluyen fuerza bruta de credenciales, malware de botnets y explotación de vulnerabilidades en firmware desactualizado. Según el informe de ZipDo (2024), el 25% de los ciberataques dirigidos a organizaciones, involucrarán dispositivos IoT para 2025.

Dispositivos con configuraciones inseguras. El informe de JumpCloud (2025) indica que más del 50% de los dispositivos IoT tienen vulnerabilidades críticas que los hackers pueden explotar actualmente y el mismo informe de JumpCloud (2025) señala que las fallas de seguridad en IoT cuestan a las empresas un promedio de $330,000 por incidente.

Estas cifras confirman que el IoT representa un campo con alta exposición al riesgo, pero también con oportunidades para mejorar la postura de seguridad desde el diseño, por lo que las

estadísticas sirven como fundamento para justificar la necesidad de aplicar medidas de defensa en profundidad.

Casos Reales de Ataques

Ataque a Hospitales con Bombas de Insulina IoT (2023)

- Vulnerabilidad: Dispositivos médicos con firmware sin firmar digitalmente.
- Ataque: Manipulación remota de dosis administradas.
- Fuente: *CyberArk (2024)*.

Botnet "Meris" (2024)

- Método: Infección de routers IoT mediante exploits en protocolo TR-069.
- Impacto: Ataques DDoS de 21 millones de solicitudes por segundo.
- Fuente: *Panda Security (2024)*.

Protocolos de Seguridad en IoT: Mecanismos de Protección para Comunicaciones Seguras

Clasificación de Protocolos de Seguridad para IoT

Los protocolos de seguridad en IoT deben equilibrar robustez con eficiencia energética por lo que estos se categorizan en:

Protocolos de Cifrado.

- ***TLS/SSL***. Estándar para comunicaciones cliente-servidor (ej. AWS IoT Core)
- **DTLS.** Versión para UDP usada en CoAP
- **AES-128/256.** Cifrado simétrico para dispositivos limitados

Protocolos de Autenticación.

- **OAuth 2.0.** Para autorización en APIs
- **X.509.** Certificados digitales en arquitecturas PKI
- **MQTT-SN.** Con autenticación por tokens JWT

Protocolos de Integridad.

- **HMAC**. Códigos de autenticación de mensajes
- **SHA-256**. Hash para verificación de firmware

(Fuente: NIST IR 8259A, 2021; Barbara, s.f.)

Vulnerabilidades en Protocolos Comunes

MQTT sin Autenticación puede ser un riesgo ya que Broker comprometido puede inyectar mensajes por lo que la solución a estos riesgos es usar Mosquitto con plugin auth-by-topic

CoAP sin DTLS, se conocen de casos reales como ataque a sensores de infraestructura urbana (OWASP, 2023), por lo que una solución a estos riesgos es implementar OSCORE para cifrado objeto-a-objeto

Zigbee sin AES-128, un ejemplo puede ser la interceptación de llaves inteligentes Z-Wave por lo que la recomendación es actualizar a Zigbee 3.0 con seguridad de malla

ISO/IEC 27032:2023: Nuevo estándar para seguridad en IoT Edge ISO/IEC 27030

Buenas Prácticas de Seguridad en IoT: Estrategias para Implementación Segura

Política de Seguridad IoT para Organizaciones

Requisitos Mínimos (Basados en NIST SP 800-82):

- Inventario de dispositivos: Mantener registro de todos los activos IoT con: Modelo, firmware, protocolos usados y fechas de actualización y vulnerabilidades conocidas
- Control de acceso mediante autenticación multifactor (MFA) para administración y principio de mínimos privilegios (Zero Trust)
- Protección de datos a través de cifrado AES-256 para datos en tránsito/reposo y anonimización de datos sensibles (ej: GDPR para wearables)

Checklist de Hardening para Dispositivos IoT

Tabla 5.

Checklist de Hardening

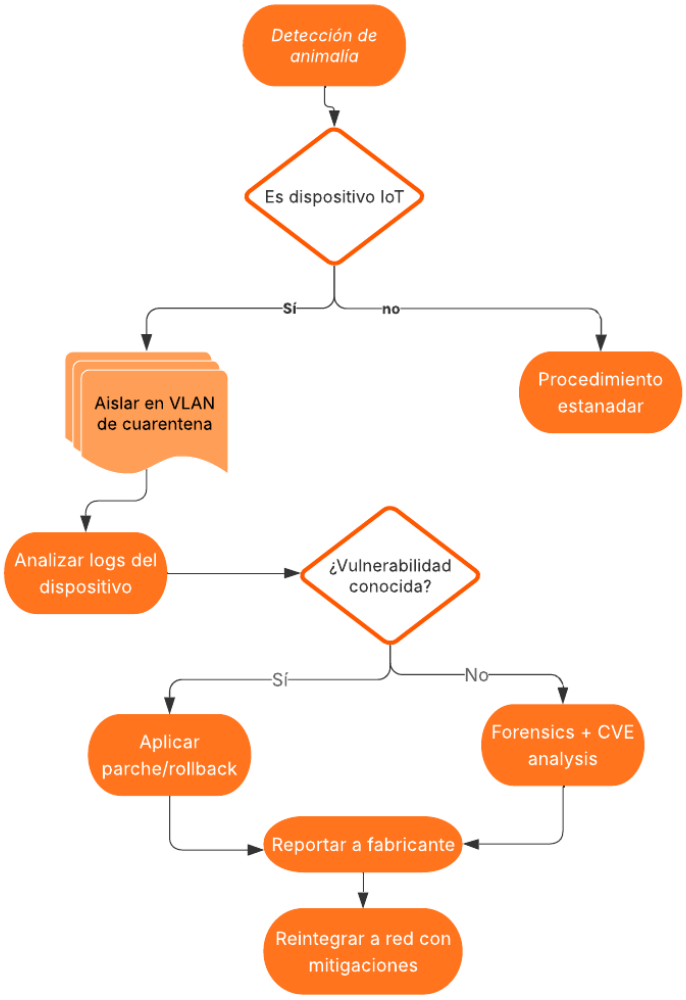
Área	Acción	Herramientas Recomendadas
Autenticación	Cambiar credenciales predeterminadas	OpenSSL para generar claves
Red	Segmentar red IoT en VLAN separada	Cisco ISE, pfSense
Cifrado	Habilitar TLS 1.3 + ECDSA	Let's Encrypt (certificados)
Firmware	Parchear mensualmente	Microsoft Azure Device Update
Monitorización	Implementar SIEM para detección de anomalías	Splunk IoT

Nota. Tabla adaptada de OWASP IoT Security Verification Standard (2024).

