



Modelo de gestión en ciberseguridad y domótica con enfoque en resiliencia aplicada a casas iot automatizadas.

Proyecto de investigación

Iván Fernando Ardila Villabona
1.007.439.790

Cesar Javier Pardo Garnica
91.534.940

UNIDADES TECNOLÓGICAS DE SANTANDER

Facultad de Ciencias e Ingenierías

Ingeniería de sistemas

Bucaramanga 18 de septiembre de 2026



Modelo de gestión en ciberseguridad y domótica con enfoque en resiliencia aplicada a casas iot automatizadas.

Proyecto de Investigación

AUTORES

Iván Fernando Ardila Villabona

1.007.439.790

Cesar Javier Pardo Garnica

91.534.940

Trabajo de Grado para optar al título de
Ingeniería de sistemas

DIRECTOR

Víctor Andrés Ochoa Correa

UNIDADES TECNOLÓGICAS DE SANTANDER

Facultad de Ciencias e Ingenierías

Ingeniería de sistemas

Bucaramanga 18 de septiembre de 2026

Nota de Aceptación

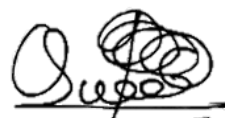
El proyecto “Modelo de gestión en ciberseguridad y domótica con enfoque en resiliencia aplicada a casas iot automatizadas” realizado por los estudiantes Cesar Javier Pardo Garnica e Iván Fernando Ardila Villabona, se encuentra aprobado en cumplimiento de los requisitos exigidos por las Unidades Tecnológicas de Santander para optar al título de ingeniería de sistemas.

Según acta de aprobación: 23

Fecha: 2026-09-29.



Firma del Evaluador



Firma del Director

DEDICATORIA

Para nuestras familias las cuales han estado apoyándonos incondicionalmente a cumplir nuestras metas, en caso especial nuestros padres los cuales han tenido la confianza en nosotros y nos han animado a dar lo mejor.

A las Unidades Tecnológicas de Santander a la cual como institución ha estado apoyando la educación en el departamento, como a su gran planta de docentes que posee actualmente la cual han impartido conocimiento en nuestro proceso de aprendizaje, hasta en la durante y post pandemia ahí están sus docentes. Muchas Gracias.

En especial a los Docentes, directivos y asociados a la coordinación de sistemas los cuales han sido una pieza fundamental en el proceso del momento de la inscripción hasta el momento del trabajo de grado. Muchas Gracias. A nuestros Compañeros de cursos que han sido fundamental en este proceso de aprendizaje y crecimiento profesional.

AGRADECIMIENTOS

El esfuerzo que requiere realizar una tesis es comparable a la determinación que se siente al concluirla. Detrás de este logro hay un valioso conocimiento transmitido por personas que han dedicado su vida a enseñar y compartir su saber con el fin de transformar el mundo.

Por esta razón, agradezco a todos los profesores de la carrera que acompañaron con dedicación mi proceso académico. Cada uno sembró semillas que seguiré cosechando en mis futuros pasos académicos y laborales. Destaco especialmente la labor de Víctor Ochoa Correa, quien participó de forma activa en todo el proyecto, con paciencia, dedicación, generosidad y solidaridad, llenando mi camino de perseverancia.

TABLA DE CONTENIDO

RESUMEN EJECUTIVO	11
INTRODUCCIÓN.....	12
1. DESCRIPCIÓN DEL TRABAJO DE INVESTIGACIÓN.....	15
1.1. PLANTEAMIENTO DEL PROBLEMA.....	15
1.2. JUSTIFICACIÓN	17
1.3. OBJETIVOS	19
1.3.1. OBJETIVO GENERAL	19
1.3.2. OBJETIVOS ESPECÍFICOS	19
1.4. ESTADO DEL ARTE	20
2. MARCO REFERENCIAL	22
2.1. MARCO TEÓRICO.....	22
2.2. MARCO CONCEPTUAL	24
2.3. MARCO LEGAL	25
3. DISEÑO DE LA INVESTIGACIÓN	27
4. DESARROLLO DEL TRABAJO DE GRADO.....	29
4.1. ¿QUÉ SON LOS DISPOSITIVOS IoT PARA EL HOGAR?	29
4.1.1. SU FUNCIONAMIENTO EL CICLO DE LA AUTOMATIZACIÓN.	29
4.1.2. ¿PARA QUÉ SIRVEN EN EL DÍA A DÍA?	31
4.1.3. COMPONENTES QUE CONFORMAN UN HOGAR INTELIGENTE.	32
4.2. VULNERABILIDADES CRÍTICAS EN DISPOSITIVOS IoT DOMÉSTICOS.....	39
4.2.1. DIAGNÓSTICO DE VULNERABILIDADES POR CATEGORÍA.....	40
4.2.2. MATRIZ DE DIAGNÓSTICO DE VULNERABILIDADES POR TIPO DE DISPOSITIVO.	46
4.2.3. REPRESENTACIÓN DE UN ATAQUE MEDIANTE DIAGRAMAS.....	48
4.3. ANALIZAR LOS TIPOS DE AMENAZAS.....	51
4.3.1. IDENTIFICACIÓN DE VULNERABILIDADES Y DEFINICIÓN DEL ALCANCE DEL ANÁLISIS....	52
4.3.2. CRITERIOS DE EVALUACIÓN.....	54
4.3.3. SUSTENTO NORMATIVO.....	55
4.3.4. CLASIFICACIÓN DE AMENAZAS.....	57

4.3.5.	EVALUACIÓN DE IMPACTO Y PROBABILIDAD	64
4.3.6.	PRIORIZACIÓN Y PLAN DE MITIGACIÓN	68
4.3.7.	DOCUMENTACIÓN Y TRAZABILIDAD DEL ANÁLISIS.	71
4.4.	CONSTRUCCIÓN DEL MODELO.	74
4.4.1.	CONSTRUCCIÓN DEL MODELO INICIAL.....	75
4.4.2.	MAGNITUD Y BASE DEL PROBLEMA EN EL MODELADO.....	77
4.4.3.	ANÁLISIS DE VULNERABILIDADES POR CAPA.....	80
4.4.4.	VULNERABILIDADES DE SOFTWARE.....	81
4.4.5.	FACTOR HUMANO.....	82
4.5.	MODELO INICIAL PROPUESTO: ARQUITECTURA DE 5 CAPAS.	82
4.6.	ESTRATEGIAS DE IMPLEMENTACIÓN.	91
4.7.	CONSTRUCCIÓN DE UN ENTORNO DE SIMULACIÓN PARA LA FASE DE PRUEBAS Y TEST DE FUNCIONALIDAD.	93
4.7.1.	CONSTRUCCIÓN DE UN ENTORNO SIMULADO PARA VALIDAR EL MODELO	96
4.8.	FASE DE DEMOSTRACIÓN DE VULNERABILIDADES.....	103
4.9.	MODELO FINAL.....	126
4.9.1.	UN MODELO DE PROTECCIÓN POR CAPAS PARA DISPOSITIVOS IoT, REDES IoT, INFORMACIÓN Y USUARIOS.....	126
4.9.2.	FUNDAMENTACIÓN DEL MODELO, HEREDADO DE LA INVESTIGACIÓN MODELO INICIAL. 128	
4.9.3.	ARQUITECTURA GENERAL DE CINCO CAPAS MODELO FINAL.....	130
4.9.4.	GESTIÓN DE DISPOSITIVOS Y SUS RIESGOS DENTRO DEL MODELO.	149
4.9.5.	MOTOR DE EVALUACIÓN DEL MODELO.	152
4.9.6.	INTEGRACIÓN CON NIST CSF 2.0.....	152
4.9.7.	INDICADORES PARA EVALUAR EL MODELO FINAL.	155
4.9.8.	SEGURIDAD DURANTE TODO EL CICLO DE VIDA DEL DISPOSITIVO.	158
4.9.9.	PRINCIPIOS FUNDAMENTALES DEL MODELO.....	160
5.	<u>RESULTADOS.....</u>	<u>162</u>
6.	<u>CONCLUSIONES.....</u>	<u>170</u>
7.	<u>RECOMENDACIONES</u>	<u>173</u>
7.1.	RECOMENDACIONES PARA FABRICANTES E INTEGRADORES.....	173
7.2.	RECOMENDACIÓN SOBRE DISPOSITIVOS SIN SOPORTE.....	174
7.3.	RECOMENDACIÓN PARA LAS ACTUALIZACIONES	174
7.4.	RECOMENDACIÓN PARA ELIMINAR CREDENCIALES PREDETERMINADAS	175
7.5.	RECOMENDACIONES PARA FUTURAS VERSIONES DEL MODELO	176
8.	<u>REFERENCIAS BIBLIOGRÁFICAS</u>	<u>177</u>

LISTA DE FIGURAS

Figura 1. Etapas de seguimiento.....	27
Figura 2. Smart Hub Conexión.....	33
Figura 3. Smart Hub.	33
Figura 4. Enchufe inteligente fuente.	34
Figura 5. Enchufe inteligente.....	34
Figura 6. Bobilla inteligente 1.	35
Figura 7. Bobilla inteligente 2.	35
Figura 8. MoesGo WiFi IR Control.	36
Figura 9. cámara lot Tapo.	37
Figura 10. cámara lot.....	37
Figura 11. TP-Link Tapo T110 Sensor de Contacto.	37
Figura 12. CLICKLIFE Sensor.....	38
Figura 13. CLICKLIFE Sensor de Temperatura Y Humedad Inteligente.	38
Figura 14. XUK kit de alarma de seguridad inteligente para el hogar.....	39
Figura 15. Diagrama Fallas en Autenticación.....	48
Figura 16. Diagrama Cifrado Deficiente.....	49
Figura 17. Diagrama Actualizaciones de Firmware Inseguras.	50
Figura 18. Diagrama Exposición a Redes Inseguras	51
Figura 19. Proceso de gestión de riesgos de seguridad de la información.	57
Figura 20. Ataque a Dyn.....	63
Figura 21. Puntuaciones CVSS.....	66
Figura 22. Nivel de riesgo.....	68
Figura 23. Comparación entre arquitectura de red plana	71
Figura 24. Diagrama de red.....	87
Figura 25. Topografía.	97
Figura 26. Conexión establecida.....	99
Figura 27. Conexión del computador y configuración.	100
Figura 28. Acceso al gateway.	101
Figura 29. Dispositivos en la red.	103
Figura 30. Configuración y programación.....	108
Figura 31. Programación 1.....	109
Figura 32. Programación 1.1.....	110
Figura 33. Muestra de funcionalidad No.1.	111
Figura 34. Muestra de funcionalidad No.2 tras 5 segundos de inactividad.....	112
Figura 35. Muestra de funcionalidad No.3.	113
Figura 36. Muestra de funcionalidad No.4.	113
Figura 37. Programación 1.2.....	114
Figura 38. Programación 1.2.1.....	115
Figura 39. Demostración de funcionalidad No.3.....	116
Figura 40. El antes y el ahora cifrado.	116
Figura 41. Ligth IoT Vulnerabilidad.	119

Figura 42. Programación 2.....	120
Figura 43. Muestra de funcionalidad No.4.....	121
Figura 44. Programación 2.1.....	123
Figura 45. Muestra de funcionalidad No5. Firma valida.....	124
Figura 46. Muestra de funcionalidad No5. Firma no valida.....	125
Figura 47. El antes y el ahora, firmas.....	125
Figura 48. Modelo principio.....	130
Figura 49. Capas del modelo.....	131
Figura 50. Seguridad de software.....	134
Figura 51. Diagrama de credenciales.....	135
Figura 52. Diagrama de sensor básico.....	138
Figura 53. Diagrama de actualización.....	140
Figura 54. Diagrama de red única.....	141
Figura 55. Red por segmentos.....	142
Figura 56. Diagrama de gobernanza.....	149
Figura 57. Ejemplo de gestión de dispositivo.....	151
Figura 58. Pasos simplificados.....	154
Figura 59. Ciclo de vida.....	158
Figura 60. resultados de credenciales.....	166

LISTA DE TABLAS

Tabla 1. Tipos de protocolo.	30
Tabla 2. Matriz de Vulnerabilidades.	47
Tabla 3. A1 Alcance del análisis de amenazas.	53
Tabla 4. A2 Consideraciones de riesgo y metas de mitigación	56
Tabla 5. B1 Transformación de vulnerabilidades en amenazas clasificadas por naturaleza, mecanismo y consecuencia.	58
Tabla 6. B2 Correspondencia entre las amenazas priorizadas.	59
Tabla 7. C1 Comparativa técnica entre las botnets Mirai y Mozi documentadas en este objetivo.	61
Tabla 8. D1 Escalas de impacto y probabilidad aplicadas al análisis de amenazas IoT domésticas.	65
Tabla 9. D2 Matriz de evaluación de riesgo.	65
Tabla 10. E1 Mapa de calor de riesgo.	67
Tabla 11. F1 Plan de mitigación diferenciado por nivel de riesgo.	70
Tabla 12. Tabla maestra de trazabilidad.	72
Tabla 13. De complemento a Matriz de Vulnerabilidades.	73
Tabla 14. Análisis de contexto	78
Tabla 15. vectores de ataque.	80
Tabla 16. Matriz de Factores de riesgo en dispositivos.	90
Tabla 17. Matriz de riesgo a nivel software de dispositivos.	93
Tabla 18. controles de configuración y descripción.	145
Tabla 19. Factores de riesgo tabla adicional.	150
Tabla 20. Matriz Evaluativa.	152
Tabla 21. Integración NIST con el modelo propuesto.	153
Tabla 22. Matriz de caso.	156
Tabla 23. Tabla de resultados de vulnerabilidad.	157
Tabla 24. Principios.	161
Tabla 25. Resultado, evidencia y fundamento.	163

RESUMEN EJECUTIVO

Este proyecto tiene como objetivo construir un modelo de ciberseguridad basado en el análisis de riesgos, con el fin de fortalecer el manejo adecuado de incidentes de ciberseguridad en todas las operaciones de pequeñas empresas, entidades o domésticos que cuentan con servicios informáticos lot.

Para lograrlo, se inicia con la detección de los riesgos para estas entidades que cuentan con servicios informáticos lot, esto se realizara mediante un análisis de posibles amenazas, apoyándose en la norma ISO 27005:2022 (Iso 27005, 2022), la cual establece los procedimientos necesarios para el manejo y detección de riesgos de seguridad. Este proceso comienza con la identificación de activos, seguido del análisis de sus escenarios de riesgo y la definición de los controles adecuados para mitigar los impactos de la materialización de dichos riesgos.

Con el propósito de garantizar un adecuado manejo de incidentes de ciberseguridad, se realiza la selección de las normas adecuadas según criterios selectivos. Posteriormente, se construye el modelo de ciberseguridad, incorporando en el manejo de incidentes los riesgos críticos y los controles correspondientes para cumplir con el objetivo del proyecto.

PALABRAS CLAVE: informática, riesgos, domótica “iot”, Modelo, ciberseguridad

INTRODUCCIÓN

El empleo de las tecnologías de la información y las comunicaciones dentro de las pequeñas empresas e individuales no jurídicos, junto con la cuarta revolución industrial, posee un carácter de enfoque tecnológico. El conocimiento especializado que estas herramientas brindan y facilitan la creación, masificación, diversificación y transferencia de la información que actualmente los individuos y las compañías acceden a través del ciberespacio.

Este fenómeno impulsa el avance tecnológico, aunque al mismo tiempo genera niveles de exposición que pueden ocasionar daños sobre la información propia de cada individuo o entidad.

Por esta razón, los esfuerzos dirigidos a implementar sistemas que reduzcan los riesgos de ciberseguridad tanto en tecnologías actuales como en las nuevas tecnologías se deben de realizar análisis de seguridad de manera constante. En consecuencia, el propósito central de este trabajo se fundamenta en la “construcción de un modelo de ciberseguridad para entidades o personas naturales que implementen servicios informáticos, basado en referentes nacionales e internacionales, con el fin de establecer un manejo adecuado de incidentes de seguridad.”

En Colombia, las inversiones en seguridad han aumentado progresivamente, pero aún resultan insuficientes frente al elevado crecimiento de los ataques cibernéticos que acompañan la rápida convergencia tecnológica. Tomando como ejemplo Para el año 2026, El 60% de las empresas enfrenta ciberriesgos sin planes de respuesta

definidos, afirma Trend Micro (ACIS, 2019), según la CRC en “Ciberriesgos También se manifestó. Para el año 2026, se proyecta que el cibercrimen será la tercera economía más grande a nivel mundial, impulsado principalmente por los avances en inteligencia artificial y computación cuántica.

Estos progresos facilitan la ejecución de ataques autónomos y la generación de audio y vídeo manipulados a través de deepfakes y contenido sintético, permitiendo a los atacantes suplantar identidades confiables y acceder a sistemas protegidos (CRC, 2025).