Flujograma de Respuesta a Incidentes en IoT

Figura 2.

Flujograma IoT



Nota. La imagen muestra un flujograma de ejemplo sobre el proceso ante incidentes en IoT

Ejemplo práctico: *"En 2023, un ataque a termostatos industriales se mitigó aislando los dispositivos y revocando certificados comprometidos en promedio 2 horas"* (Panda Security, 2024).

Estrategias por Capa Tecnológica

Capa Física. Como estrategias para la capa física:

- Protección anti-tampering (consiste en un conjunto de tecnologías diseñadas para evitar la manipulación y alteración de los sistemas de seguridad) a través de sellados inviolables y sensores de apertura
- TPM (Trusted Platform Module) consiste en un chip de seguridad basado en hardware, integrado en la placa base de un ordenador para almacenar claves criptográficas.

Capa de Red. Como estrategias se puede mencionar:

- Network Segmentation al usar Zonas DMZ para dispositivos IoT críticos.
- Protocolos seguros como MQTT over WebSockets + TLS (puerto 443 para evadir bloqueos) y IPSec para comunicaciones gateway-to-cloud

Capa de Aplicación. Como estrategia se recomienda:

- Secure Coding Validar inputs en APIs REST (evitar inyección SQL).
- Usar JWT con expiración corta (menor a 15 minutos), esto ayuda a minimizar el riesgo de uso indebido o robo del token. La aplicación debe verificar la fecha de caducidad del token

Caso de Éxito: Intervención IoT para la Seguridad del Paciente en Hospital de Ontario, Canadá

Uno de los sectores más sensibles y desafiantes para implementar redes IoT seguras es el de salud, debido a la naturaleza crítica de los datos, la variedad de dispositivos médicos conectados y la necesidad de cumplir con normativas de privacidad y protección de datos.

En el año 2022, un hospital en Ontario, Canadá, implementó una serie de intervenciones IoT en una unidad hospitalaria con el objetivo de mejorar la seguridad del paciente, por lo que entre las medidas desplegadas se incluyeron camas inteligentes, estaciones de higiene de manos, insignias RFID, estaciones móviles de monitoreo y sistemas para alertar sobre caídas de pacientes.

Retos identificados:

- Alta frecuencia de caídas de pacientes, especialmente en mayores de 75 años, lo que representaba un riesgo para la integridad física.
- Necesidad de mejorar el cumplimiento de los protocolos de higiene de manos, lo que afecta directamente la prevención de infecciones hospitalarias.
- Resistencia inicial a nuevas tecnologías por parte del personal y ajustes en los procesos operativos para incorporar los sistemas IoT.

Solución adoptada:

- Diseño de la intervención IoT con dispositivos que alertan visualmente cuando se requiere higiene de manos y registro automático del cumplimiento.
- Instalación de sistemas de notificación para caídas de pacientes, integrados con sensores en camas y dispositivos móviles de alerta.
- Capacitación del personal clínico en el uso de los dispositivos y sensibilización frente al riesgo de caídas e infecciones.

Resultados logrados:

- Reducción significativa en la tasa de caídas de pacientes tras la intervención.

- Mejora en el cumplimiento de protocolos de higiene de manos, lo que contribuye a reducir infecciones relacionadas.
- Mejor percepción por parte del personal de la seguridad de los pacientes y de los procesos hospitalarios.

Referencia Yesmin, T., Carter, M. W., & Gladman, A. S. (2022). Internet of things in healthcare for patient safety: an empirical study. *BMC Health Services Research*, *22*(1). https://doi.org/10.1186/s12913-022-07620-3

Si bien las buenas prácticas definidas por ISO/IEC 27030 (2023) promueven la seguridad desde el diseño y la gestión integral de los dispositivos, los resultados de la encuesta reflejan un bajo nivel de adopción. Esta brecha evidencia la falta de políticas públicas y de formación técnica en seguridad digital, especialmente en contextos domésticos donde las configuraciones por defecto siguen siendo la norma.

Estrategias Actuales y Emergentes en Seguridad para IoT en 2025

En 2025, la seguridad en el Internet de las Cosas (IoT) ha adoptado enfoques más robustos y proactivos frente a un panorama de amenazas creciente y según Blanton (2025), “el 88 % de los profesionales de TI creen que los dispositivos IoT representan una amenaza real para sus organizaciones”, lo que ha llevado a una rápida adopción de nuevas estrategias de mitigación. Por lo que damos a conocer las más relevantes:

Modelo de Confianza Cero (Zero Trust)

El modelo de seguridad de Confianza Cero se ha consolidado como una práctica estándar en entornos IoT, ya que este enfoque asume que ninguna entidad, interna o externa, es confiable por defecto, requiriendo una verificación continua de identidad y comportamiento para acceder a

recursos, así, la implementación de arquitecturas de Confianza Cero ha demostrado ser eficaz para mitigar riesgos asociados a dispositivos comprometidos dentro de la red Blanton, S. (2025).

Seguridad desde el diseño (Security by Design)

Las organizaciones están incorporando la ciberseguridad desde las etapas iniciales de diseño y desarrollo de dispositivos IoT, esto incluye la implementación de procesos de arranque seguro, actualizaciones de firmware firmadas digitalmente y mecanismos de autenticación robustos, también se promueve la transparencia mediante la adopción de listas de materiales de software (SBOM), facilitando la identificación y gestión de vulnerabilidades en la cadena de suministro de software (Ly & Ly, 2025).

Aplicación de Criptografía Post-Cuántica

Ante la amenaza emergente de la computación cuántica, se están adoptando algoritmos de criptografía resistentes a ataques cuánticos en dispositivos IoT, por ejemplo, proveedores de telecomunicaciones están probando tarjetas SIM que incorporan algoritmos de criptografía post-cuántica seleccionados por el NIST, como CRYSTALS-Kyber, para proteger las comunicaciones móviles (Ly & Ly, 2025).

Implementación de Blockchain para la Seguridad de IIoT

La tecnología blockchain se está utilizando para mejorar la seguridad en entornos de IoT industrial (IIoT), al proporcionar un registro inmutable de transacciones y autenticaciones, blockchain ayuda a garantizar la integridad de los datos y la autenticidad de los dispositivos, fortaleciendo la confianza en sistemas distribuidos (*Trend Report: The Most Important IIoT Trends in 2025*, n.d.), por lo que en IIoT, esto permite registrar transacciones entre sensores sin un servidor central, asegurando la trazabilidad de procesos sin riesgo de manipulación.

Certificación de dispositivos inteligentes

Iniciativas como la marca "US Cyber Trust Mark" han sido lanzadas para ayudar a los consumidores a identificar dispositivos inteligentes que cumplen con estándares específicos de seguridad cibernética, por lo que esta certificación, similar a la etiqueta Energy Star para eficiencia energética, indica que un dispositivo ha sido probado y cumple con criterios como la emisión de actualizaciones de software y la transferencia segura de datos a la nube (Feiner, 2025).

Convergencia de Seguridad Física y Cibernética

La integración de funciones de seguridad física y cibernética dentro de las organizaciones, conocida como convergencia de seguridad, se está volviendo cada vez más común y este enfoque permite una gestión de riesgos más coherente y eficaz, abordando las amenazas híbridas que afectan tanto a activos físicos como digitales.

La aplicada a detección de amenazas

Finalmente, la inteligencia artificial ha alcanzado una madurez operativa significativa. Según Bryghtpath (2025), “la IA es capaz de detectar anomalías en el comportamiento de dispositivos IoT que un equipo humano no podría reconocer en tiempo real”, por lo que esta capacidad predictiva permite responder de forma preventiva, antes de que una amenaza se materialice, adicional, estas tecnologías permiten analizar patrones de comportamiento de dispositivos, identificar anomalías que puedan indicar una brecha de seguridad y proporcionar alertas tempranas para una respuesta proactiva

Implementación de Honeypots

Panasonic ha desarrollado una estrategia proactiva para mejorar la seguridad de sus dispositivos IoT mediante la implementación de honeypots, denominados "Astira", que simulan dispositivos reales para atraer y analizar malware, ya que esta iniciativa ha permitido a la empresa capturar y estudiar diversas cepas de malware, contribuyendo al desarrollo del Módulo de Resiliencia e Inmunidad contra Amenazas (Threim), que detecta y bloquea malware en sus dispositivos. En pruebas realizadas, Threim logró una tasa de detección del 86% en dispositivos con procesadores ARM (Newman, 2023).

Estándar Europeo EN 17927 (SESIP)

En Europa, se ha establecido el estándar EN 17927, también conocido como Security Evaluation Standard for IoT Platforms (SESIP), que proporciona una metodología para realizar evaluaciones de ciberseguridad en productos y componentes dentro del ecosistema IoT, en este estándar se introduce cinco niveles de aseguramiento, permitiendo evaluaciones escalables según la complejidad e intención de uso del producto

Esquema de Etiquetado de Ciberseguridad en Singapur

Singapur ha implementado el Cybersecurity Labelling Scheme (CLS), un esquema que califica los dispositivos inteligentes según su nivel de ciberseguridad, y este sistema ayuda a los consumidores a tomar decisiones informadas y motiva a los fabricantes a mejorar la seguridad de sus productos, además, Singapur ha establecido acuerdos de reconocimiento mutuo con países como Finlandia y Alemania para facilitar el acceso al mercado y la conformidad con estándares internacionales (*IoT Cybersecurity Landscape in 2024 | 1NCE*, n.d.).

Aplicación Estratégica de la Seguridad por Capas en Entornos IoT: ¿Cómo, Por Qué y Para Qué?

La aplicación efectiva de estrategias de seguridad por capas en redes IoT no debe limitarse a la teoría, sino que debe traducirse en acciones prácticas, sostenibles y adaptables a diferentes contextos y para lograrlo, es fundamental responder a tres preguntas clave: ¿cómo se aplican?, ¿por qué son necesarias? y ¿para qué sirven?

Como aplicarlas

La implementación de estrategias por capas se realiza integrando soluciones específicas en cada una de las capas de la arquitectura IoT:

- En la capa de percepción, se deben incorporar sensores con firmware firmado digitalmente, cifrado local de datos y mecanismos anti-manipulación física. Ejemplo: uso de chips TPM y actualización segura mediante OTA (Over-The-Air).
- En la capa de red, se debe aplicar segmentación VLAN, protocolos como MQTT sobre TLS, y firewalls especializados. Ejemplo: una red hospitalaria que separa sensores médicos de redes administrativas.
- En la capa de procesamiento, es necesario habilitar entornos de ejecución confiables (TEE), contenedores seguros como Docker con políticas AppArmor, y validación de integridad de software. Ejemplo: edge computing en un gateway con análisis de datos locales.
- En la capa de almacenamiento, se recomienda el cifrado en reposo (ej. AES-256), replicación de datos, RBAC y herramientas de backup. Ejemplo: bases de datos de pacientes protegidas en AWS HealthLake o Azure Cosmos DB.

- En la capa de aplicación, se aplican prácticas de desarrollo seguro como autenticación 2FA, validación de entradas, control de sesiones, y auditoría centralizada. Ejemplo: dashboards médicos con roles diferenciados para médicos, técnicos y pacientes.

¿Por qué aplicarlas?

La adopción de estrategias de seguridad por capas en entornos IoT responde a la necesidad de hacer frente a un panorama de amenazas cada vez más complejo y dinámico, ya que a diferencia de las redes tradicionales, el ecosistema IoT presenta una combinación de dispositivos heterogéneos, muchos de ellos con recursos limitados, conectados de forma permanente y en entornos altamente distribuidos y esto los convierte en objetivos atractivos para atacantes que buscan vulnerabilidades fáciles de explotar.

Aplicar medidas específicas en cada capa permite establecer múltiples líneas de defensa, de forma que, si una de ellas falla, las siguientes puedan contener o mitigar el impacto. Esta filosofía de seguridad, conocida como defensa en profundidad, se ha convertido en una práctica recomendada por organismos como la ISO/IEC 27001, el NIST y la ENISA, debido a su eficacia comprobada en proteger infraestructuras críticas.

Además, estas estrategias se aplican por las siguientes razones clave:

- Reducción de la superficie de ataque: Cada capa representa un punto potencial de entrada para ciberatacantes al proteger individualmente cada una, se limita la posibilidad de acceso no autorizado o manipulación de datos.
- Prevención de ataques persistentes: Muchas amenazas actuales como el ransomware o los ataques APT (Advanced Persistent Threats) se propagan lateralmente en la red y una arquitectura segmentada con controles por capa frena esa expansión.

- Minimización del impacto financiero y reputacional: Los ciberataques en entornos IoT pueden generar parálisis operativa, pérdida de datos sensibles o incluso riesgos para la vida humana (en el caso de dispositivos médicos) ya que las medidas preventivas ayudan a evitar costos legales, operativos y de reputación.
- Cumplimiento normativo: Diversos sectores como salud, banca, manufactura o ciudades inteligentes están regulados por normas que exigen controles estrictos de seguridad, por ejemplo, la Ley General de Protección de Datos Personales en Colombia, el GDPR en Europa o la HIPAA en EE. UU. exigen protección técnica y organizativa de la información procesada por dispositivos IoT.
- Adaptabilidad y escalabilidad segura: La segmentación por capas permite escalar las soluciones IoT sin comprometer la seguridad, ya que a medida que se agregan nuevos sensores, aplicaciones o plataformas, se pueden integrar directamente en la capa correspondiente con sus respectivas protecciones.