Hoy en día, las personas naturales y entidades deben considerar la creación de estrategias que les permitan mantenerse alineadas con los sucesos de seguridad que se presentan. De acuerdo con la firma especializada en seguridad Kaspersky (KASPERSKY, 2019), en Latinoamérica, entre julio de 2018 y julio de 2019, los bloqueos más frecuentes se originaron por infecciones de algún tipo de malware.

En reafirmación de la problemática regional, la Asociación Colombiana de Ingenieros de Sistemas (ACIS, 2019) señala que el 41% de las dificultades de seguridad se relacionan con errores humanos, mientras que el 24% corresponden al phishing y el 22% a la instalación de software no autorizado.

Esto evidencia que los ataques más comunes continúan siendo los mecanismos preferidos por los ciberdelincuentes para infiltrarse en los entornos individuales/personales o en las entidades.

A continuación, se presentan el planteamiento del problema los objetivos general específicos de este proyecto, cuya finalidad es fortalecer los controles asociados a la prevención de eventos de seguridad derivados de ataques recurrentes y, en caso

de que dichos controles no resulten efectivos, integrar un sistema de gestión de incidentes que permita contar con un modelo que cubra ambos frentes de manera sistemática.

1. DESCRIPCIÓN DEL TRABAJO DE INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA.

El uso continuo de tecnologías IoT en las viviendas de Santander ha transformado la forma de interactuar con los sistemas eléctricos, de seguridad y confort en cada una de las casas. Sin embargo, ha traído consigo una serie de vulnerabilidades cibernéticas que han evolucionado comprometiendo la privacidad, la disponibilidad de servicios y la integridad de los datos personales (MENDOZA, 2024).

A falta de modelos de gestión adaptados al contexto local que impide una defensa estructurada ante amenazas como accesos no autorizados, infecciones por malware y ataques de denegación de servicio distribuido (DLTCode, 2025), que afectan directamente la disponibilidad y seguridad de los hogares inteligentes esa carencia limita la capacidad de respuesta ante incidentes y dificulta la implementación de medidas preventivas eficaces.

Además, Los dispositivos IoT domésticos no cuentan con actualizaciones constantes, como cifrado robusto y autenticación, convirtiéndose en puntos vulnerables dentro de la red doméstica, esas debilidades permiten el robo de datos sensibles, el control remoto no autorizado y la propagación de malware entre dispositivos, afectando la seguridad integral del hogar (Garcia-Milà, 2023).

La ausencia de resiliencia operativa— entendida como la capacidad de resistir, absorber y recuperarse ante incidentes— agrava el impacto de ataques y genera interrupciones prolongadas y pérdida de confianza en automatizaciones (TechConsulting, 2025; Arteaga, F., & Alonso Lecuit, J., 2024).

Esta problemática se origina a falta de integración entre los principios de ciberseguridad, la arquitectura domótica y la gestión de riesgos adaptada a hogares inteligentes. En Santander, no existen modelos base que orienten la protección de estos entornos desde una perspectiva sistémica, escalable y resiliente. ¿Cómo puede un modelo base de gestión en ciberseguridad y domótica fortalecer la protección de casas IoT automatizadas en Santander?

1.2. JUSTIFICACIÓN

La creciente digitalización en los hogares plantea desafíos urgentes en materia de seguridad, especialmente en los contextos donde la adopción de tecnologías IoT supera la capacidad técnica para gestionarlas. En Santander, esta brecha se traduce en una exposición creciente a amenazas cibernéticas que afectan la vida cotidiana de los ciudadanos (MENDOZA, 2024).

La propuesta de un modelo base de gestión en ciberseguridad y domótica con enfoque en resiliencia responde a la necesidad de establecer lineamientos teóricos que orienten la protección de las casas inteligentes (DLTCode, 2025), este trabajo busca aportar una estructura base conceptual que permita anticipar riesgos, fortalecer la capacidad de respuesta ante incidentes y garantizar la continuidad de los servicios automatizados.

Al integrar principios de ciberseguridad con arquitectura domótica y gestión de riesgos, que promueve una visión sistémica que trasciende la solución técnica y se convierte en una herramienta para la toma de decisiones informadas (Arteaga, F., & Alonso Lecuit, J., 2024).

La relevancia de esta investigación radica en el potencial para generar conocimiento aplicable, fomentar la alfabetización digital en todos los entornos domésticos y contribuir a diseñar las políticas públicas que orienten a la protección de las infraestructuras residenciales conectadas.

Además, ofrecer una base metodológica para las futuras investigaciones y los desarrollos tecnológicos que busquen mejorar la seguridad y resiliencia de los hogares inteligentes en Colombia (TechConsulting, 2025). Este enfoque también permite visualizar los riesgos que enfrentan los usuarios no técnicos, quienes por

desconocer las implicaciones de seguridad en sus dispositivos conectados. Al proponer un modelo base, se facilita la creación de guías, buenas prácticas y estrategias replicables en otros contextos regionales. En conjunto, esta propuesta representa un aporte significativo al fortalecimiento de la seguridad digital en el entorno doméstico colombiano (Albarrán, 2024).

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Proteger los sistemas y dispositivos de casas IoT automatizadas mediante un modelo que asegure la defensa ante amenazas cibernéticas y la continuidad de los servicios en caso de incidentes.

1.3.2. OBJETIVOS ESPECÍFICOS

- 1) Diagnosticar las vulnerabilidades más comunes en dispositivos IoT domésticos, incluyendo fallas en autenticación, cifrado, actualizaciones y exposición a redes inseguras.
- 2) Analizar los tipos de amenazas cibernéticas que afectan la infraestructura digital de hogares inteligentes, como accesos no autorizados, malware y ataques DDoS, con base en estudios de caso y literatura especializada.
- 3) Validar el modelo funcional mediante simulación asegurando la ciberseguridad IoT, e implementando los mecanismos de seguridad definidos, con el fin de evaluar su resistencia frente a amenazas comunes en entornos domésticos.

1.4. ESTADO DEL ARTE

Implementaciones de domótica con IoT.

En el contexto colombiano, se han desarrollado iniciativas relevantes que demuestran la viabilidad técnica y académica de la domótica basada en IoT en entornos residenciales. (Mendoza, Mendoza Padilla & Marín, 2020) presentaron un prototipo funcional de vivienda inteligente con sensores y control remoto mediante aplicación móvil, destacando la integración de automatización en iluminación, seguridad y confort.

Por su parte, (Cuevas Tumay, Castillo Gómez, López Giraldo, 2022) diseñaron una arquitectura tecnológica para una casa de dos plantas en Bogotá, utilizando simulación para validar la eficiencia de los sistemas domóticos en respuesta a eventos de seguridad.

A nivel internacional, (Moreira, Isaac, Silva, Ylber, 2025), desde la Universidad Politécnica Salesiana en Ecuador, desarrollaron un prototipo de residencia automatizada utilizando tecnología IoT.

El proyecto integró sensores y actuadores conectados a microcontroladores, permitiendo funciones como el ajuste automático de temperatura, iluminación por presencia y apagado programado de dispositivos, con el objetivo de mejorar la eficiencia energética y el confort residencial.

Por otro lado, (TOALA PILAY & GUTIERREZ TUBAY, 2024), en la Universidad Estatal del Sur de Manabí, implementaron una infraestructura IoT basada en tecnología ZigBee para el control inteligente de cortinas en una sala académica.

F-DC-125

INFORME FINAL DE TRABAJO DE GRADO EN MODALIDAD DE
PROYECTO DE INVESTIGACIÓN, DESARROLLO TECNOLÓGICO,
MONOGRAFÍA, EMPRENDIMIENTO Y SEMINARIO

VERSIÓN: 2.0

El sistema, vinculado a una aplicación móvil y asistente virtual, automatiza el entorno y mejora la eficiencia operativa, evidenciando el potencial de la domótica aplicada a espacios funcionales.

ELABORADO POR:
Docencia

REVISADO POR:
Sistema Integrado de Gestión

APROBADO POR: Líder del Sistema Integrado de Gestión
FECHA APROBACIÓN: Octubre de 2023

2. MARCO REFERENCIAL

2.1. MARCO TEÓRICO.

La ciberseguridad se desarrolla como respuesta al crecimiento de los entornos digitales interconectados, donde la información circula constantemente entre sistemas. Su propósito principal es resguardar dichos activos frente a posibles riesgos. De acuerdo con la Unión Internacional de Telecomunicaciones (ITU, 2021).

Este campo abarca no solo herramientas tecnológicas, sino también políticas, prácticas organizacionales, mecanismos de gestión y estrategias orientadas a la protección integral de la información y los usuarios.

Dentro de este contexto, la gestión de riesgos se convierte en un eje fundamental, ya que permite identificar, analizar y tratar las posibles amenazas que pueden afectar los activos tecnológicos y en gran medida a sus usuarios o terceros prestadores de servicios tecnológicos.

Las vulnerabilidades, entendidas como debilidades inherentes o adquiridas en los sistemas, pueden ser explotadas por agentes internos o externos. Estas amenazas pueden clasificarse según su origen, ya sea humano o mediante agentes "IA" (ISO 42001, 2023), así como por su intencionalidad.

El concepto de riesgo cibernético surge entonces como la probabilidad de que un incidente comprometa los recursos tecnológicos de un individuo u organización.

Para su adecuada gestión, es necesario integrarlo en todos los procesos de seguridad, permitiendo una visión transversal que facilite la toma de decisiones.

Una de las principales medidas para reducir estos riesgos es la implementación de controles, los cuales pueden ser de carácter individual, técnico o estratégico (Arteaga, F., & Alonso Lecuit, J., 2024). No obstante, su aplicación no garantiza por sí sola la eliminación del riesgo, por lo que resulta indispensable acompañarlos de procesos de seguimiento, evaluación y mejora continua.

Ante el incremento de amenazas en el entorno digital, diversas entidades han propuesto modelos y estándares para fortalecer la seguridad de la información. En el caso de MINTIC (MINTIC, 2025), se plantea un enfoque que permite a las organizaciones gestionar la privacidad y protección de sus datos de manera estructurada. Asimismo, normas internacionales como ISO 31000 (IEC-ISO 31010, 2019) proporcionan lineamientos generales para la administración del riesgo.

Mientras que a su vez la ISO 27005 (ISO 27005 2022) se enfoca específicamente en la seguridad de la información mediante un enfoque basado en el ciclo PHVA. La gestión de riesgos no solo contribuye a disminuir la exposición a amenazas, sino que también permite determinar qué riesgos deben ser aceptados, mitigados o transferidos. Para que este proceso sea efectivo, debe integrarse dentro de un modelo de seguridad flexible y sostenible en el tiempo.

En este sentido, la gestión de incidentes cobra relevancia como complemento de la gestión de riesgos. Su finalidad es responder de manera organizada ante eventos que puedan afectar la operación de la organización. Estándares como ISO/IEC 27035 y guías como NIST SP 800-61 ofrecen metodologías para la preparación,

detección, análisis y recuperación ante incidentes, promoviendo una respuesta eficiente y oportuna (NIST SP 800-61 Rev. 3, 2025).

Finalmente, la aplicación de estos enfoques resulta especialmente relevante en organizaciones que dependen de servicios informáticos para su funcionamiento. Esto incluye desde plataformas de comunicación y sistemas de almacenamiento, hasta infraestructuras en la nube, virtualización y soporte técnico especializado, todos ellos fundamentales en la operación actual de las empresas.

2.2. MARCO CONCEPTUAL.

El Internet de las cosas (IoT): es un sistema formado por diversos subsistemas que consisten en distintos dispositivos de hardware. Estos dispositivos cumplen una o varias funciones específicas y se encuentran conectados entre sí, creando una red inteligente.

Su función principal consiste en la recolección de datos con el objetivo de reforzar la inteligencia artificial, lo que hace al sistema más eficiente y accesible para diversos usos domésticos o laborales.

IoT Software: es una capa de la plataforma IoT que se encuentra ubicada en la nube esta se encarga de reunir los servicios de software esenciales IoT se enfoca en conectar de manera segura el “digital twin” de las cosas conectadas, procesa y analiza datos proporcionando así APIs para consumir y exponer servicios.

2.3. MARCO LEGAL.

Ley 1978 del 25 de julio de 2019.

se crean las condiciones para que Colombia llegue a 70 % de los hogares conectados a Internet, gracias a la reactivación de la inversión en el sector TIC que permitirá el despliegue de infraestructura de alto costo. Además, con los proyectos de conectividad y la transformación de la televisión pública hacia la oferta multiplataforma, se acelerará la reducción de la brecha digital. (República, LEY 1978 DE 2019, 2019)

Ley 1341 de 2009 Art 1.

Parágrafo artículo 1°. El servicio postal continuará rigiéndose por las normas especiales pertinentes, en particular la Ley 1369 de 2009, con las excepciones específicas que contenga la presente Ley.

El servicio de radiodifusión sonora continuará rigiéndose por las disposiciones específicas expresamente señaladas para ese servicio en la presente Ley. Para todos los efectos de la presente Ley, la provisión de redes y servicios de telecomunicaciones incluye la provisión de redes y servicios de televisión.

El servicio de televisión abierta radiodifundida continuará rigiéndose por las normas especiales pertinentes, en particular la Ley 182 de 1995, la Ley 335 de 1996, la Ley 680 de 2001 y demás normas que las modifiquen, adicionen o sustituyan.

Al servicio de radiodifusión sonora y al de televisión abierta radiodifundida les será aplicable la presente Ley en las disposiciones específicas expresamente señaladas para estos servicios. (República, LEY 1341 DE 2009, 2009)

Ley 1273 del 5 de enero de 2009.

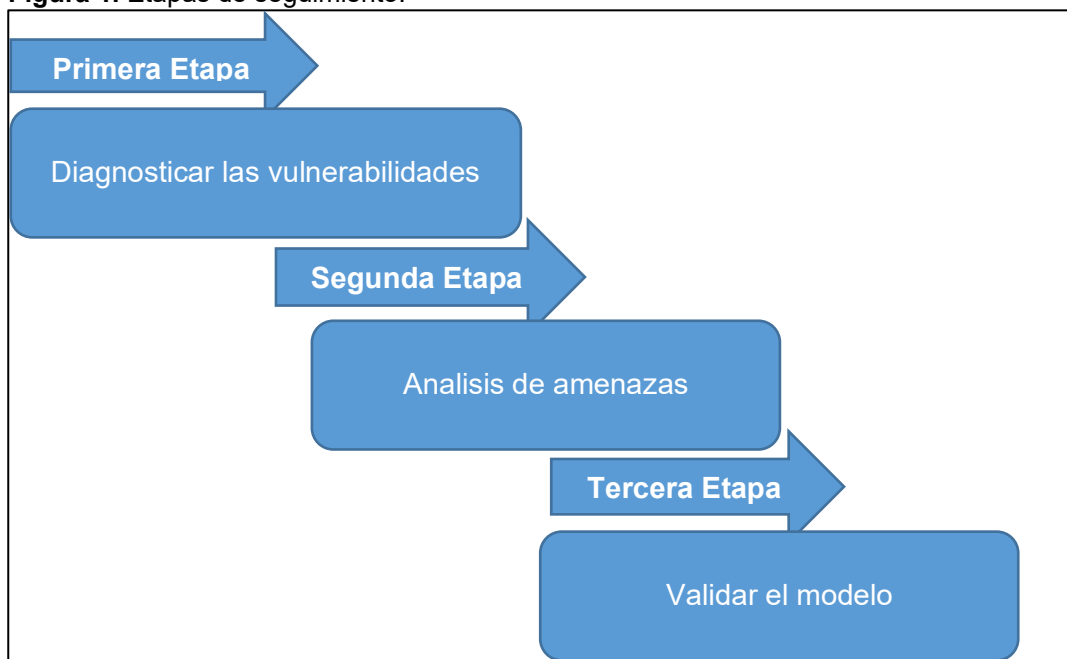
Ley de Delitos Informáticos, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones; con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes (Republica, LEY 1273 DE 2009, 2009)

3. DISEÑO DE LA INVESTIGACIÓN

El actual proyecto busca como finalidad la implementación y o utilización de un modelo de ciberseguridad aplicado a un entorno de domótica lot en hogares u entidades como negocios o pequeñas empresas con el fin de conocer y mitigar riesgos a su infraestructura propia o brindada por un tercero como servicio de este modo determinar causas analizar factores de riesgo.

Para desarrollar el siguiente proyecto se definirán 3 etapas que coincidirían al unisonó con los objetivos planteados correspondiendo a cada objetivo específico propuesto, cada etapa tendrá puntos a desarrollar para dar cumplimiento a dicha etapa.

Figura 1. Etapas de seguimiento.



Fuente: Autor.

Dichas etapas pueden demostrar la resolución de riesgos a través del razonamiento lógico es un proceso mental que implica aplicar la lógica, mediante este tipo de razonamiento se puede partir de una o varias premisas para llegar a una conclusión que puede ser verdadera, falsa o posible.