¿Para qué aplicarlas?

Las estrategias de seguridad por capas en entornos IoT no solo se implementan como medidas preventivas, sino como elementos habilitadores de confianza, funcionalidad y sostenibilidad tecnológica en sistemas altamente interconectados y su aplicación permite a las organizaciones operar, innovar y escalar soluciones IoT sin comprometer la integridad, disponibilidad ni confidencialidad de los datos.

Estas estrategias sirven, principalmente, para:

- Garantizar la continuidad operativa de servicios críticos
- Proteger la privacidad del usuario final

- Facilitar la toma de decisiones confiables
- Impulsar la innovación segura
- Mejorar la resiliencia organizacional
- Fomentar la interoperabilidad sin sacrificar la seguridad

Encuesta sobre Uso y Seguridad en Dispositivos IoT

Con el fin de conocer las prácticas actuales de seguridad adoptadas por usuarios de dispositivos IoT en entornos residenciales y empresariales, se diseñó un cuestionario breve, donde el propósito principal de esta encuesta fue identificar los hábitos de configuración, actualización y monitoreo de los equipos, así como el nivel de conocimiento que los usuarios poseen sobre medidas de seguridad aplicables a este tipo de tecnologías.

La encuesta estuvo dirigida a usuarios de cámaras de seguridad, sensores de movimiento y alarmas, con el fin de contar con una visión cercana de cómo se emplean y protegen los dispositivos IoT en contextos cotidianos.

A continuación, se presentan las preguntas del cuestionario:

1. ¿En qué tipo de espacio utiliza dispositivos IoT? (Vivienda, Negocio, Ambos).
2. ¿Qué dispositivos IoT utiliza actualmente?
3. ¿Quién configuró inicialmente el dispositivo?
4. ¿Cambió la contraseña predeterminada del dispositivo?
5. ¿Conoce o utiliza protocolos de comunicación seguros?
6. ¿Realiza actualizaciones periódicas de firmware en sus dispositivos?

7. ¿Qué medidas de seguridad aplica en su red Wi-Fi?
8. ¿Monitorea el estado de sus dispositivos IoT regularmente?
9. ¿Cómo percibe la vulnerabilidad de sus dispositivos frente a ciberataques?
10. En caso de falla o incidente de seguridad, ¿sabe qué acciones tomar?
11. ¿Le interesaría contar con una guía práctica de seguridad para IoT?

Al concluir la presentación del cuestionario, resulta necesario detallar el proceso seguido para su diseño, aplicación y análisis, por lo que en este sentido, se expone de manera explícita la metodología de investigación, describiendo las fuentes consultadas, los criterios de selección de información, las etapas del estudio y el procedimiento aplicado para la recolección y análisis de los datos obtenidos a través de la encuesta.

Desarrollo y Metodología

Enfoque de la investigación

La investigación se desarrolló bajo un enfoque descriptivo y analítico, combinando la revisión documental de fuentes académicas e institucionales con el levantamiento de información empírica a través de una encuesta aplicada a usuarios de dispositivos IoT en entornos domésticos y empresariales, por lo que este enfoque permitió no solo describir las principales características y riesgos asociados al Internet de las Cosas, sino también contrastar las percepciones y prácticas de seguridad de los usuarios con los lineamientos propuestos por organismos internacionales como ENISA (2024), NIST (2021) e ITU (2022).

Fuentes de información

Para el desarrollo de esta investigación se recurrió a una combinación de fuentes primarias y secundarias que permitieron obtener una visión completa, actual y fundamentada del estado de la seguridad en entornos de IoT, los cuales se describen a continuación de acuerdo a los tipos de información recopilada y los criterios empleados para su selección.

Fuentes primarias

Se aplicó una encuesta dirigida a 20 usuarios de IoT en Bogotá, entre viviendas particulares y negocios, enfocados principalmente en cámaras de seguridad, alarmas, sensores de movimiento y dispositivos de contro de acceso.

Fuentes secundarias

Se revisaron artículos académicos, reportes institucionales y documentos técnicos de organismos internacionales (ENISA, NIST, ISO, ITU, OMS, ISO/IEC), seleccionando aquellos

con vigencia entre 2019 y 2025 y que abordaran aspectos de seguridad, privacidad, riesgos y buenas prácticas en IoT.

Criterios de selección

Se priorizaron fuentes con reconocimiento internacional, actualidad en el tema y pertinencia directa con el problema de investigación.

Diseño de la investigación

El desarrollo de la investigación se estructuró en cuatro etapas:

Revisión documental

Análisis de definiciones, marcos normativos y estrategias de seguridad propuestas en literatura académica y técnica.

Diseño de la guía práctica

Elaboración de un manual con medidas y buenas prácticas para la implementación segura de redes IoT.

Construcción y aplicación de la encuesta

Cuestionario de 10 preguntas cerradas y mixtas orientado a identificar las prácticas de seguridad en usuarios de IoT en viviendas y negocios.

Tabulación y análisis de resultados

Organización de datos en tablas y gráficos, seguidos de un análisis descriptivo y comparativo con la literatura consultada.

Instrumento de recolección de datos

El instrumento empleado fue una encuesta estructurada compuesta por preguntas cerradas (dicotómicas y de opción múltiple) y preguntas mixtas, donde su diseño buscó obtener información sobre: Nivel de adopción de medidas básicas de seguridad en IoT, conocimiento y uso de protocolos seguros de comunicación, prácticas de actualización de firmware y cambio de contraseñas, percepción de vulnerabilidad frente a amenazas en IoT y disposición de los usuarios para recibir guías de seguridad.

Población y muestra

La población objetivo fueron usuarios de dispositivos IoT en contextos residenciales y empresariales de pequeña escala, donde la muestra estuvo conformada por 20 participantes seleccionados mediante un muestreo no probabilístico de conveniencia, lo cual permitió acceder a casos representativos del uso cotidiano de cámaras, sensores y alarmas en el sector doméstico e industrial en la ciudad de Bogotá.

Análisis de la información

Los datos recolectados fueron organizados y procesados en hojas de cálculo, generando tablas y gráficos descriptivos y posteriormente, se efectuó un análisis interpretativo en el que los resultados fueron contrastados con la revisión documental, lo cual permitió identificar brechas de seguridad entre las prácticas actuales de los usuarios y las recomendaciones establecidas por organismos internacionales.