Algunos temas Propuestos y los cuales hemos abordado de los mismos para nuestro modelo son:

Primera etapa del 4.1 al 4.2: En esta etapa se buscará recopilar información relacionada a vulnerabilidades se demostrarán casos asociados se recopilará información de dispositivos y se realizarán descripciones de estos mismos de los mismos con el fin de Construir una matriz evaluativa de riesgos.

Segunda etapa todo el 4.3: En esta etapa se buscará el análisis y la cuantificación de posibles amenazas que afectan a un sistema y mediante las cuales un tercero podría aprovechar para vulnerar a dichos sistemas convierten a esta etapa en primordial ya que toma las amenazas de la etapa anterior y cuantifica el riesgo que pueda representar.

Tercera etapa del 4.4 al 4.9: En esta etapa se buscará construir un modelo de seguridad dividido en dos fases una se encargará se recopilar los datos anteriores de las etapas 1 y 2 que están asociadas a los objetivos, construyendo así un modelo inicial y un entorno simulado demostrativo.

La segunda fase tiene como fin de que el lector entienda como podría actuar los ciberdelincuentes usando un entorno demostrativo, para ello se construirá dicho entorno. Finalizando en la construcción el modelo Final.

4. DESARROLLO DEL TRABAJO DE GRADO

4.1. ¿Qué son los dispositivos IoT para el hogar?

El término IoT es la abreviatura de "Internet de las Cosas" (Internet of Things) y denota la gran red de objetos físicos de uso habitual (no solo computadoras o teléfonos) que cuentan con integrados sensores, software y otras tecnologías para conectarse a internet y recoger e intercambiar datos. (Fortinet,2021).

Al aplicar esta tecnología en el hogar ya existe el concepto de "hogar inteligente" (o smart home). Básicamente, se trata de cualquier dispositivo de tu hogar que sea capaz de "hablar" contigo y entre otros dispositivos a través de internet para hacerte la vida un poco más fácil (Mokosmart,2020).

4.1.1. Su funcionamiento el ciclo de la automatización.

El funcionamiento de estos comunes dispositivos sigue un esquema regular que puede resumirse en 4 pasos (ekidom, 2023):

- 1. Sensor (Recoger).** El dispositivo utiliza sus sensores para recoger información del entorno (temperatura, movimiento, iluminación, humedad...).
- 2. Actuar.** Un actuador ejecuta una acción física. Encender una luz, abrir una cerradura, activar una alarma, subir una persiana, etc.
- 3. Procesar y decidir.** La información recogida por los sensores es enviada a un controlador central (en ocasiones en la nube, o un dispositivo local como un hub) donde se procesa para obtener una decisión (activar un actuador, enviarte una alerta...).

4. Controlar. Tú, como usuario, puedes interactuar con el sistema a través de una interfaz: la app de tu teléfono celular, el asistente personal (ej. Alexa, Google Home) o bien mediante comandos de voz.

5. El "Idioma" que hablan. Para que los dispositivos se entiendan entre sí, necesitan un idioma común. A esto se le llama protocolos de comunicación. Los más comunes en el hogar son (areatecnologia.com):

Protocolo, ¿Qué es?, ventajas clave.

Tabla 1. Tipos de protocolo.

Protocolo	¿Qué es?	Ventajas Clave
Wi-Fi	La misma red que usas para tu teléfono, computador, tv, ect.	Fácil configuración, alta velocidad y no necesitas un dispositivo central adicional (hub) para la mayoría de los casos. Ideal para enviar vídeos de tus cámaras
Zigbee	Un protocolo de bajo consumo y bajo costo.	Ideal para sensores pequeños (de puertas, movimiento, temperatura). Consume muy poca batería. Suelen necesitar un "hub" que actúe como traductor para que se comuniquen con tu WiFi.

Nota: Tabla elaborada por el autor.

4.1.2. ¿Para qué sirven en el día a día?

Se enumeran a continuación algunos usos prácticos, aunque estos son casi innumerables. Los ejemplos que daré son algunos de los más comunes conforme he ido investigando (prometeo-fp.com,2024):

Comodidad y control a distancia (Ahorro Energético): puedes dar órdenes para encender/apagar luces, bajar/subir persianas, encender calefacción, etc. a través de un pedido verbal o mediante el teléfono sin tener que levantarte del sofá o cuando ya has salido de casa, evitando una posible pérdida económica. Las acciones se pueden hacer con horarios y rutinas.

Simulación de presencia (Seguridad): puedes programar las luces o el televisor de tu casa a un horario, y hacer que se enciendan y apaguen de la misma forma que si estuvieras en casa los días que no lo estás, haciendo así creer que hay alguien en el interior, disuadiendo de este modo a los intrusos.

Supervisar y alertar en tiempo real (Seguridad): puedes recibir alertas en tu móvil cuando se ha abierto una puerta o ventana, si hay detección de movimiento cuando no estás, o bien si hay flujo de humo/gas/agua pudiendo actuar al instante.

Información y registro: puedes conocer el consumo energético de tu hogar o de tus electrodomésticos, o bien saber quién ha pasado por tu casa cuando recuperas las imágenes que ofrece la cámara.

4.1.3. Componentes que conforman un hogar inteligente.

los dispositivos IoT para el hogar pueden transformar tu casa en un espacio más cómodo, eficiente y seguro. Se ha preparado una lista con los más comunes y útiles, su descripción imagen y dónde encontrarlos.

Sobre algunos de estos dispositivos se llevará a cabo el análisis de ciberseguridad llegando así a el modelo propuesto en el objetivo del siguiente proyecto de grado, analizando los riesgos que se pueden presentar ante un cibercriminal o delincuente con la suficiente preparación y conocimiento para vulnerar dichos dispositivos.

Listas de componentes para el hogar.

A continuación, se listarán los componentes más comunes y o accesibles para el hogar con el fin de dar a conocer que dispositivos convierten nuestro hogar en un hogar inteligente, si bien los dispositivos a continuación no pretenden ser un estándar, los más nuevo u lo más avanzado que se pueda adquirir en el mercado concluyendo así de este modo, solo se busca comprender las cualidades de como iniciar en un hogar inteligente en sus primeras etapas.

El centro de control (Hub o Gateway).

También antes de comenzar, es importante saber que algunos dispositivos requieren un cerebro o hub. Este pequeño artefacto se conecta al router y permite que todos los dispositivos puedan comunicarse entre sí y con los usuarios a través de internet.

Descripción: es la unidad central que conecta los dispositivos mediante protocolos (por ejemplo, Zigbee, Z-Wave o Bluetooth) que permite que se controlen desde una sola app y con la voz.

Ejemplos: Amazon Echo Plus, Samsung SmartThings Hub, Hub de TP-Link Tapo.

Dónde comprarlo: en Amazon, tiendas de electrónica como Powerplanet, o en las páginas de los propios fabricantes como Amazon (Echo) o TP-Link.

Figura 3. Smart Hub.



Fuente: Tapo Smart HomeBase.

Figura 2. Smart Hub Conexión.



Fuente: Tapo Smart HomeBase.

Enchufe Inteligente.

Descripción: Convierte cualquier aparato "tonto" (lámpara, ventilador, cafetera) en uno inteligente. Lo conectas a la pared y el aparato conectado a él y de este modo te permite encender/apagar desde el teléfono celular, programar horarios y usar comandos de voz, también se cuenta con modelos para interior y exterior (jardín).

Ejemplos: OIOSEN.

Dónde comprarlo: en Amazon, tiendas de electrónica como Powerplanet, Leroy Merlin o en las páginas de los propios fabricantes.

Figura 5. Enchufe inteligente.



Fuente: OIOSEN.

Figura 4. Enchufe inteligente fuente.



Fuente: OIOSEN.

Bombilla inteligente.

Descripción: Cambia la iluminación de tu hogar. Puedes regular su intensidad, cambiar de color, programar horarios (ej. que se enciendan al atardecer) y controlarlas por voz o desde el teléfono celular.

Ejemplos: Govee, Amazon Basic.

Dónde comprarlo: Amazon, tiendas de electrónica como Powerplanet, IKEA o en las páginas de los propios fabricantes.

Figura 6. Bobilla inteligente 1.



Fuente: Amazon.

Figura 7. Bobilla inteligente 2.



Fuente: Amazon.

Mando universal IR.

Descripción: Transforma en inteligentes tus aparatos con mando a distancia por infrarrojos (como el TV, el aire acondicionado o el ventilador). Aprende las señales de tus mandos y luego los controlas desde el teléfono celular o por voz simplificando o reduciendo la cantidad de mandos a distancias a un solo dispositivo de control universal.

Ejemplos: MoesGo, NOUS.

Dónde comprarlo: Amazon, Aliexpress o en las páginas de los propios fabricantes.

Figura 8.MoesGo WiFi IR Control.



Fuente: MoesGo.

Cámara de seguridad.

Descripción: Vigila tu hogar estés donde estés. Ofrecen visión nocturna, detección de movimiento (y a veces de personas/mascotas), audio bidireccional para hablar, y almacenan las grabaciones en la nube o en una tarjeta SD.

Ejemplos: Tapo TP-Link, Blink.

Dónde comprarlo: Amazon, tiendas de electrónica como Powerplanet o en las páginas de los propios fabricantes.

Figura 9. cámara lot Tapo.



Fuente: TP-Link.

Figura 10. cámara lot.



Fuente: TP-Link.

Sensor de puertas/ventanas.

Descripción: Te avisa si se abre una puerta o ventana. Es la base de un sistema de alarma casero. Se suele vincular con un Hub para activar alarmas, luces o notificaciones en tu teléfono celular.

Ejemplos: Tapo TP-Link.

Dónde comprarlo: Amazon o en las páginas de los propios fabricantes.

Figura 11.TP-Link Tapo T110 Sensor de Contacto.



Fuente: TP-Link.

ELABORADO POR:
Docencia

REVISADO POR:
Sistema Integrado de Gestión

APROBADO POR: Líder del Sistema Integrado de Gestión
FECHA APROBACIÓN: Octubre de 2023

Sensor de temperatura/humedad.

Descripción: Te permite monitorizar el clima de tu hogar. Puedes programar acciones automáticas, como encender un humidificador si el ambiente está muy seco o un ventilador si hace calor.

Ejemplos: Clicklife, Tapo TP-Link.

Dónde comprarlo: Amazon o en las páginas de los propios fabricantes.

Figura 13. CLICKLIFE Sensor de Temperatura Y Humedad Inteligente.

Sensor de temperatura y humedad Wi-Fi con retroiluminación



Fuente: Clicklife.

Figura 12. CLICKLIFE Sensor.



Fuente: Clicklife.

Central de Alarma.

Descripción: Es el cerebro de tu seguridad. Conecta todos los sensores (puertas, movimiento, humo) y, si alguien salta la alarma, puede emitir una sirena, enviarte una alerta y hasta notificar a una central receptora de alarmas.

Ejemplos: XUK-security.

Dónde comprarlo: Amazon o en las páginas de los propios fabricantes.

Figura 14. XUK kit de alarma de seguridad inteligente para el hogar.



Fuente: xuk- security

4.2. Vulnerabilidades críticas en dispositivos IoT domésticos.

El ecosistema IoT y su exposición.

Los dispositivos IoT de hogar, como, por ejemplo: sensores, enchufes inteligentes, cámaras IP, etc., han cambiado nuestras vidas; sin embargo, desgraciadamente esta interconexión ha aumentado considerablemente la superficie de ataque.

En el 2025 un informe de seguridad indicaba que las redes de hogares inteligentes eran atacadas, en promedio, 29 veces en apenas 24 horas con datos captados en 6,1 millones de hogares y 58 millones de dispositivos (Total Defense, 2026).

Además, el 6,6 % de los usuarios de dispositivos conectados ha vivido problemas asociadas a la seguridad o a la privacidad. La propia naturaleza del ecosistema IoT fragmentada, unida a limitaciones del hardware y otros aspectos que no favorecen la estandarización han creado las condiciones idóneas para que aparezcan vulnerabilidades que se pueden explotar fácilmente (Fortinet, s. f.).

4.2.1. Diagnóstico de vulnerabilidades por categoría.

(1) Fallas en autenticación.

Esta es, probablemente, la vulnerabilidad más extendida y explotada en el IoT doméstico. Se manifiesta de varias formas.

Credenciales por defecto débiles o genéricas: Por lo habitual, los dispositivos IoT instalados de fábrica presentan credenciales por defecto, es decir, un nombre de usuario y una contraseña por defecto débiles o genéricas (ej. admin/admin) (WeLiveSecurity, 2023); dado que los dispositivos IoT son obviados por los usuarios, dicha credencial por defecto a menudo permanece sin ser modificada (Rootstack, s. f.).

Los ciberdelincuentes son capaces de realizar el mapeo de dispositivos IoT a la búsqueda de dicho tipo de dispositivos en Internet mediante scripts automatizados, siendo capaces de tomar control del dispositivo en cuestión en pocos segundos.

La famosa botnet Mirai, responsable de ataques distribuidos de denegación de servicio (DDoS) ha sido capaz de propagarse aprovechándose de esta debilidad (Encryption Consulting, 2025).

Falta de autenticación en instrucciones sensibles: Un ejemplo reciente y con una gran gravedad es la vulnerabilidad CVE-2025-8627 (con una puntuación CVSS de 8,8/10) en el enchufe inteligente TP-Link KP303.

Esta vulnerabilidad permite a un atacante en la misma red, realizar instrucciones de protocolo sin autenticar, lo que puede llevar a apagados no deseados del dispositivo, y posiblemente, a la fuga de datos sensibles (Feedly, 2025).

Ausencia de autenticación multifactor (MFA/2FA): La gran mayoría de los aparatos, así como sus aplicaciones complementarias, no tienen capas adicionales de autenticación, por lo que son vulnerables si una contraseña es débil, reutilizada o robada en una fuga de datos por la falta de protección de contraseña en la aplicación Selenium.

(2) Cifrado deficiente o inexistente.

La protección de los datos en tránsito y en reposo es fundamental para la privacidad y la seguridad. En el IoT doméstico, esta área presenta graves carencias:

Datos en texto plano en la red local: Un gran número de dispositivos envía información a través de la red WiFi sin cifrar dicha información; esto permite que un

atacante que haya adquirido acceso a la misma red (por ejemplo, mediante la utilización de una contraseña WiFi débil o por el compromiso de un dispositivo) consiga interceptar y leer toda la información que viaja por la red (Rootstack, s. f.).

Este tipo de ataque se conoce como "Man-in-the-Middle" (MitM) o "ataque de intermediario", y puede acabar exponiendo desde las imágenes de una cámara de vigilancia hasta las credenciales de acceso a servicios externos (Cloudflare, s. f.).

Fuga de credenciales WiFi: Varios dispositivos almacenan o transmiten las credenciales de la red WiFi de casa sin cifrar. Un experimento de Kaspersky mostró cómo una cafetera de café inteligente era capaz de enviar información lo suficientemente poco cifrada como para que un investigador pudiese descubrir la contraseña maestra de toda la red WiFi del dueño (Total Defense, 2026).

Almacenamiento inseguro de datos: Campo: vulnerabilidades de hardware: no solo la comunicación era un problema. La vulnerabilidad CVE-2025-50777 en una cámara de seguridad AZIOT también provocaba un acceso root a este tipo de dispositivo.

Esta vulnerabilidad daba acceso a las credenciales WiFi y al servicio ONVIF en texto plano. En cuanto se tenía acceso a la cámara, se revelaban estas credenciales. (Feedly, 2025).

Cifrado en reposo o ausente: La inexistencia de medidas de cifrado en los datos almacenados de forma local en el dispositivo es un riesgo real ante el robo del hardware, donde un potencial atacante podría extraer dicha información de la memoria del aparato.

(3) problemas con las actualizaciones de firmware

La capacidad de un dispositivo para recibir e instalar actualizaciones de firmware de forma segura es esencial para corregir vulnerabilidades descubiertas después de su lanzamiento. Sin embargo, esta es una de las debilidades más sistémicas del sector:

Mecanismos de actualización inseguros: Cientos de dispositivos carecen de mecanismos seguros para actualizar su firmware. Incluyen la descarga de parches a través de caminos no cifrados (HTTP en vez de HTTPS); carecen de los procesos para verificar la integridad y autenticidad (lo que permite ataques de modificación 'Man-in-the-Middle'); o carecen de mecanismos 'anti-rollback' que permitan re-instalar versiones anteriores y vulnerables. (Keyfactor, 2020).

Falta de soporte a largo plazo (Obsolescencia): Con frecuencia, los fabricantes de dispositivos a bajo precio dejan de dar soporte al software un poco después de la aparición del producto. Como consecuencia, los dispositivos dejan de recibir parches de seguridad importantes durante la vida útil del dispositivo, lo que los convierte en puntos ciegos de seguridad de forma inalterable dentro de la red del hogar.

La categoría de dispositivos de streaming y televisores inteligentes pueden ser especialmente incompetentes con kernels obsoletos y débiles cadenas de suministro de firmware. (Rootstack, s. f.) (Total Defense, 2026).

Actualizaciones no automáticas y falta de notificaciones: Incluso en la existencia de actualizaciones, el proceso no suele ser automático, ya que algunos dispositivos no notifican al usuario de ello, lo que da la responsabilidad al consumidor, que normalmente ignora que dicha acción también debería realizarla

él. O bien algunos otros requieren de un reinicio manual, dejando el sistema expuesto durante el proceso de actualizaciones. (Keyfactor, 2020).

Manipulación en la cadena de suministro: La debilidad podría ser detectada antes de que el terminal se encontrara en disposición del usuario final. La cadena de suministro del firmware, que frecuentemente integra componentes de código abierto y programadores de terceras partes, es un punto sensible donde puede introducirse código malicioso (Total Defense, 2026).

En 2025 se dieron a conocer casos de delincuentes cibernéticos que añadieron firmware malicioso en los dispositivos Android de streaming empleados antes de abrir la caja por parte de los compradores. (Encryption Consulting, 2025).

(4) Exposición a redes Inseguras.

El ecosistema doméstico depende de la red WiFi y del router como núcleo central, lo que introduce vectores de ataque adicionales:

Dispositivos como puerta de entrada: Un router para el hogar se considera el "punto de acceso digital" para todo el hogar. Si un ciberdelincuente consiguiera acceder a él, podría monitorizar el tráfico de todos los dispositivos conectados, tener acceso a las cámaras de seguridad, robar credenciales personales y hacer secuestros (espionaje y robos) a gran escala (Total Defense, 2026), convirtiendo la red en un gran ataque para el hogar.

Una de las tendencias de la seguridad detectadas por F5 Labs fue que los escaneos de vulnerabilidades dirigidos a routers terminaron con un incremento del 91% en 2024 (Total Defense, 2026).

Formación de bot-nets para ataques DDoS: Al respecto, tal y como hemos mencionado en las líneas anteriores, los dispositivos IoT inseguros son un aspecto a tener en cuenta, ya que son el principal objetivo de la creación de grandes botnets. Cloudflare registró, hasta el año 2025.

Un ataque DDoS de ingentes y singulares proporciones, es decir, uno que fue lanzado por una variante de la botnet Mirai, cuyo origen fueron 13.000 dispositivos IoT inseguros (Keyfactor, 2020).

Igual hay que tener en cuenta el ataque DDoS de 22,2 Tbps, el cual se ha relacionado con ataques DDoS que se han lanzado desde dispositivos de hogares comprometidos, dando prueba así de la capacidad destructiva a través de las botnets (Fortinet, s. f.).

Segmentación de red deficiente: En la mayoría de las viviendas, todos los dispositivos (incluyendo el IoT) están conectados a la misma red WiFi que ordenadores y teléfonos personales.

Es decir, que cuando un atacante compromete un sensor de puerta o una bombilla poco segura, puede utilizar dicho dispositivo como punto de pivote o "lanzadera" (movimiento lateral hacia otras máquinas) para desplazarse a través de la red y atacar equipos de mayor valor, tales como:

Un computador portátil que almacene datos bancarios un dispositivo celular o teléfono móvil que almacena credenciales de dispositivos que monitorean el hogar entre otros aparatos conectados a la red que pueden ser vulnerables ante dichos ataques (SentinelOne, 2025).

Protocolos de red obsoletos: La falta de auditorías regulares y el uso de protocolos inalámbricos antiguos incrementan la exposición a ataques conocidos, como KRACK (Key Reinstallation Attack), que compromete la seguridad de las redes WiFi protegidas con WPA2 o protocolos más antiguos a este.

Con el fin de tomar control de la red inalámbrica permitiendo al atacante capturar el tráfico de la misma comprometiendo información privada o bloqueando el acceso a red de sus legítimos usuarios.

4.2.2. Matriz de diagnóstico de vulnerabilidades por tipo de dispositivo.

A continuación, se realiza la matriz y haciendo uso de la información obtenida de los anteriores análisis de los dispositivos se construirá una matriz la cual mediante esta se otorgarán niveles de usando un formato de escala que va de la siguiente forma.

Para los dispositivos dependiendo de su nivel de vulnerabilidad hacendera según su determinado análisis dando estos posibles resultados: baja, media, alta y critica, así de este modo se continuará evaluando los siguientes parámetros en los dispositivos como: su Autenticación, Cifrado, Actualizaciones y Redes “conexión”.

Tabla 2.Matriz de Vulnerabilidades.

Categoría de Dispositivo	Autenticación	Cifrado	Actualizaciones	Redes y conexión
Enchufe Inteligente	Crítica: Comandos sin la autenticar (Ej. CVE-2025-8627).	Alta: Puede filtrar datos mediante la red e información del propio dispositivo	Alta: Las vulnerabilidades se solucionan parcheando el firmware.	Alta: El atacante debe estar en la misma red, facilitando el pivoteo
Cámara IP	Crítica: Credenciales débiles o acceso root sin autenticar.	Crítica: Transmisiones de vídeo en texto plano y almacenamiento inseguro de credenciales Wifi	Crítica: Firmware con RCE (CVE-2025-65817) y falta de parches	Crítica: Son un objetivo principal para formar parte de botnets y ataques DDoS
Sensores varios	Media: A menudo usan credenciales de fábrica.	Media: Depende del fabricante, algunos transmiten datos sin cifrar.	Crítica: Suelen tener una vida útil larga sin soporte de software. Su firmware es difícil de actualizar.	Crítica: Su bajo consumo y necesidad de estar siempre activos los hace ideales para botnets.
Asistentes de Voz / Hubs	Alta: Son el punto central, una intrusión aquí compromete todo el ecosistema.	Crítica: Pueden exponer conversaciones privadas y datos de la cuenta	Alta: Su software debe actualizarse regularmente.	Crítica: Un hub comprometido permite al atacante controlar todos los dispositivos conectados
Bombillas Inteligentes	Media: Las más simples a menudo tienen autenticación débil.	Baja: Suelen estar en redes locales aisladas (como Zigbee), pero pueden ser un punto de entrada.	Baja a Media: Las bombillas más económicas raramente reciben actualizaciones.	Alta: En redes Wifi abiertas, pueden ser un punto de entrada vulnerable.

Nota: Tabla elaborada por el autor.

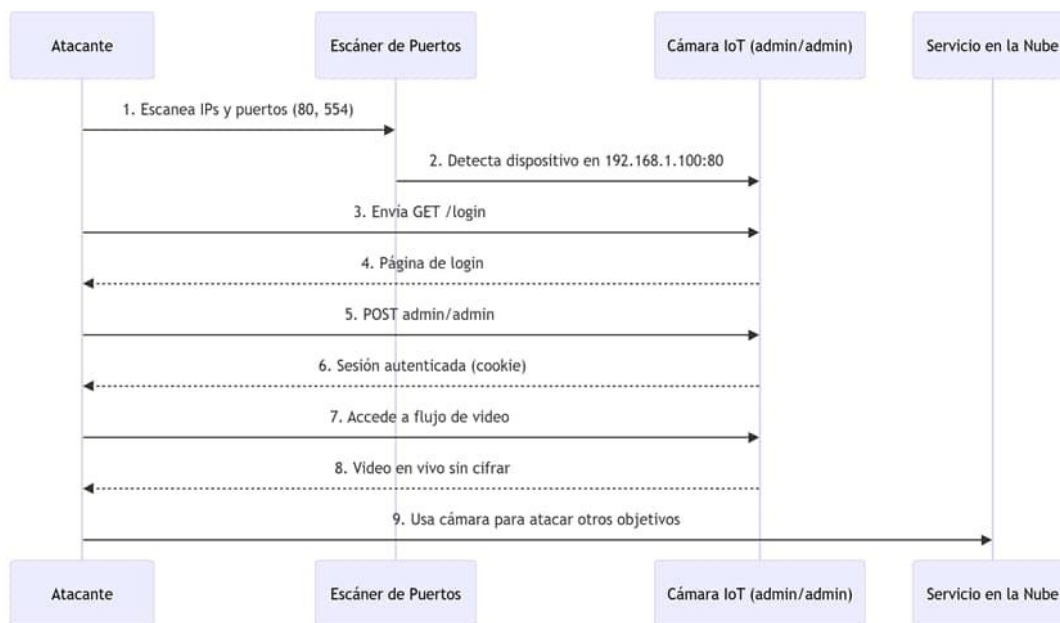
4.2.3. Representación de un ataque mediante diagramas

Para desarrollar cada una de las cuatro principales vulnerabilidades (autenticación, cifrado, actualizaciones y redes inseguras), cada una de estas vulnerabilidades dispone de un diagrama de secuencia UML correspondiente que ilustra, paso a paso, cómo un atacante puede explotar la vulnerabilidad en un hogar inteligente mediante dicha vulnerabilidad. Los diagramas siguen la notación textual estándar, por lo que puedes visualizarlo sin mayores inconvenientes.

1. Vulnerabilidad: Fallas en Autenticación (Credenciales por defecto)

Escenario: El atacante escanea la red en busca de un dispositivo IoT (ej. cámara IP) que todavía usa admin/admin.

Figura 15. Diagrama Fallas en Autenticación.



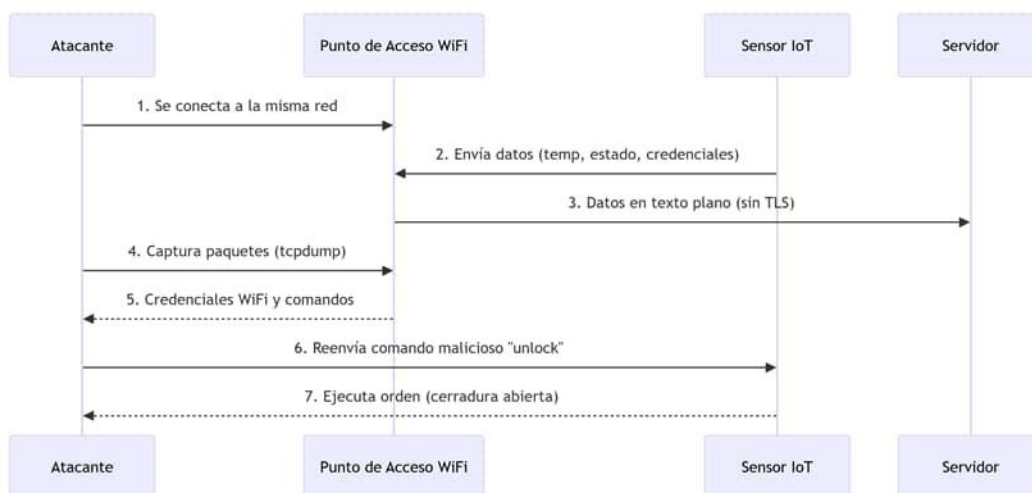
Fuente: Autor.

Explicación: El atacante solo necesita un escáner de redes (como Nmap o Shodan) para localizar dispositivos expuestos. Luego, con credenciales por defecto, obtiene control total. El paso crítico es la falta de cambio de credenciales por parte del usuario.

2. Vulnerabilidad: Cifrado Deficiente (Datos en texto plano)

Escenario: El atacante se conecta a la misma red WiFi (o realiza un ataque Man-in-the-Middle) y captura el tráfico no cifrado del dispositivo.

Figura 16. Diagrama Cifrado Deficiente.



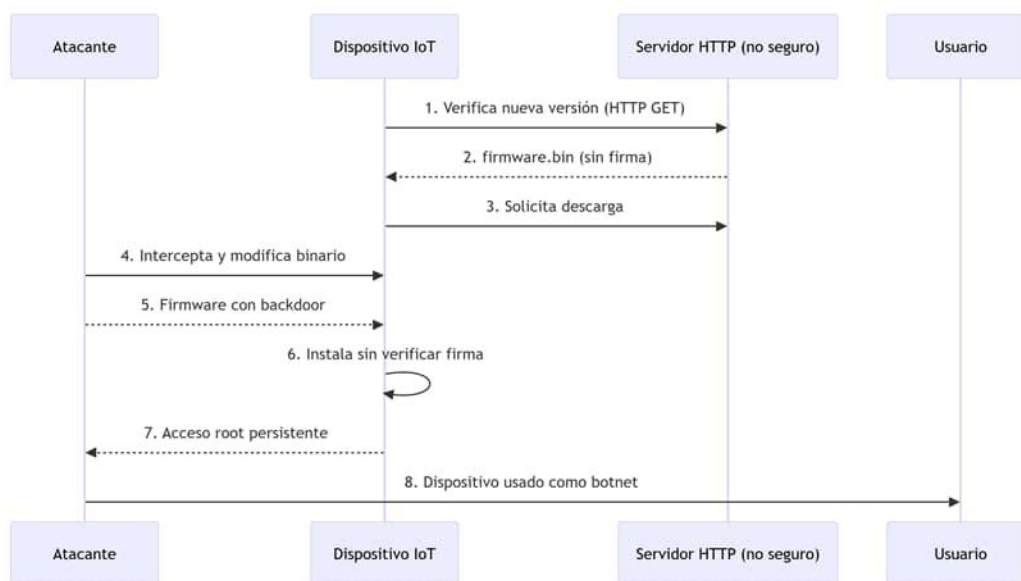
Fuente: Autor.

Explicación: La vulnerabilidad clave es que el dispositivo no cifra el tráfico ni verifica la integridad. El atacante puede leer y modificar los paquetes. Esto es común en sensores baratos y cámaras antiguas.

3. Vulnerabilidad: Actualizaciones de Firmware Inseguras (Sin HTTPS ni firma)

Escenario: El atacante intercepta la descarga de una actualización y la reemplaza con firmware malicioso (ataque Man-in-the-Middle en la actualización).

Figura 17. Diagrama Actualizaciones de Firmware Inseguras.



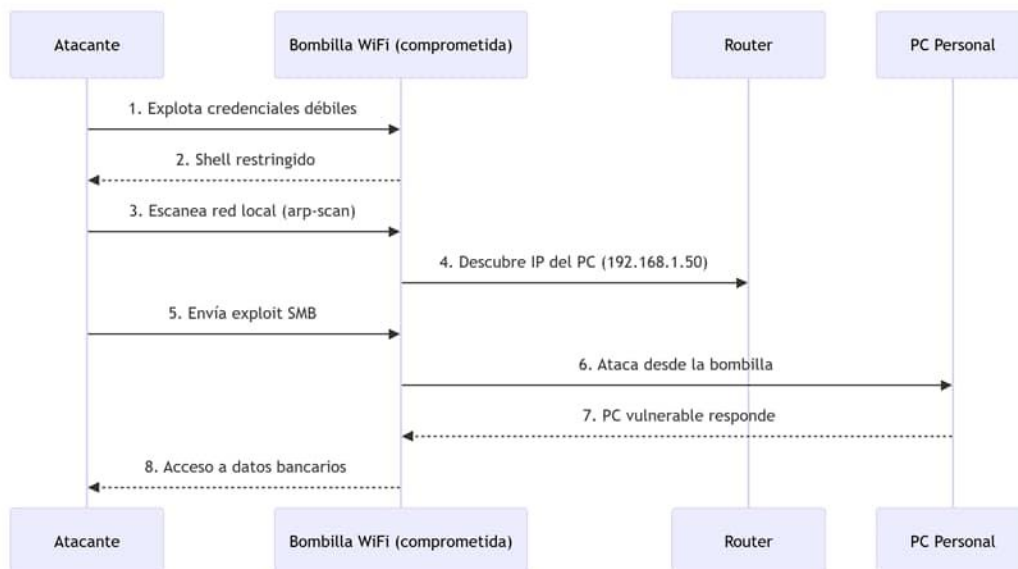
Fuente: Autor.

Explicación: El ataque es posible porque la actualización se descarga por HTTP sin cifrar y el dispositivo no valida la firma digital del firmware. Así, el atacante puede inyectar código malicioso que se ejecutará con altos privilegios.

4. Vulnerabilidad: Exposición a Redes Inseguras (Movimiento lateral desde IoT hacia red principal)

Escenario: El atacante compromete un dispositivo IoT vulnerable (ej. bombilla WiFi) y lo usa como lanzadera para atacar el ordenador personal del usuario.

Figura 18. Diagrama Exposición a Redes Inseguras



Fuente: Autor.

Explicación: El error principal es que todos los dispositivos (IoT y ordenadores personales) están en la misma subred sin segmentación. Una vez que el atacante controla cualquier IoT con baja seguridad, puede moverse lateralmente hacia equipos más valiosos. La mitigación es usar una red de invitados para los IoT.