Análisis de Resultados

Los resultados permitieron identificar varios hallazgos relevantes:

Tipo de espacio y dispositivos utilizados

El 55% de los encuestados usa IoT en negocios, el 20% en viviendas y el 25% en ambos. Los dispositivos más comunes son cámaras de seguridad (presentes en más del 90% de los casos), seguidos por sensores de movimiento o humo y alarmas inteligentes.

Figura 3.

Grafica espacio

Nota. La imagen muestra el resultado obtenido en la encuesta, con respecto a el tipo de espacio y dispositivos utilizados

Figura 4.

Grafica dispositivos utilizados

Nota. La imagen muestra el resultado obtenido en la encuestade acuerdo con los dispositivos mas utilizados

Configuración inicial

En el 60% de los casos, la instalación fue realizada por personal de la empresa vendedora. El 25% fue configurado por técnico especializado, y el 15% no lo recuerda lo que sugiere poca apropiación técnica por parte de los usuarios finales.

Figura 5.

Grafica de configuración de los dispositivos

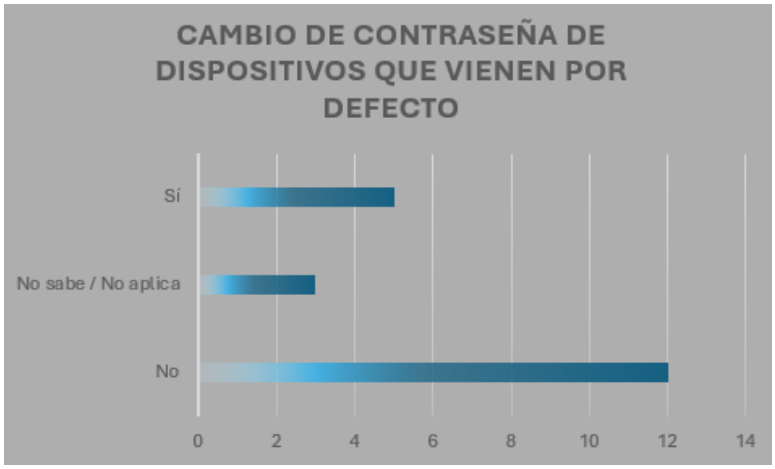
Nota. La imagen muestra el resultado obtenido en la encuesta, donde se identifica quien realiza la configuración de los dispositivos

Cambio de contraseñas por defecto

Solo el 25% de los encuestados afirmó haber cambiado las contraseñas predeterminadas, mientras que un 15% manifestó no saber o no aplicar esta medida, lo cual representa una debilidad crítica en la seguridad básica de los dispositivos. Esto coincide con el OWASP IoT Top 10 (2021), que señala el uso de credenciales por defecto como una de las vulnerabilidades más frecuentes en entornos IoT.

Figura 6.

Grafica sobre cambio de contraseñas



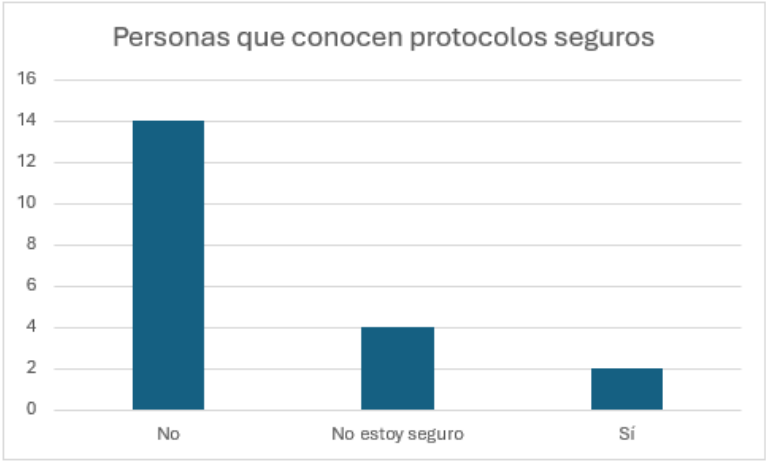
Nota. La imagen muestra el resultado obtenido en la encuesta de acuerdo con el cambio de contraseñas que vienen por defecto en los dispositivos

Conocimiento de protocolos seguros

El 70% de los participantes indicó no conocer si sus dispositivos utilizan cifrado o protocolos seguros, y un 20% expresó no estar seguro, y esto refleja una falta general de conciencia sobre mecanismos básicos de protección de datos.

Figura 7.

Grafica de conocimiento en protocolos



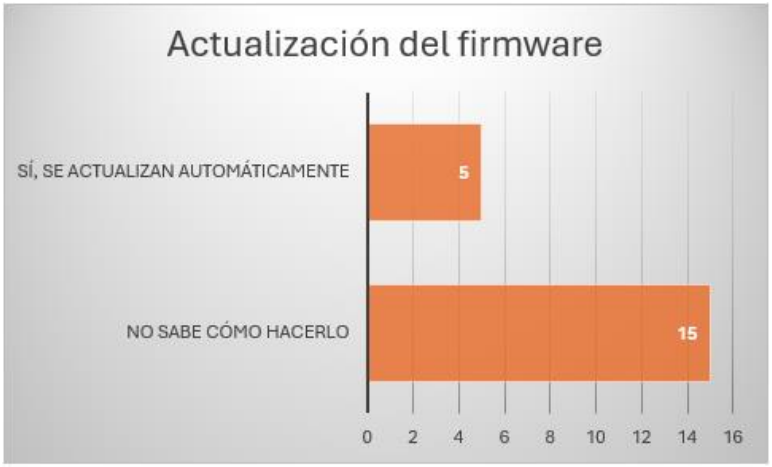
Nota. La imagen muestra el resultado obtenido en la encuesta, con respecto al conocimiento de protocolos seguros por parte de los usuarios.

Actualización del firmware

Un 75% no sabe cómo actualizar sus dispositivos, y solo un 25% indicó que sus equipos se actualizan automáticamente, ya que el bajo nivel de mantenimiento pone en riesgo la seguridad, pues muchas vulnerabilidades se corrigen mediante parches de software, adicionalmente este hallazgo contrasta con las recomendaciones de NIST (2021), que establece la necesidad de garantizar actualizaciones periódicas y verificables como un requisito mínimo de ciberseguridad en IoT.

Figura 8.