4.3. Analizar los tipos de amenazas.

El diagnóstico de vulnerabilidades realizado permitió establecer un mapa claro de las debilidades más comunes en dispositivos IoT domésticos, tales como fallas en autenticación, cifrado insuficiente, firmware sin actualizaciones y exposición a redes inseguras. Sin embargo, identificar vulnerabilidades es solo el primer paso:

El verdadero riesgo surge cuando estas debilidades son aprovechadas por actores maliciosos para ejecutar amenazas cibernéticas.

En este sentido, el análisis en los tipos de amenazas cibernéticas se va a centrar en cómo dichas vulnerabilidades se transforman en ataques concretos como accesos no autorizados, infecciones de malware, ataques de denegación de servicio distribuido (DDoS), suplantación de identidad y manipulación de datos, apoyándose en estudios de casos y literatura especializada.

Este análisis permitirá comprender la relación directa entre las fallas técnicas y los escenarios de ataque, aportando insumos críticos para el diseño de un modelo de gestión en ciberseguridad y domótica resiliente, según los lineamientos establecidos en la norma (ISO 27005:2022) sobre gestión de riesgos de seguridad de la información y en el informe (NIST IR 8228) sobre consideraciones de ciberseguridad y privacidad en entornos IoT.

4.3.1. Identificación de vulnerabilidades y definición del alcance del análisis.

Antes de transformar las vulnerabilidades del Objetivo 1 en amenazas, es necesario delimitar formalmente sobre qué dispositivos recae el análisis y bajo qué criterios se va a evaluar cada amenaza.

Esta delimitación evita que el análisis se disperse y garantiza que los resultados sean comparables entre sí, requisito indispensable para construir la matriz de riesgos en la Evaluación de impacto y probabilidad.

Alcance del análisis: dispositivos objeto de estudio.

Tabla 3. A1 Alcance del análisis de amenazas.

Categoría de dispositivo	Rol dentro del hogar inteligente	Vulnerabilidad heredada del Objetivo 1
Cámaras IP (seguridad/vigilancia)	Captura y transmisión de video/audio en tiempo real	Cifrado deficiente; credenciales por defecto
Sensores (puerta/ventana, temperatura/humedad)	Recolección de datos del entorno para activar rutinas	Cifrado deficiente; exposición a redes inseguras
Hubs / gateways (unidad central de control)	Orquestación y enrutamiento de todos los dispositivos conectados	Fallas de autenticación; actualizaciones de firmware inseguras
Bombillas inteligentes	Automatización de iluminación, punto de entrada típico en redes planas	Exposición a redes inseguras; protocolos obsoletos
Asistentes virtuales (altavoces inteligentes)	Interfaz de voz y puente hacia servicios en la nube	Fallas de autenticación; cifrado deficiente en la transmisión de comandos

Nota: Tabla elaborada por el autor, Alcance del análisis de amenazas y su relación con el diagnóstico del Objetivo 1.

Se seleccionan estas cinco categorías por representar, en conjunto, la totalidad de los vectores de riesgo identificados en la sección “4.2” (autenticación, cifrado, actualizaciones y red); el enchufe inteligente, el mando universal y la central de alarma inventariados en la sección “4.1” quedan cubiertos de forma transversal por las mismas cuatro categorías de vulnerabilidad y no requieren un tratamiento diferenciado adicional para efectos de este análisis.

El dimensionamiento de esta problemática se apoya en cifras recientes: entre enero y octubre de 2025, las tecnologías de Bitdefender detectaron 13 600 millones de

ataques y bloquearon 4600 millones de intentos de explotación de vulnerabilidades en dispositivos IoT de consumo, a partir de telemetría de 6,1 millones de hogares inteligentes y más de 58 millones de dispositivos, con un promedio de 22 dispositivos conectados por hogar (Bitdefender & NETGEAR, 2025).

El mismo informe desagrega las vulnerabilidades conocidas por tipo de dispositivo: los dispositivos de streaming concentran el 26%, los televisores inteligentes el 21% y las cámaras IP el 9% del total documentado, lo que confirma con datos empíricos que las cámaras de seguridad incluidas en el alcance de este análisis se encuentran entre las categorías de mayor exposición reportada en la industria (Bitdefender & NETGEAR, 2025).

4.3.2. Criterios de evaluación.

Cada amenaza identificada en la “Clasificación de amenazas” se evalúa bajo tres criterios complementarios, que se aplican de manera consistente en toda la sección:

Impacto: magnitud del daño que produciría la materialización de la amenaza sobre la confidencialidad, la integridad o la disponibilidad de la información y de los servicios del hogar inteligente.

Probabilidad: frecuencia o verosimilitud con que la amenaza podría materializarse, considerando la facilidad técnica del ataque y la exposición real del dispositivo.

Tipo de amenaza: naturaleza del ataque según su mecanismo (por ejemplo, suplantación, manipulación, divulgación de información o denegación de servicio), lo que permite agrupar amenazas afines y diseñar controles específicos por familia.

4.3.3. Sustento normativo.

La norma ISO/IEC 27005:2022, Seguridad de la información, ciberseguridad y protección de la privacidad y la orientación para la gestión de riesgos de seguridad de la información, aporta el proceso metodológico que estructura este objetivo:

identificación de activos, identificación de amenazas y vulnerabilidades asociadas, estimación de la probabilidad y el impacto, y determinación del nivel de riesgo (ISO/IEC 27005, 2022). Los puntos del 4.3.1 al 4.3.5 de este apartado que siguen de forma literal esa secuencia.

Por su parte, el informe NIST IR 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, complementa a ISO/IEC 27005 al señalar que los dispositivos IoT poseen características únicas frente a la TI tradicional-interacción directa con el mundo físico, capacidades de cómputo y memoria restringidas, y dificultad para operar.

Actualizar o monitorear el dispositivo que alteran la probabilidad de explotación de una amenaza (National Institute of Standards and Technology [NIST], 2019).

Por esta razón, la escala de probabilidad que se construye en el punto “4.3.5. Evaluación de impacto y probabilidad” no se basa únicamente en la frecuencia estadística del ataque, sino también en estas características propias del IoT doméstico.

Para operacionalizar el criterio de tipo de amenaza definido más arriba, este objetivo retoma de forma explícita la estructura que NIST IR 8228 propone para razonar sobre el riesgo IoT: tres consideraciones de riesgo que diferencian a estos

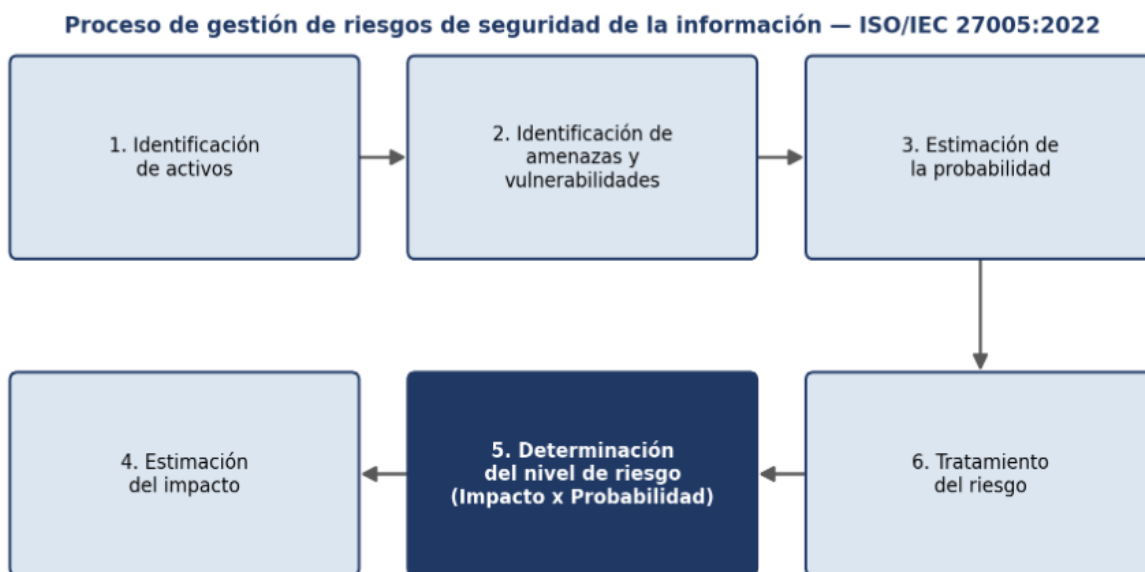
dispositivos de la TI convencional, y tres metas de mitigación sobre las cuales dichas consideraciones repercuten (National Institute of Standards and Technology [NIST], 2019).

Tabla 4. A2 Consideraciones de riesgo y metas de mitigación

Elemento de NIST IR 8228	Descripción oficial (resumida)	Aplicación en este objetivo
Consideración 1 - Interacción con el mundo físico	Muchos dispositivos IoT interactúan con el entorno físico de forma que la TI convencional normalmente no lo hace, lo que exige reconocer el impacto físico de un compromiso	Sustenta el impacto catastrófico asignado a sensores y centrales de alarma en la Tabla C
Consideración 2 - Acceso, gestión y monitoreo del dispositivo	Muchos dispositivos IoT no pueden ser accedidos, gestionados o monitoreados de la misma forma que un equipo de TI convencional	Explica por qué la detección tardía se incorpora en la escala de probabilidad de la Tabla C
Consideración 3 - Disponibilidad, eficiencia y efectividad de las capacidades	Las capacidades de ciberseguridad y privacidad disponibles en un dispositivo IoT suelen ser distintas -y con frecuencia menores- que las de un dispositivo de TI convencional	Sustenta la necesidad de medidas de mitigación diferenciadas por nivel de riesgo del Punto 4.3.6
Meta 1 - Proteger la seguridad del dispositivo	Evitar que el dispositivo sea usado para ejecutar ataques, incluida su participación en botnets DDoS	Corresponde a las amenazas de secuestro por credenciales (Mirai) y movimiento lateral (Dyn)
Meta 2 - Proteger la seguridad de los datos	Proteger la confidencialidad, integridad y disponibilidad de los datos recolectados, almacenados o transmitidos por el dispositivo	Corresponde a la amenaza de interceptación de tráfico (Nest/AZIOT)
Meta 3 - Proteger la privacidad de las personas	Proteger la privacidad de las personas afectadas por el procesamiento de su información, más allá de la protección del dispositivo y de los datos	Corresponde al factor humano y a las medidas de concienciación del Punto 4.3.6

Nota: Tabla elaborada por el autor basada en el NIST IR 8228 aplicadas a este objetivo (National Institute of Standards and Technology [NIST], 2019).

Figura 19. Proceso de gestión de riesgos de seguridad de la información.



Fuente: Autor.

4.3.4. Clasificación de amenazas

Siguiendo la lógica de un análisis de amenazas propio de la ingeniería de sistemas, cada una de las cuatro vulnerabilidades diagnosticadas en el Objetivo 1 se transforma aquí en una amenaza concreta, clasificada según su naturaleza (mecanismo de ataque, adaptado del modelo STRIDE de clasificación de amenazas) y su consecuencia sobre el triángulo de confidencialidad, integridad y disponibilidad (CID).

Cada amenaza se ilustra con un caso documentado en la literatura de ciberseguridad IoT, lo que evita conjeturas y ancla el análisis en evidencia verificable.

Tabla 5. B1 Transformación de vulnerabilidades en amenazas clasificadas por naturaleza, mecanismo y consecuencia.

Vulnerabilidad (Objetivo 1)	Amenaza concreta	Naturaleza / mecanismo	Consecuencia (CID)	Caso documentado
Fallas en autenticación (credenciales por defecto, sin MFA)	Secuestro del dispositivo por acceso no autorizado	Suplantación de identidad: escaneo masivo (Shodan/Nmap) y prueba automatizada de credenciales de fábrica	Confidencialidad e integridad: control remoto no autorizado del dispositivo	Mirai Botnet
Cifrado deficiente o inexistente	Interceptación de tráfico y robo de credenciales	Divulgación de información: captura de tráfico en texto plano (Man-in-the-Middle) dentro de la red local	Confidencialidad: exposición de video, audio o credenciales WiFi	Nest Thermostat
Actualizaciones de firmware inseguras	Inyección de firmware malicioso y persistencia	Manipulación: descarga de actualizaciones por canal no cifrado, sin firma digital ni verificación de integridad	Integridad y disponibilidad: el dispositivo queda bajo control permanente del atacante	Mozi Botnet
Exposición a redes inseguras y protocolos obsoletos	Movimiento lateral y formación de botnets para DDoS	Denegación de servicio: pivote desde un IoT comprometido hacia la red principal; agregación de miles de dispositivos en una botnet	Disponibilidad: interrupción de servicios propios y de terceros a gran escala	Ataque a Dyn (2016)

Nota: Tabla elaborada por el autor.

Como marco de clasificación complementario, de uso extendido en la industria, cada amenaza se contrasta además con el OWASP IoT Top 10 (2018), la lista de las diez categorías de debilidad más críticas en el ciclo de vida de un dispositivo IoT publicada por la OWASP Foundation (2018).

Tabla 6. B2 Correspondencia entre las amenazas priorizadas.

Amenaza (Objetivo 2)	Categoría OWASP IoT Top 10 (2018)	Descripción oficial (resumida)
Secuestro por credenciales por defecto (Mirai)	11 - Weak, Guessable, or Hardcoded Passwords	Uso de credenciales fácilmente vulnerables por fuerza bruta, públicamente disponibles o no modificables, incluidas puertas traseras en el firmware
Interceptación de tráfico y robo de credenciales (Nest/AZIOT)	17 - Insecure Data Transfer and Storage	Ausencia de cifrado o de control de acceso sobre datos sensibles en tránsito, en reposo o durante el procesamiento
Firmware malicioso y persistencia (Mozi)	14 - Lack of Secure Update Mechanism	Incapacidad de actualizar el dispositivo de forma segura: sin validación de firmware, sin entrega cifrada, sin mecanismos anti-rollback
Movimiento lateral y botnets DDoS (Dyn)	12 - Insecure Network Services / 19 - Insecure Default Settings	Servicios de red innecesarios o inseguros expuestos a internet, junto con configuraciones de fábrica que no restringen el acceso

Nota: Tabla elaborada por el autor, basada en datos obtenidos OWASP IoT Top 10 (2018) (OWASP Foundation, 2018).

Caso 1. Mirai Botnet.

La botnet Mirai, cuyo código fuente fue publicado por su autor en 2016, infecta dispositivos IoT domésticos como cámaras IP, routers y grabadores digitales probando de forma automatizada un listado de credenciales de fábrica sin modificar.

La Agencia de Ciberseguridad e Infraestructura de los Estados Unidos advirtió formalmente sobre esta amenaza al identificar que decenas de miles de dispositivos

IoT inseguros fueron reclutados en cuestión de horas (Cybersecurity and Infrastructure Security Agency [CISA], 2016).

El análisis retrospectivo de Antonakakis et al. (2017), presentado en el USENIX Security Symposium, documenta que la botnet llegó a superar los 600 000 dispositivos infectados, confirmando que la falla de autenticación por defecto la misma diagnosticada en la sección “4.2.1” de este documento es replicable a escala masiva.

Caso 2. Nest Thermostat.

En la conferencia Black Hat USA 2014, Jin et al. (2014) demostraron que el termostato inteligente Nest carecía de un mecanismo de arranque seguro (secure boot), lo que permitía a un atacante con acceso físico de pocos segundos instalar un firmware modificado y desde allí, interceptar el tráfico de red del hogar, incluidas las credenciales WiFi transmitidas sin cifrado robusto.

Este caso ilustra, en un dispositivo de consumo masivo, el mismo patrón descrito en la sección “4.2.1” para la cámara AZIOT (CVE-2025-50777): la ausencia de cifrado en tránsito o en reposo convierte un dispositivo doméstico en una puerta de entrada a la totalidad de la red del hogar.

Caso 3. Mozi Botnet.

Mozi es una botnet de arquitectura punto a punto (peer-to-peer), derivada parcialmente del código de Mirai, que explota contraseñas Telnet débiles y cerca de una decena de vulnerabilidades de firmware sin parchear en routers y gateways domésticos.

El equipo de seguridad de Microsoft documentó que, entre octubre de 2019 y junio de 2020, Mozi llegó a representar cerca del 90 % del tráfico malicioso observado en dispositivos IoT, y que la botnet logra persistencia adaptando su método de infección a la arquitectura específica de cada fabricante de gateway, incluidos Netgear, Huawei y ZTE (Microsoft Security, 2021).

Tabla 7. C1 Comparativa técnica entre las botnets Mirai y Mozi documentadas en este objetivo.

Característica	Mirai (2016)	Mozi (2019-2020)
Arquitectura de comando y control	Centralizada: servidor C2 único	Punto a punto (P2P), sin servidor central
Vector de infección inicial	Credenciales Telnet/SSH por defecto	Credenciales Telnet débiles y vulnerabilidades de firmware sin parchear
Dispositivos objetivo	Cámaras IP, routers, DVR	Routers y gateways domésticos (Netgear, Huawei, ZTE)
Origen del código	Original; código fuente publicado en 2016	Derivado parcialmente del código de Mirai
Objetivo principal	Ataques DDoS a gran escala	Persistencia, DDoS, exfiltración de datos y secuestro de sesiones HTTP/DNS
Escala documentada	Más de 600 000 dispositivos infectados (pico)	Cerca del 90 % del tráfico malicioso IoT observado (oct. 2019 - jun. 2020)
Caso vinculado en este documento	Caso 4 - Ataque a Dyn	Caso 3 - persistencia en gateways domésticos

Nota: Tabla elaborada por el autor.

Este caso corresponde directamente a la vulnerabilidad de actualizaciones de firmware inseguras descrita en la sección “4.2.1”: sin verificación de firma ni canal cifrado, el dispositivo no puede distinguir una actualización legítima de una maliciosa.

Caso 4. Ataque a Dyn (octubre de 2016).

El 21 de octubre de 2016, el proveedor de DNS gestionado Dyn sufrió tres oleadas de ataques de denegación de servicio distribuido que dejaron inaccesibles servicios como Twitter, Netflix, PayPal, Spotify y GitHub durante varias horas.

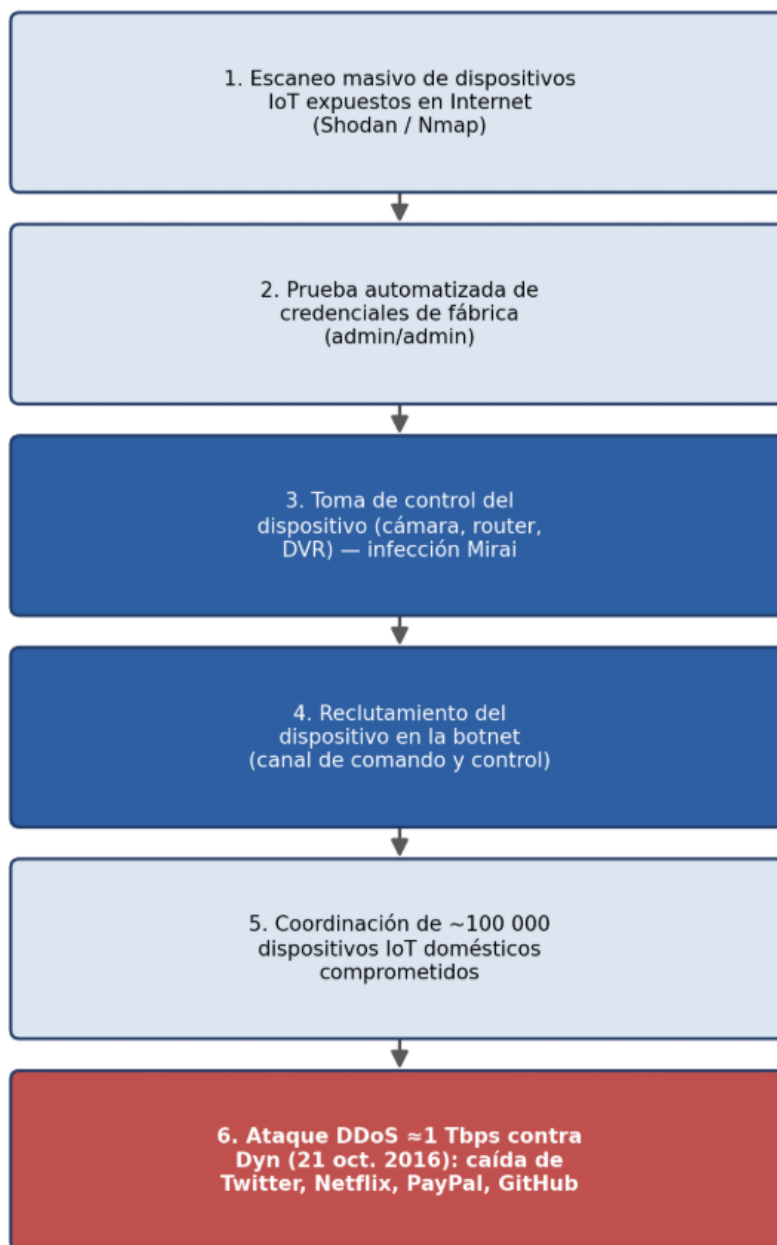
El tráfico malicioso, cercano a 1 Tbps, provino de aproximadamente 100 000 dispositivos IoT domésticos infectados con Mirai, cámaras, DVR y routers que los atacantes utilizaron como plataforma de lanzamiento tras comprometerlos tal como se describe en el Caso 1 (Cloudflare, s. f.).

El ataque a Dyn es el ejemplo más citado en la literatura de ciberseguridad para demostrar que la falta de segmentación de red y el uso de protocolos obsoletos en el hogar, vulnerabilidades diagnosticadas en la sección “4.2.1” de este documento no solo ponen en riesgo al propietario del dispositivo, sino que convierten cada hogar inteligente en un vector de ataque contra infraestructura crítica de terceros.

Descripción: Figuras 20. Cadena de ataque desde la vulnerabilidad de autenticación por defecto (Caso 1, Mirai) hasta la denegación de servicio distribuido contra Dyn (Caso 4, 2016).

Figura 20. Ataque a Dyn.

De la vulnerabilidad de autenticación al ataque a Dyn



Fuente: Autor.

4.3.5. Evaluación de impacto y probabilidad

Con las cuatro amenazas clasificadas, se procede a estimar su impacto y su probabilidad de ocurrencia, siguiendo el proceso de valoración de riesgo de ISO/IEC 27005 (2022) y adaptando la escala de probabilidad a las características propias del IoT doméstico descritas en NIST IR 8228 (National Institute of Standards and Technology [NIST], 2019). El nivel de riesgo se calcula como el producto Impacto x Probabilidad, sobre una escala de 1 a 5 en cada eje.

Como respaldo técnico adicional a la escala de impacto, las puntuaciones reportadas en la Ilustración C (7,5 a 9,1) siguen la metodología del Common Vulnerability Scoring System versión 3.1, publicada por FIRST.org, que calcula un puntaje base a partir del vector de ataque (red, adyacente, local o físico).

La complejidad del ataque, los privilegios requeridos y la interacción del usuario, combinados con el impacto sobre la confidencialidad, la integridad y la disponibilidad (FIRST, 2019).

Esta es la misma metodología que emplean el NVD del NIST y los fabricantes citados en la sección “4.2” de este documento para puntuar las vulnerabilidades allí reportadas, lo que garantiza consistencia entre el diagnóstico del Objetivo 1 y la evaluación de impacto de este objetivo.

Tabla 8. D1 Escalas de impacto y probabilidad aplicadas al análisis de amenazas IoT domésticas.

Nivel	Impacto (ISO/IEC 27005:2022)	Probabilidad (NIST IR 8228)
1	Insignificante: efecto perceptible mínimo, sin exposición de datos ni pérdida de control del dispositivo	Raro: requiere acceso físico prolongado y conocimiento técnico avanzado
2	Menor: afectación puntual a un dispositivo aislado, sin propagación	Improbable: exige condiciones específicas poco frecuentes en el hogar (p. ej. red ya comprometida)
3	Moderado: exposición de datos personales o pérdida temporal de disponibilidad de un servicio	Posible: explotable por un atacante con herramientas estándar y acceso a la red local
4	Mayor: control remoto no autorizado del dispositivo o de varios dispositivos del hogar	Probable: explotable de forma remota con herramientas automatizadas de uso común (p. ej. escáneres de red)
5	Catastrófico: pérdida total de control del ecosistema doméstico y/o uso del hogar como plataforma de ataque a terceros	Casi certero: vulnerabilidad publicada y explotada activamente en campaña (botnet conocida)

Nota: Tabla elaborada por el autor.

Tabla 9. D2 Matriz de evaluación de riesgo.

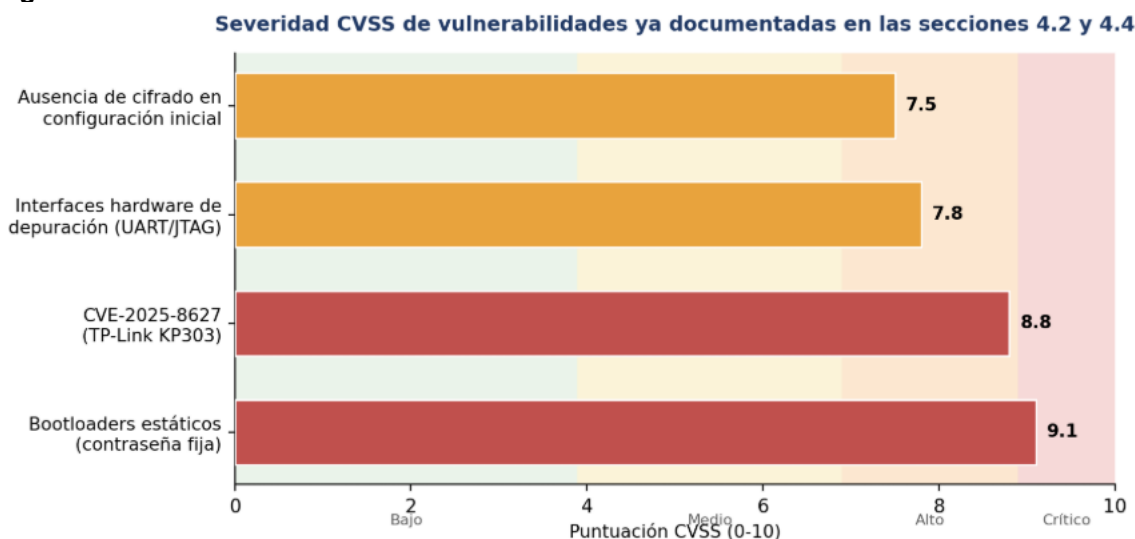
Amenaza	Impacto	Probabilidad	Riesgo (I x P)	Nivel de riesgo
Secuestro por credenciales por defecto (Mirai)	4 – Mayor	5 – Casi certero	20	Crítico
Interceptación de tráfico / robo de credenciales (Nest, AZIOT)	4 – Mayor	3 – Posible	12	Elevado
Firmware malicioso y persistencia (Mozi)	5 – Catastrófico	3 – Posible	15	Crítico
Movimiento lateral y botnets DDoS (Dyn)	5 – Catastrófico	4 – Probable	20	Crítico

Nota: Tabla elaborada por el autor, Matriz de evaluación de riesgo de las cuatro amenazas priorizadas. Riesgo = Impacto x Probabilidad.

Se adoptan tres niveles de riesgo operativos, consistentes con el alcance definido para este objetivo: moderado (riesgo entre 1 y 9), elevado (riesgo entre 10 y 15) y crítico (riesgo entre 16 y 25). Tres de las cuatro amenazas priorizadas como el secuestro por credenciales por defecto, firmware malicioso y movimiento lateral hacia botnets DDoS.

Se ubican en nivel crítico, lo que es consistente con los indicadores ya reportados en la sección “4.2” del documento, según los cuales las redes de hogares inteligentes reciben en promedio veintinueve (29) ataques cada 24 horas (Total Defense, 2026) y donde vulnerabilidades como CVE-2025-8627 alcanzan una puntuación CVSS de 8,8 sobre 10 (Feedly, 2025).

Figura 21. Puntuaciones CVSS.



Fuente: Autor.

Descripción: Figura 21. Puntuaciones CVSS de las vulnerabilidades ya documentadas en las secciones 4.2 y 4.4 de este trabajo, como referencia empírica de severidad técnica.

Mapa de calor (heatmap) de impacto x probabilidad.

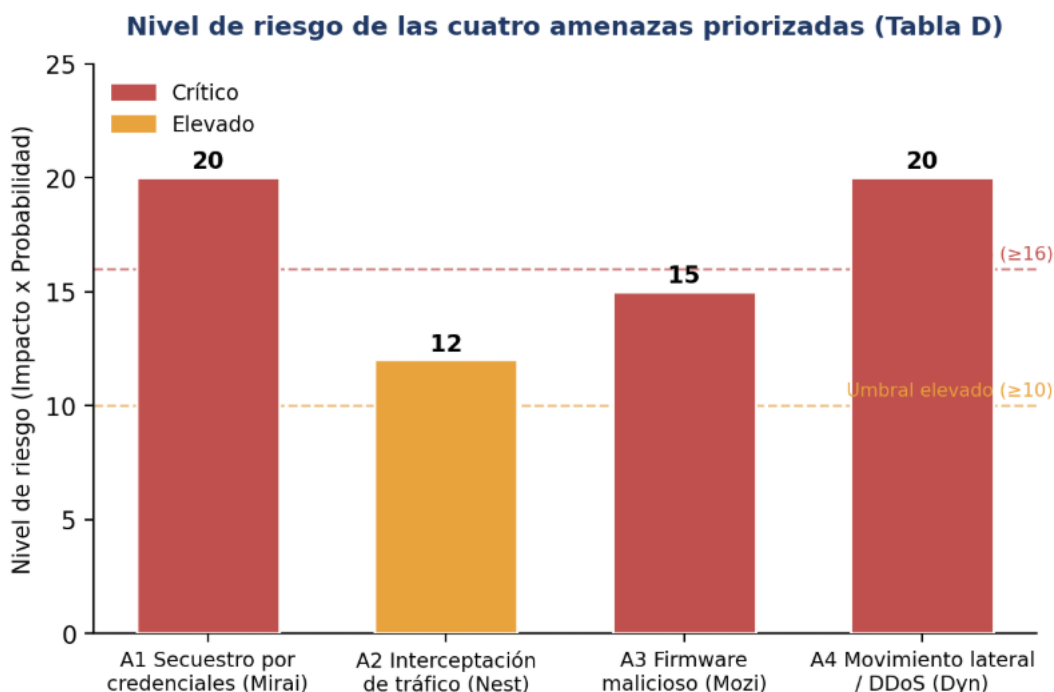
El siguiente mapa de calor ubica cada amenaza (A1-A4) en la celda correspondiente a su impacto y probabilidad, permitiendo visualizar de forma inmediata la concentración de riesgo crítico en la esquina superior derecha de la matriz.

Tabla 10. E1 Mapa de calor de riesgo.

Probabilidad\ Impacto	1. Insignificante	2. Menor	3. Moderado	4. Mayor	5. Catastrófico
5. Casi certero				A1	
4. Probable					A4
3. Posible				A2	A3
2. Improbable					
1. Raro					

Nota: Tabla elaborada por el autor, Tabla E. Mapa de calor de riesgo. A1 = secuestro por credenciales por defecto (Mirai); A2 = interceptación de tráfico (Nest/AZIOT); A3 = firmware malicioso (Mozi); A4 = movimiento lateral y botnets DDoS (Dyn). Verde = riesgo moderado, amarillo = elevado, rojo = crítico.

Figura 22. Nivel de riesgo.



Fuente: Autor.

Descripción: Figura 22 sobre la tabla D1. Nivel de riesgo (Impacto x Probabilidad) de las cuatro amenazas priorizadas, con los umbrales de clasificación aplicados en la Tabla D1

4.3.6. Priorización y plan de mitigación

A partir del nivel de riesgo obtenido en el anexo 4.3.5. Evaluación de impacto y probabilidad. Se diseñan estrategias diferenciadas según tres horizontes de acción: medidas inmediatas (aplicables sin inversión adicional, orientadas a contener el riesgo crítico), medidas preventivas (requieren configuración técnica o inversión menor) y medidas de concienciación (orientadas al factor humano).

Esta priorización alimenta directamente las cinco capas del modelo de ciberseguridad propuesto en el Objetivo Específico 3 de este documento (sección 4.5), del cual constituye el insumo de entrada.

Estas medidas se organizan siguiendo la misma lógica de las Baseline Security Recommendations for IoT de ENISA, la agencia de ciberseguridad de la Unión Europea, que agrupa las buenas prácticas de seguridad IoT en tres dominios complementarios.

Mediante las siguientes medidas de política y organización (gobernanza, gestión de activos, capacitación), medidas de personas y procesos (concienciación, gestión de proveedores) y medidas técnicas (autenticación, cifrado, actualización segura, segmentación de red) (European Union Agency for Cybersecurity [ENISA], 2017).