Grafica de actualización de firmware



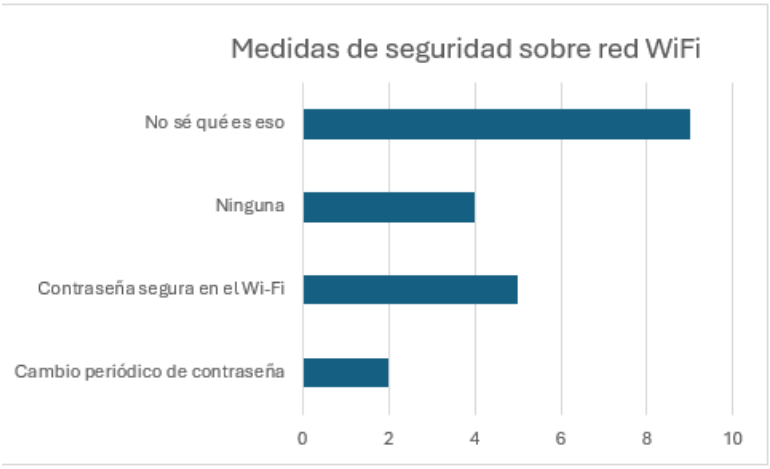
Nota. La imagen muestra el resultado obtenido en la encuesta de acuerdo con el conocimiento sobre la actualización de firmware de los dispositivos IoT

Medidas de seguridad en Wi-Fi

Aunque algunos reportaron tener contraseñas seguras o realizar cambios periódicos, un 45% respondió que no sabe qué son estas medidas o no ha implementado ninguna protección adicional, lo que puede facilitar accesos no autorizados a la red, y según ISO/IEC 27032:2023 (2023), las redes que soportan dispositivos IoT deben contar con mecanismos de cifrado robustos (WPA3) y segmentación de red para limitar la exposición de los dispositivos.

Figura 9.

Grafica sobre medidas de seguridad WiFi



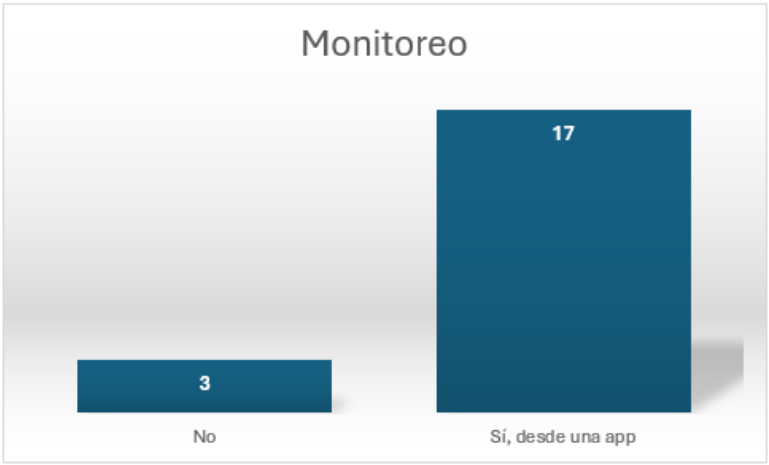
Nota. La imagen muestra el resultado obtenido en la encuesta, con respecto a las medidas de seguridad sobre las redes WiFi, implementadas por los usuarios

Monitoreo y percepción de riesgo

El 85% sí monitorea sus dispositivos desde una aplicación móvil, sin embargo, un número importante de encuestados (40%) expresó que nunca había considerado la posibilidad de ataques, lo cual denota una visión limitada sobre los riesgos reales asociados al IoT, por lo que esto resulta insuficiente frente a lo recomendado por ENISA (2024), que enfatiza la necesidad de supervisión activa y soluciones de monitoreo continuo para prevenir ataques y detectar anomalías.

Figura 10.

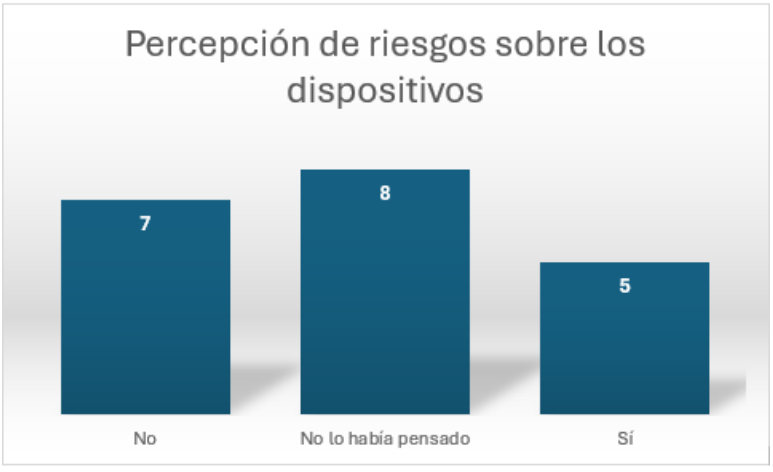
Grafica de monitoreo en dispositivos



Nota. La imagen muestra el resultado obtenido en la encuesta, en respuesta a si se realiza monitoreo sobre los dispositivos

Figura 11.

Grafica de percepción en riesgos



Nota. La imagen muestra el resultado obtenido en la encuesta, con respecto a la percepción de riesgos sobre los dispositivos por los usuarios

Capacidad de respuesta ante incidentes

El 15% indicó no saber qué hacer en caso de fallas o problemas, y un 30% declaró que nunca ha tenido un inconveniente y esta confianza excesiva podría derivar en demoras al responder ante incidentes de ciberseguridad.

Figura 12.

Grafica de respuesta ante incidentes

Nota. La imagen muestra el resultado obtenido en la encuesta de acuerdo a la respuesta ante incidentes presentados con los dispositivos IoT

Análisis crítico de los resultados

El análisis de la encuesta permitió identificar varias brechas importantes entre las prácticas reales de los usuarios y las recomendaciones establecidas por organismos internacionales.

En primer lugar, muchos usuarios no cambian las contraseñas predeterminadas de sus dispositivos IoT, lo cual contrasta con lo recomendado por NIST (2021) y ENISA (2024), que insisten en el cambio inmediato de credenciales por defecto y en el uso de contraseñas robustas, por lo que esta práctica expone a los dispositivos a ataques masivos, accesos no autorizados y botnets.

En relación con las actualizaciones de firmware, se evidenció un desconocimiento generalizado; algunos usuarios creen que son automáticas y otros no saben cómo realizarlas, entendiendo que esto va en contra de ISO/IEC 27032:2023, que establece que las actualizaciones deben ser automáticas, seguras y verificadas digitalmente.