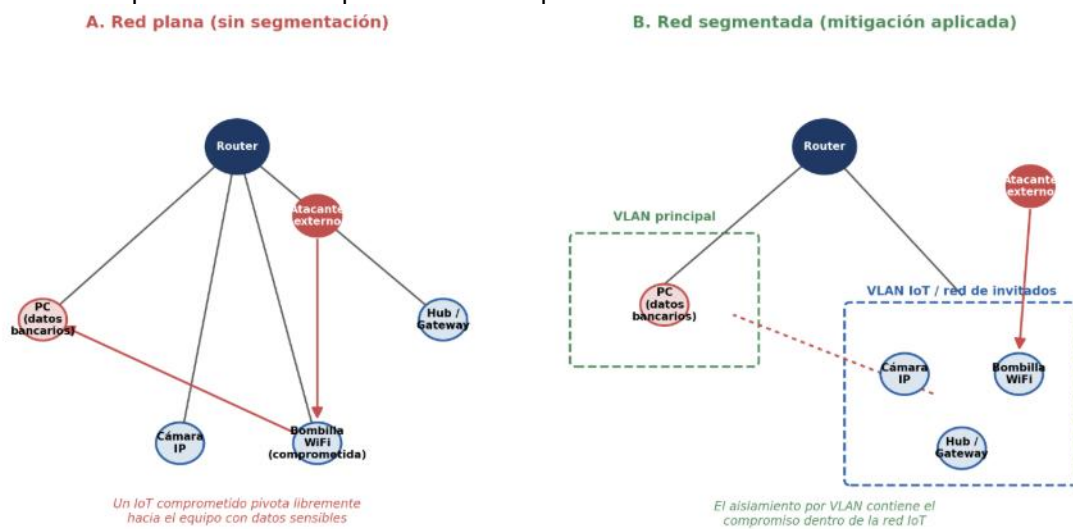
Las medidas inmediatas y preventivas de la Tabla F corresponden principalmente al dominio técnico, mientras que las medidas de concienciación corresponden al dominio de personas y procesos.

Tabla 11. F1 Plan de mitigación diferenciado por nivel de riesgo.

Nivel de riesgo	Medidas inmediatas	Medidas preventivas	Medidas de concienciación
Crítico (secuestro por credenciales, firmware malicioso, botnets DDoS)	Cambio obligatorio de credenciales por defecto; activación de MFA/2FA en cuentas y aplicaciones; segmentación inmediata de red (VLAN o red de invitados) para aislar el IoT de equipos con datos sensibles	Cifrado TLS 1.3 en tránsito; verificación de firma digital del firmware; actualizaciones automáticas con mecanismo anti-rollback; deshabilitación de puertos de depuración (UART/JTAG)	Capacitación inicial obligatoria sobre cambio de contraseñas en el primer uso; alertas contextuales que expliquen el riesgo de mantener credenciales de fábrica
Elevado (interceptación de tráfico y robo de credenciales)	Auditoría de dispositivos que transmiten datos sin cifrar; deshabilitación de servicios no utilizados (UPnP, Telnet, acceso remoto por defecto)	Monitoreo mediante IDS/IPS basado en IA/ML para detección de anomalías de tráfico; pruebas de penetración periódicas sobre el ecosistema doméstico	Guías de buenas prácticas y políticas de privacidad claras sobre los datos que recolectan cámaras y asistentes virtuales
Moderado (riesgos residuales y dispositivos de baja exposición)	Inventario actualizado de todos los dispositivos conectados	Evaluación trimestral del ecosistema IoT; política de fin de vida útil con reemplazo de dispositivos sin soporte del fabricante	Boletines informativos periódicos; uso de la guía práctica de diez pasos ya definida en la sección de Estrategias de Implementación de este documento

Nota: Tabla elaborada por el autor.

Figura 23. Comparación entre arquitectura de red plana.



Fuente: Autor.

Descripción: Figura 24. Comparación entre arquitectura de red plana (vulnerable al movimiento lateral del Caso 4) y arquitectura segmentada por VLAN, medida inmediata del nivel de riesgo crítico sobre la tabla F1.

4.3.7. Documentación y trazabilidad del análisis.

Para garantizar la replicabilidad y la validez académica del análisis, los resultados de los Puntos anteriores se consolidan en una única tabla maestra de trazabilidad, que enlaza cada vulnerabilidad del Objetivo 1 con su amenaza asociada, el caso documentado que la sustenta, el nivel de riesgo obtenido y la capa del modelo de ciberseguridad (Objetivo 3) encargada de mitigarla.

Esta tabla funciona como mapa de correlación: permite verificar, en una sola vista, que ninguna vulnerabilidad diagnosticada queda sin una amenaza, un nivel de riesgo y un control correspondiente.

Tabla 12. Tabla maestra de trazabilidad.

Vulnerabilidad (Obj. 1)	Amenaza (Obj. 2)	Caso documentado	Nivel de riesgo	Capa de mitigación (Obj. 3)
Fallas en autenticación	Secuestro por credenciales por defecto	Mirai Botnet	Crítico	Capa 2.1 – Gestión de identidades y credenciales
Cifrado deficiente o inexistente	Interceptación de tráfico y robo de credenciales	Nest Thermostat	Elevado	Capa 2.2 – Cifrado y protección de datos
Actualizaciones de firmware inseguras	Firmware malicioso y persistencia	Mozi Botnet	Crítico	Capa 2.3 – Actualizaciones seguras
Exposición a redes inseguras / protocolos obsoletos	Movimiento lateral y botnets DDoS	Ataque a Dyn (2016)	Crítico	Capa 3.1 – Segmentación de red

Nota: Tabla elaborada por el autor.

Complemento a la tabla matriz de riesgos.

CVEs ya documentados en las secciones “4.2” de este trabajo, vinculados a las amenazas priorizadas del Objetivo 2. Los campos sin puntuación CVSS reportada se dejan explícitos para no atribuir datos no verificados.

La replicabilidad del análisis queda garantizada por tres condiciones metodológicas: primero, los criterios de impacto y probabilidad se definen de forma explícita y se sustentan en normas internacionales de acceso público (ISO/IEC 27005:2022 y NIST IR 8228).

Por lo que otro investigador puede aplicar la misma escala sobre un conjunto distinto de dispositivos y obtener resultados comparables; segundo, cada amenaza se ancla en un caso documentado y verificable, en lugar de una estimación subjetiva; y tercero, el cálculo del nivel de riesgo sigue una fórmula reproducible (Impacto x Probabilidad) en lugar de un juicio cualitativo no trazable.

En conjunto, estas tres condiciones permiten que el Objetivo Específico 2 no solo describa el panorama de amenazas de los hogares inteligentes en Santander, sino que entregue al Objetivo Específico 3 una base de riesgo priorizada y justificada, sobre la cual construir y validar el modelo de ciberseguridad de cinco capas.

Tabla 13. De complemento a Matriz de Vulnerabilidades.

CVE	Dispositivo	CVSS	Vulnerabilidad asociada (Obj. 1)	Amenaza vinculada (Obj. 2)
CVE-2025-8627	Enchufe inteligente TP-Link KP303	8.8	Fallas en autenticación	Secuestro por credenciales por defecto (Mirai)
CVE-2025-50777	Cámara de seguridad AZIOT	No reportado en el documento	Cifrado deficiente (credenciales WiFi en texto plano)	Interceptación de tráfico (Nest/AZIOT)
CVE-2025-12599	Dispositivos BLU-IC	No reportado en el documento	Claves criptográficas compartidas	Firmware malicioso y persistencia (Mozi)
CVE-2025-65553	Sistema de seguridad D3D Wi-Fi ZX-G12	No reportado en el documento	Exposición a redes inseguras (bloqueo por RF en 433 MHz)	Denegación de servicio, categoría afín a movimiento lateral y botnets DDoS

Nota: Tabla elaborada por el autor.

A esto se suma que las puntuaciones de severidad utilizadas provienen de una metodología pública y auditable -CVSS v3.1 (FIRST, 2019)- y que la clasificación de amenazas se contrasta con dos marcos de referencia independientes entre sí: uno de la industria (OWASP IoT Top 10, OWASP Foundation, 2018) y uno de un organismo regulador (NIST IR 8228, National Institute of Standards and Technology [NIST], 2019).

Esta triangulación entre normas, marcos de clasificación y casos documentados permite que un tercero que replique este análisis sobre un conjunto distinto de

dispositivos IoT domésticos llegue a conclusiones metodológicamente comparables.

4.4. Construcción del modelo.

Para el cumplimiento de esta fase que corresponde al objetivo 3 se desarrollaron 2 actividades enunciadas en los puntos (4.4.1 y 4.7.1)

Actividad 1:

Desarrollar el modelo inicial para la ciberseguridad que comprenda la gestión de incidentes de seguridad, teniendo en cuenta las normas de riesgos, la ISO 27001, el NIST y las normas de gestión de incidentes, de tal forma que el modelo facilite la mitigación y el tratamiento de aquellos incidentes que sean identificados en dispositivos IoT por los residentes o prestadores del servicio TI en domótica.

La elaboración del modelo inicial comienza a partir de los resultados obtenidos en el objetivo 1 y 2, partiendo de los riesgos de cada dispositivo dedicado a la domótica y cómo eran los planes de tratamiento de los riesgos que se habían identificado como potencialmente causantes de un mayor impacto en los hogares inteligentes.

Actividad 2:

Dada la culminación de la actividad número 1 se construirá un entorno controlado de simulación el cual estará destinado a validar, demostrar y entender la estructura de una Smart home y retomando anexos del objetivo 1 y 2 para construir dicho entorno en donde se pondrá a prueba un modelo inicial planteado con el fin de flaquear sus puntos más vulnerables y corregir dichos aspectos encontrados

fortaleciendo así un modelo final más seguro, completo y robusto frente al modelo inicial propuesto.

4.4.1. Construcción del modelo inicial.

extensión de actividad 1.

El concepto de hogar inteligente ha logrado ser una realidad y, en la actualidad, estos lugares de vida han ido configurándose como un ciberecosistema digital, complejizándose poco a poco hasta alcanzar la media actual de 22 dispositivos por hogar conectado (Bitdefender, 2025).

Un cambio que ha supuesto un incremento considerable de la comodidad de las personas, pero que ha supuesto a su vez que los hogares se conviertan en los principales objetivos de los ataques cibernéticos automatizados a gran escala.

El trabajo de investigación que aquí se presenta propone un modelo de ciberseguridad multidimensional que tiene como principal objetivo abordar las vulnerabilidades que surgen de forma simultánea desde tres frentes diferentes, pero complementarios, que son: hardware, software y factor humano siendo estas descripción de las acciones previstas en el modelo que integran, a su vez, las mejores prácticas que se recogen, a su vez, en los documentos de NIST, ISO/IEC y grandes referentes de la industria (Comeau, 2025).

El citado modelo de ciberseguridad con el que se desarrolla esta investigación está estructurado en cinco capas de defensa que, siendo implementadas de forma conjunta, permiten mitigar considerablemente la exposición de los hogares inteligentes a las amenazas identificadas.

Respecto a lo anterior mencionado y con el apoyo de los anexos matriz de vulnerabilidad y matriz de riesgo propuesta en esta misma actividad, para la fase de prueba y ataque que se realizaran más adelante.

Por este se tomará en cuenta los dispositivos cuyo riesgo es representado por intromisión directa de un tercero (ciberdelincuente) y no por el método o factor de riesgo que busca atacar a la persona como individuo vulnerable extrayendo así información confidencial de la víctima mediante ingeniería social.

Este punto anterior se abarcará por el modelo final y no por el modelo inicial planteado a continuación por tal motivo se dará paso a la siguiente aclaración.

Con la construcción del modelo inicial que compete a la finalización de la actividad número uno (1) se buscara como factor prioritario en el modelo inicial solo el hardware y el software, de ese modo el factor humano como eje fundamental su prioridad escalaría en el modelo final.

Por ende, así construyendo así un modelo más sólido donde se busca concientizar al usuario con el fin de que pueda asimilar estos potenciales riesgos y a el mismo como una de las posibles víctimas en ser el blanco de posibles ataques.

De este modo se busca llegar al usuario final con información clara, precisa y concreta ya que este modelo final no busca agobiar al usuario final con tecnicismos si no estar más enfocado hacia la concientización y asimilación por parte del propio usuario como el mismo que como factor de riesgo evitando que dicha persona se vea o perciba atacada hacia su persona como el centro máximo de riesgo.

Recabando de este modo en la toma de decisiones finales como la omisión del modelo final o en su inciso factor humano.

Dada la anterior declaración y con la finalidad entender cómo se construirá el modelo inicial de manera más técnica y el respectivo modelo final de manera más estandarizada y comprensible, de esta misma forma se dará mención al factor humano en el modelo inicial ya que hace parte de mismo pero su finalidad estará completa en el modelo final.

4.4.2. Magnitud y base del problema en el modelado.

Antes de proponer una solución hay que conocer de antemano a que nos enfrentamos por tal caso se plantea una magnitud basada en datos de fuentes citadas a continuación con el fin de recabar datos iniciales para desarrollar dicho modelo inicial que tendrá como finalidad construir dicho modelo segmentado en secciones que hablan de manera resumida pero precisa en la mitigación y o reducción de factores de riesgos.

A continuación, se realizará el análisis de los artículos relacionados con la investigación realizada por Bitdefender y NETGEAR entre enero y octubre de 2025, basada en datos de 6,1 millones de hogares inteligentes en Norteamérica, Europa y Australia, revela cifras alarmantes (Bitdefender & NETGEAR, 2025).

En el cual podemos apreciar la cantidad de dispositivos por hogar en el año 2024 y su variación respecto al 2025 de la misma manera con los ataques registrados mostrando incluso al menos dos (2) ataques o intentos a los mismos por dispositivo en el hogar.

Tabla 14. Análisis de contexto

Indicador	Valor 2024	Valor 2025	Variación
Dispositivos por hogar	~10	22	+120%
Ataques IoT diarios por hogar	10	29	+190%
Ataques IoT totales analizados	N/D	13.600 millones	-
Intentos de explotación	N/D	4.600 millones	-

Nota: Tabla elaborada por el autor, esta tabla puede quedar desactualizada de acuerdo nuevas investigaciones y artículos publicados después de esta investigación.

El análisis de **13.600 millones de ataques IoT** revela que los hogares conectados están bajo asedio constante, con una frecuencia de ataque que se ha triplicado en el último año (Bitdefender & NETGEAR, 2025).

Incidentes Críticos de 2025.

El panorama de amenazas de 2025 ha estado marcado por incidentes que demuestran la capacidad destructiva de los dispositivos IoT comprometidos (Bitdefender & NETGEAR, 2025) (Comeau, 2025):

Ataque DDoS récord de 22,2 Tbps: Una botnet alimentada por routers y dispositivos IoT comprometidos logró la mayor inundación de tráfico jamás registrada (Bitdefender & NETGEAR, 2025).

BadBox: Botnet que infectó más de **un millón de dispositivos Android** antes incluso de salir de fábrica, con firmware malicioso preinstalado en más de 20 dispositivos de streaming (Bitdefender & NETGEAR, 2025).

Vulnerabilidades críticas documentadas:

- a. **CVE-2025-65553:** Sistema de seguridad D3D Wi-Fi ZX-G12 vulnerable a bloqueo por RF en el canal de 433 MHz.
- b. **CVE-2025-8627:** Enchufe inteligente TP-Link KP303 con ejecución de comandos sin autenticar (CVSS 8.8).
- c. **CVE-2025-50777:** Cámara AZIOT con almacenamiento en texto plano de credenciales WiFi.
- d. **CVE-2025-12599:** Múltiples dispositivos BLU-IC con secretos criptográficos idénticos.

Violaciones de privacidad: En Italia, atacantes explotaron cámaras IP inseguras para transmitir imágenes de hogares y probadores de tiendas a través de Telegram (Comeau, 2025).

Nuevas botnets: Emergieron PUMABOT y AISURU, que esclavizan cientos de miles de routers y dispositivos Linux(Comeau, 2025).

PUMABOT: Investigadores de Darktrace han descubierto una botnet de Linux personalizada escrita en Go que ejecuta ataques contra dispositivos Linux integrados de IoT a los que han denominado "PumaBot".

En lugar de llevar a cabo un escaneo del espacio de direcciones de Internet, el malware puede obtener de un servidor de comando y control (C2) una lista de objetivos y después facilitar la adquisición de credenciales SSH mediante un ataque de fuerza bruta.

Cuando el malware accede a un objetivo, se le provee de comandos remotos y, además, establece persistencia a través de los archivos de servicio del sistema.

Esta publicación en el blog describe un análisis técnico de las funcionalidades clave de "PumaBot" así como un análisis de los binarios asociados a la campaña.

Principales vectores de ataque

Tabla 15. vectores de ataque.

Vector de Ataque	Porcentaje	Descripción
Escaneo automatizado	>93%	Búsqueda masiva de dispositivos con credenciales por defecto
Firmware desactualizado	25%+	Dispositivos de streaming y TVs con kernels Linux sin parchear
Credenciales débiles	90%	Contraseñas por defecto y falta de autenticación multifactor
Cifrado ausente	N/D	Transmisión de datos en texto plano y credenciales sin cifrar

Nota: Tabla elaborada por el autor, "tómese en contexto actual" esta tabla puede quedar desactualizada de acuerdo nuevas investigaciones y artículos publicados después de esta investigación.