Asimismo, se observó que la mayoría de los usuarios utiliza redes Wi-Fi con configuraciones mínimas de seguridad y sin segmentación, lo cual contradice las recomendaciones de Microsoft (2023) y NIST (2021), que proponen el uso de cifrado robusto (como WPA3) y la aplicación del modelo Zero Trust, y esta brecha incrementa el riesgo de intrusiones al compartir la red con dispositivos personales.

En cuanto al monitoreo, los usuarios revisan únicamente las aplicaciones móviles de sus dispositivos, lo que limita la detección temprana de incidentes. ENISA (2024) sugiere implementar supervisión activa, análisis de anomalías y alertas en tiempo real, elementos que no están presentes en la mayoría de los casos evaluados.

Además, se evidenció una baja percepción de vulnerabilidad entre los usuarios, quienes no consideran que sus dispositivos puedan ser atacados, y es contrario a lo advertido por ENISA (2024) y OWASP (2021), quienes destacan que la concientización es el primer paso hacia la protección.

Finalmente, se identificó un alto interés en disponer de una guía práctica de seguridad, lo cual coincide con las recomendaciones de ISO/IEC 27032:2023 y ENISA (2024), que promueven la creación de recursos accesibles para los usuarios finales, por lo que esta oportunidad permite reforzar la formación y mejorar las buenas prácticas en el uso cotidiano del IoT.

Conclusión del análisis

Los resultados de esta encuesta confirman que, aunque el uso de tecnologías IoT se ha masificado en entornos residenciales y comerciales, existe una brecha importante en términos de prácticas de seguridad, conocimiento técnico y conciencia de riesgos, ya que esto refuerza la necesidad de difundir guías prácticas, capacitaciones comunitarias y herramientas accesibles que permitan mejorar la protección de estos entornos inteligentes.

Los resultados obtenidos permiten confirmar la hipótesis planteada: los usuarios finales son el eslabón más débil en la cadena de seguridad del IoT, así como señala ENISA (2024), la ciberseguridad efectiva depende no solo de los mecanismos tecnológicos, sino también de la conciencia y hábitos de los usuarios, por lo que en este sentido, los hallazgos de la encuesta demuestran que la educación digital y la disponibilidad de recursos formativos son factores determinantes para reducir la exposición a riesgos.

Conclusiones

La presente monografía ha permitido evidenciar la creciente importancia de implementar medidas sólidas de ciberseguridad en entornos basados en el Internet de las Cosas (IoT), particularmente en escenarios donde la confidencialidad, la integridad y la disponibilidad de la información son críticas, como en el sector salud o infraestructuras industriales, y a través del análisis de conceptos, riesgos, estándares internacionales y herramientas de protección, se ha logrado construir una guía práctica que orienta a técnicos, ingenieros y responsables de TI en la adopción de arquitecturas IoT más seguras. A lo largo del desarrollo de esta monografía se cumplieron satisfactoriamente los objetivos propuestos, generando aportes significativos tanto a nivel técnico como académico en el campo de la seguridad en redes IoT.

Se logró mediante una revisión exhaustiva de literatura, el análisis de estándares internacionales, la identificación de vulnerabilidades comunes, y la construcción de una guía práctica respaldada con herramientas, flujogramas y recomendaciones aplicables.

Se abordaron los riesgos con base en el OWASP IoT Top 10, ejemplos reales de ataques como el malware Mirai, y se evidenció la criticidad de amenazas como contraseñas por defecto, firmware sin firma digital, y protocolos de comunicación inseguros.

Se estudiaron protocolos como MQTT, CoAP, ZigBee, y LoRaWAN, evaluando sus ventajas y limitaciones, así como se resaltó la necesidad de implementar autenticación fuerte, cifrado TLS, y mecanismos como OAuth 2.0 o X.509.

Se analizaron marcos como ISO/IEC 27030, NIST SP 800-213, y SESIP. Además, se expusieron prácticas como segmentación por VLAN, hardening, actualizaciones OTA seguras y Zero Trust.

Se diseñó una estrategia de defensa en profundidad, dividida por capas (percepción, red, procesamiento, almacenamiento y aplicación), incluyendo herramientas, casos reales y tecnologías emergentes como honeypots, blockchain y criptografía post-cuántica.

Se construyó una Guía Práctica estructurada que incluye checklist, políticas organizacionales, medidas por capa tecnológica, y un caso de éxito real en hospitales, además de una encuesta aplicada que valida la pertinencia del proyecto en el entorno real.

La investigación evidencia que la seguridad en el IoT no puede limitarse al ámbito técnico, ya que se requiere un enfoque sistémico que combine normas, concientización y responsabilidad compartida, por lo tanto, a futuro será necesario promover políticas de certificación de dispositivos IoT y fortalecer la formación en ciberseguridad desde niveles educativos básicos, especialmente en países en desarrollo.

Este proyecto resalta la necesidad de adoptar un enfoque proactivo en la protección de entornos IoT, especialmente en sectores críticos como salud, industria o ciudades inteligentes, donde se reafirma que la seguridad debe implementarse desde el diseño, bajo el principio de security by design, y que la sensibilización de los usuarios es un componente clave.

Referencias Bibliográficas:

Anderson, J. (2024, October 22). Securing the Internet of Things (IoT): Strategies for 2025 and beyond. Bryghtpath. https://bryghtpath.com/securing-the-internet-of-things/

Ashton, K. (2009). That 'Internet of Things' Thing. RFID Journal. http://www.rfidjournal.com/articles/view?498

Barbara. (n.d.). Protocolos de comunicación IoT que debes conocer - Barbara. https://www.barbara.tech/es/blog/protocolos-iot-que-deberias-conocer

Blanton, S. (2025, May 21). IoT security risks: stats and trends to know in 2025. JumpCloud. https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025

CyberArk Software. (2025, April 23). Identity Security Landscape | CyberArk. CyberArk. https://www.cyberark.com/threat-landscape/?utm_source=google&utm_medium=paid_search&utm_term=threat_landscape_report_nam_spanish_mx_cr_co&utm_content=threat_landscape_report&utm_campaign=identity_security&gclid=Cj0KCQjw8cHABhC-ARIsAJnY12wqNM1XsfhRKD2r18xhPowzGI8nEz_JemZt4SwFzyoL7WN37K0I-tAaAumyEALw_wcB&gad_source=1&gad_campaignid=19770135810&gbraid=0AAAAAD_gt5GglW4xogPr_jO_uWVm3NDQX

Dark Reading. (2024, junio 10). Severe RCE bugs in industrial IoT devices put critical infrastructure at risk. Dark Reading.

https://www.darkreading.com/ics-ot-security/severe-rce-bugs-industrial-iot-devices-devices-cyberattack

ENISA. (2024). ENISA Threat Landscape 2023/2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

ESET. (s.f.). 2025 Ataques a dispositivos IoT: termostatos inteligentes y vulnerabilidades. https://www.eset.com

Feiner, L. (2025, January 7). US Cyber Trust Mark launches as the Energy Star of smart home security. The Verge. https://www.theverge.com/2025/1/7/24338168/us-cyber-trust-mark-smart-home-security?utm_source=chatgpt.com

Home - OWASP Top 10:2021. (n.d.). https://owasp.org/Top10/es/

Identity Security Threat Landscape 2024 Report. (n.d.). Identity Security Threat Landscape 2024 Report. https://www.cyberark.com/resources/ebooks/identity-security-threat-landscape-2024-report?utm_medium=paid_search&utm_source=google&utm_campaign=identity_security&utm_content=threat_landscape_report&utm_term=threat_landscape_report_nam_spanish_mx_cr_co

Informe interinstitucional o interno 8259A del NIST Referencia básica de las capacidades de ciberseguridad de los dispositivos de IoT Mayo de 2020. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8259Aes.pdf

Informe sobre el panorama de amenazas a la seguridad de la identidad 2024

Instituto Nacional de Estándares y Tecnología (NIST). (2021). Referencia básica de las capacidades de ciberseguridad de los dispositivos de Internet de las cosas

(IoT)https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8259Aes.pdf?utm_source=chatgpt.com

IoT Cybersecurity Landscape in 2024 | 1NCE. (n.d.). 1NCE. https://www.1nce.com/en-ap/resources/news-insights/blog/iot-cybersecurity-landscape?utm_source=chatgpt.com

ISO/IEC 27032:2023. (n.d.). ISO. https://www.iso.org/standard/76070.html

Jecrespom. (2024, March 18). Arquitecturas IoT – Aprendiendo Arduino. Aprendiendo Arduino. https://aprendiendoarduino.wordpress.com/tag/arquitecturas-iot/

Ly, K., & Ly, K. (2025, April 18). 5G and IoT Trends 2025: What Tech Leaders Need to Know Now. Designveloper. https://www.designveloper.com/blog/5g-and-iot/

Microsoft. (2023). Zero Trust Principles for IoT and OT environments. Microsoft Corporation.

Newman, L. H. (2023, August 9). Panasonic warns that IoT malware attack cycles are accelerating. WIRED. https://www.wired.com/story/panasonic-iot-malware-honeypots/?utm_source=chatgpt.com

Newman, S. (2025, April 8). What is the Mirai Botnet? Corero Network Security. https://www.corero.com/what-is-the-mirai-botnet/

NIST. (2021). NIST Special Publication 800-213: IoT Device Cybersecurity Guidance for the Federal Government. National Institute of Standards and Technology ENISA

Security, P. (2024, October 1). IOT Archives. Panda Security Mediacenter. https://www.pandasecurity.com/es/mediacenter/iot/

Statista. (2025, June 26). Number of IoT connected devices worldwide 2019-2030, by communications technology. https://www.statista.com/statistics/1194688/iot-connected-

devices-communications-technology/?srsltid=AfmBOopsHK3WnRccHn4tBWtVkTZHaOYHJGAibiFoWvQ_eUfDDBCFFOe4

The Hacker News. (2021, 13 de enero). Amazon fixes Ring app vulnerability that exposed users' video feeds. https://thehackernews.com/2021/01/amazon-ring-app-vulnerability.html

Trend Report: The most important IIoT Trends in 2025. (n.d.). Susietec. https://www.susietec.com/en/blog/2025-01/trend-report-most-important-iiot-trends-2025

Universidad Europea. (2023, July 3). El Internet de las cosas en la vida cotidiana. https://universidadeuropea.com/blog/internet-cosas-vida-cotidiana/

WHO (World Health Organization). (2023). Digital health and Internet of Things in healthcare. Ginebra: WHO.

Wikipedia contributors. (2024, mayo 24). Snowflake data breach. Wikipedia.

https://en.wikipedia.org/wiki/Snowflake_data_breach

Yesmin, T., Carter, M. W., & Gladman, A. S. (2022). Internet of things in healthcare for patient safety: an empirical study. BMC Health Services Research, 22(1). https://doi.org/10.1186/s12913-022-07620-3

ZipDo. (2024). IoT Security Industry Statistics. https://zipdo.co/iot-security-industry-statistics/

Apéndice

Herramienta de recolección de datos: Encuesta aplicada

A continuación, se presenta el cuestionario utilizado para la recolección de información en el estudio “Implementación de redes seguras en entornos de IoT”.

*Encuesta sobre uso y seguridad en dispositivos Io*T

1. ¿Qué tipo(s) de dispositivos IoT utiliza actualmente en su vivienda o negocio?

- Cámaras de seguridad
- Alarmas
- Sensores de movimiento o humo
- Cerraduras inteligentes
- Asistentes virtuales (Alexa, Google Home, etc.)
- Otros: _____

2. ¿Quién configuró inicialmente sus dispositivos IoT?

- Usted mismo
- Técnico especializado
- Personal de la empresa que vendió el equipo
- No lo recuerda

3. ¿Ha cambiado las contraseñas por defecto de los dispositivos IoT después de la instalación?

- Sí

- No
- No sabe / No aplica

4. ¿Conoce si sus dispositivos usan protocolos de conexión segura (por ejemplo, HTTPS, cifrado WPA2/WPA3, etc.)?

- Sí
- No
- No estoy seguro

5. ¿Ha actualizado alguna vez el software o firmware de sus dispositivos IoT?

- Sí, de forma manual
- Sí, se actualizan automáticamente
- No
- No sabe cómo hacerlo

6. ¿Usa alguna de estas medidas de seguridad en su red local (Wi-Fi)?

- Contraseña segura en el Wi-Fi
- Cambio periódico de contraseña
- Red separada para dispositivos IoT
- Ninguna
- No sé qué es eso

7. ¿Monitorea la actividad o el estado de sus dispositivos IoT?

- Sí, desde una app
- Solo cuando algo falla

- No

8. ¿Considera que sus dispositivos IoT podrían ser vulnerables a ataques o hackeos?

- Sí
- No
- No lo había pensado

9. En caso de pérdida de conexión o fallas, ¿sabe qué hacer o a quién contactar?

- Sí
- No
- Nunca he tenido un problema

10. ¿Estaría interesado en recibir una guía básica o asesoría sobre cómo mejorar la seguridad de sus dispositivos IoT?

- Sí
- No
- Tal vez