4.4.3. Análisis de vulnerabilidades por capa.

Vulnerabilidades de hardware.

Los dispositivos IoT domésticos, diseñados con restricciones de costo y consumo energético, presentan vulnerabilidades hardware críticas:

- **Interfases hardware de depuración:** puertos UART, JTAG y SPI pública y físicamente expuestas permiten extraer el firmware y credenciales de la terminal de sistema o aplicaciones de usuarios. La metodología de

evaluación de las vulnerabilidades publicada en el 2025 pone de manifiesto las protecciones inadecuadas en las interfases hardware de debugs de 7.8 CVSS.

- **Claves criptográficas compartidas:** Múltiples dispositivos de un mismo fabricante utilizan secretos criptográficos idénticos, como se documentó en CVE-2025-12599 para dispositivos BLU-IC.
- **Ataques de canal lateral:** Dispositivos en entornos accesibles son vulnerables a manipulación física, extracción de datos e inyección de código malicioso.
- **Bootloaders estáticos:** Contraseñas de bootloader fijas que permiten compromiso total del dispositivo (CVSS 9.1).

4.4.4. Vulnerabilidades de Software.

El software de los dispositivos IoT presenta múltiples vectores de explotación (véase en la tabla 2 matriz de riesgos):

- **Firmware sin firmar:** Actualizaciones descargadas por canales no seguros (HTTP) sin verificación de integridad.
- **Ausencia de cifrado:** Transmisión de credenciales en texto plano durante la configuración inicial (CVSS 7.5).
- **Contraseñas por defecto:** Vulnerabilidad sistemática documentada en numerosos dispositivos.
- **Atributos ocultos:** Vulnerabilidad inherente a plataformas de automatización IoT donde atributos configurables vía API no son gestionables por el usuario.

- Desbordamientos de búfer: Como el documentado en dispositivos Realtek AmebaD.

4.4.5. Factor humano.

El eslabón más débil en la cadena de seguridad IoT es el usuario final:

Falta de concienciación: Estudio de 2025 revela que los usuarios desconocen los riesgos asociados a sus dispositivos inteligentes.

Contraseñas reutilizadas y débiles: La mayoría de los usuarios no cambia las credenciales por defecto.

Configuración incorrecta: Dispositivos dejados con configuraciones de fábrica que exponen información sensible.

Falta de actualizaciones: Los usuarios no aplican parches de seguridad, ya sea por desconocimiento o por la complejidad del proceso.

4.5. Modelo inicial propuesto: Arquitectura de 5 capas.

El modelo propuesto se estructura en cinco capas de defensa que abordan las vulnerabilidades identificadas en el objetivo 2 para ser abordadas desde una perspectiva integral.

Capa 1: Seguridad de hardware.

Selección de Dispositivos Seguros Recomendaciones para personal prestador del servicio y consumidores, es el etiquetado de seguridad Adoptado por el marco de

etiquetado de ciberseguridad ISO/IEC 27404:2025, que define requisitos para programas de etiquetado de productos IoT de consumo (International Organization for Standardization [ISO], 2023). Este estándar cubre:

- Riesgos y amenazas asociados a productos IoT.
- Roles y responsabilidades de los stakeholders.
- Evaluación de conformidad.
- Emisión y mantenimiento de etiquetas.

Arquitectura de referencia NIST: Implementar la arquitectura de integración de hogar inteligente propuesta por NIST CSWP 34, que establece un modelo de alto nivel para abordar riesgos (National Institute of Standards and Technology [NIST], 2025).

- **Criterios de selección mínimos:**
 - Puertos de depuración deshabilitados en producto final.
 - Claves criptográficas únicas por dispositivo.
 - Módulo de seguridad hardware (HSM) o Trusted Platform Module (TPM).
 - Arranque seguro (Secure Boot) con verificación de firma.

Protección contra manipulación física.

Diseño resistente a manipulación: Carcasas que dificultan el acceso a interfaces internas.

Detección de apertura: Sensores que alertan sobre intentos de manipulación física al dispositivo activando de este modo una alarma silenciosa o el mecanismo de borrado a continuación.

Borrado seguro: Mecanismos que eliminan datos sensibles ante detección de manipulación y o intromisión.

Capa 2: Seguridad de software y firmware.

Capa 2.1 Gestión de identidades y credenciales:

Contraseñas únicas por dispositivo: Eliminación de credenciales por defecto (Constantinescu, 2025).

Autenticación multifactor (MFA/2FA): Obligatoria para acceso remoto.

Gestores de contraseñas: Recomendación de uso para evitar fatiga de contraseñas (Constantinescu, 2025).

Certificados digitales: Autenticación basada en certificados para dispositivos críticos.

Capa 2.2 Cifrado y protección de datos:

Cifrado en tránsito: TLS 1.3 obligatorio para todas las comunicaciones.

Cifrado en reposo: Almacenamiento cifrado de credenciales y datos sensibles.

Protocolos seguros: Deshabilitación de protocolos obsoletos (SSL, TLS 1.0/1.1).

Capa 2.3 Actualizaciones seguras:

Canal seguro: Descarga de firmware exclusivamente por HTTPS.

Firma digital: Verificación de integridad y autenticidad del firmware.

Actualizaciones automáticas: Activadas por defecto con notificación al usuario.

Mecanismo anti-rollback: Prevención de instalación de versiones antiguas vulnerables.

Ventana de parcheo reducida: Los atacantes explotan vulnerabilidades de kernel Linux rápidamente; los fabricantes deben publicar parches en plazo.

Capa 2.4 Desarrollo seguro:

OWASP Top 10 IoT: Adopción del estándar para evaluación de seguridad.

Pruebas de penetración: Realizadas antes del lanzamiento y periódicamente.

Análisis de firmware: Herramientas como IoT Sleuth para detección de vulnerabilidades a nivel binario.

Cadena de suministro segura: Verificación de componentes de código abierto y desarrolladores externos.

Capa 3: Seguridad de Red.

La arquitectura plana tradicional (todos los dispositivos en la misma red) es particularmente susceptible a acceso no autorizado y movimiento lateral.

Capa 3.1 Arquitectura por segmentación:

Contención de ataques: Un dispositivo IoT comprometido no puede acceder a la red principal. Aislamiento de dispositivos críticos, visibilidad y control gradual del tráfico.

Capa 3.2 Configuración segura del router:

El router es la "puerta de entrada digital" al hogar y debe ser asegurado como prioridad (Constantinescu, 2025).

- **WPA3/WPA2:** Cifrado de red robusto con contraseña segura
- **SSID no identificable:** Evitar nombres que revelen información personal
- **WPS desactivado:** Wi-Fi Protected Setup es un vector de ataque conocido
- **Firewall activo:** Filtrado de tráfico entrante no solicitado
- **Actualizaciones automáticas:** Firmware del router actualizado regularmente
- **Cambio de credenciales:** Contraseña de administración del router única y robusta

Capa 3.3 Monitorización de Red:

Sistema de Detección de Intrusiones (IDS): Implementación basada en IA y ML para identificación de amenazas en tiempo real.

Análisis de anomalías: Detección de patrones de tráfico inusuales.

Alertas configurables: Notificaciones ante actividad sospechosa.

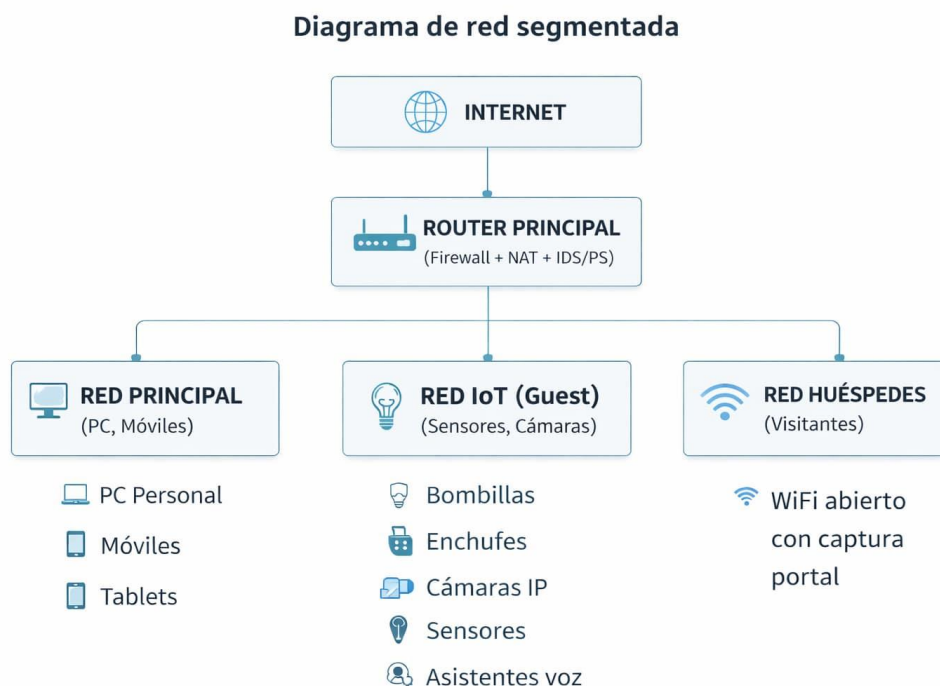
Arquitectura recomendada.

La arquitectura recomendada para la protección de los dispositivos y teniendo en cuenta una posible intromisión a la red por parte de un atacante es la siguiente: Dividir la red principal en subredes más pequeñas con el fin de separar dispositivos los cuales se agruparán de la siguiente manera.

Dispositivos IoT, separar los dispositivos IoT del resto de aparatos como teléfonos, tablets y computadoras personales es un paso a la mitigación de las amenazas que se puedan presentar, a su vez dividir una vez más la red para dispositivos de

terceros como los huéspedes como se muestra a continuación en el siguiente diagrama.

Figura 24. Diagrama de red



Fuente: Autor.

Capa 4: Factor humano y concienciación

La investigación del artículo “An investigation of security risks regarding the user awareness of IoT devices in the home” ha demostrado que la falta de concienciación es un factor crítico en la seguridad del IoT doméstico. Las estrategias propuestas incluyen:

Programa de formación básica:

- 1. Inventario de dispositivos:** Mantener un registro actualizado de todos los dispositivos IoT conectados.
- 2. Cambio inmediato de credenciales:** Modificar todas las contraseñas por defecto durante la configuración inicial.
- 3. Actualizaciones regulares:** Verificar y aplicar parches de seguridad mensualmente.
- 4. Principio de mínimo privilegio:** Deshabilitar funcionalidades no utilizadas (micrófonos, cámaras, acceso remoto).

Canales de formación:

Aplicaciones móviles: Guías interactivas de seguridad integradas en las apps de los fabricantes.

Asistentes de voz: Alertas de seguridad y recomendaciones proactivas.

Materiales visuales: Infografías y vídeos tutoriales accesibles.

Capa 4.1 Diseño centrado en el usuario:

Los marcos de seguridad centrados en el factor humano para hogares inteligentes propuestas son:

- **Interfaces intuitivas:** Configuraciones de seguridad claras y accesibles.
- **Notificaciones contextuales:** Alertas que explican el riesgo en términos comprensibles.
- **Automatización segura:** Configuraciones predeterminadas que priorizan la seguridad.

- **Feedback visual:** Indicadores de estado de seguridad en dispositivos y apps.

Capa 4.2 Gestión del ciclo de vida:

- **Fin de vida útil:** Reemplazo de dispositivos que ya no reciben actualizaciones de seguridad.
- **Desactivación segura:** Procedimientos para eliminar datos y desvincular dispositivos antes de desecharlos.
- **Evaluación periódica:** Revisión trimestral del ecosistema IoT doméstico.

Capa 5: Gestión del ciclo de vida

Estándares y Certificaciones

- **NIST Cybersecurity Framework (CSF 2.0)**, (National Institute of Standards and Technology [NIST], 2025).
- **NIST Privacy Framework (PF 1.0)**, (National Institute of Standards and Technology [NIST], 2025).
- **NIST IR 8425:** Perfil del núcleo de IoT para productos IoT de consumo, (National Institute of Standards and Technology [NIST], 2025).
- **ISO/IEC 27404:2025:** Etiquetado de ciberseguridad para IoT de consumo, (International Organization for Standardization [ISO], 2023).

Capa 5.1 Evaluación de riesgos:

Metodología cualitativa de evaluación de riesgos conforme a ISO/IEC 27005, (SGS Academy, 2025).

Tabla 16. Matriz de Factores de riesgo en dispositivos.

Activo Critico	Amenazas	Probabilidad	Impacto	Riesgo
Router/Gateway	Compromiso, DDoS	Alta	Crítico	Alto
Cámaras IP	Fuga de privacidad	Alta	Alto	Alto
Asistentes de voz	Escucha, fuga datos	Media	Alto	Medio-Alto
Sensores	Manipulación, DDoS	Media	Medio	Medio
Electrodomésticos	Manipulación, DDoS	Media	Medio	Medio
Electrodomésticos	Secuestro, botnet	Media	Medio	Medio

Nota: Tabla elaborada por el autor.

Capa 5.2 Auditorías y cumplimiento:

- **Auditorías periódicas:** Evaluación de seguridad del ecosistema IoT al menos anualmente.
- **Pruebas de penetración:** Simulación de ataques para identificar vulnerabilidades.
- **Cumplimiento normativo:** Adaptación a regulaciones locales e internacionales.

4.6. Estrategias de implementación.

Para implementadores prestadores de servicio y Profesionales: Los prestadores de servicios IoT están en primera línea para desplegar y asegurar estos ecosistemas complejos brindando un servicio profesional y seguro para sus clientes de forma segura (CE Pro, 2025).

Pasos por seguir checklist:

- **Segmentación de red:** Configuración de VLANs para aislamiento de dispositivos IoT.
- **Monitorización:** Implementación de soluciones IDS/IPS.
- **Inventario:** Documentación detallada de todos los dispositivos instalados.
- **Mantenimiento:** Programación de actualizaciones y auditorías periódicas.

Para usuarios finales, guía práctica de 10 pasos: se crea una lista previa para los usuarios finales con 10 pasos a seguir y así mantener la seguridad del hogar (CE Pro, 2025).

1. **Inventario:** Lista todos los dispositivos conectados a Internet en tu hogar.
2. **Cambia contraseñas:** Todas las credenciales por defecto deben ser modificadas.
3. **Actualiza firmware:** Verifica y aplica todas las actualizaciones disponibles.
4. **Seguridad WiFi:** Usa WPA3/WPA2 con contraseña robusta.
5. **Red de invitados:** Conecta todos los dispositivos IoT a la red de invitados.
6. **Desactiva WPS:** Elimina este vector de ataque conocido.
7. **Deshabilita funciones no usadas:** Apaga micrófonos, cámaras y acceso remoto innecesarios.
8. **Monitoriza:** Revisa regularmente qué dispositivos están activos en tu red.

9. **Actualiza regularmente:** Establece un recordatorio mensual para verificar actualizaciones.
10. **Reemplaza dispositivos obsoletos:** Sustituye aquellos que ya no reciben soporte.

El objetivo de la sección anterior se construyó orientado la evaluación del modelo inicial de ciberseguridad, para ello se plantearon 10 preguntas con el fin de seleccionar dispositivos que cumplan con los parámetros de seguridad.

- ¿El fabricante publica informes de seguridad y vulnerabilidades?
- ¿El dispositivo recibe actualizaciones de firmware regulares?
- ¿Las actualizaciones se descargan por HTTPS con verificación de firma?
- ¿Se pueden cambiar todas las credenciales por defecto?
- ¿Ofrece autenticación multifactor?
- ¿Los datos se transmiten cifrados (TLS)?
- ¿Se pueden deshabilitar funciones no utilizadas (micrófono, cámara)?
- ¿El dispositivo tiene etiquetado de seguridad (ISO/IEC 27404)?
- ¿El fabricante tiene un programa de divulgación de vulnerabilidades?
- ¿El dispositivo permite actualizaciones automáticas?

Presentación de matriz de riesgo a nivel software del modelo inicial como complemento de la matriz de riesgos en dispositivos.

Tabla 17. Matriz de riesgo a nivel software de dispositivos.

Vulnerabilidad	Capa	CVSS	Mitigación	Prioridad
Credenciales por defecto	SW	9.8	Cambio inmediato, MFA	 Crítica
Firmware sin firmar	SW	8.8	Firmas digitales, HTTPS	 Alta
Datos en texto plano	SW	7.5	TLS 1.3, cifrado	 Alta
Interfaces depuración	HW	7.8	Deshabilitar en producción	 Alta
Bootloader estático	HW	9.1	Secure Boot, contraseña única	 Crítica
Falta de segmentación	Red	8.5	VLANs, red de invitados	 Alta
Usuario no concienciado	Humano	7.0	Formación, interfaces intuitivas	 Media

Nota: Tabla elaborada por el autor. Matriz de complemento a la matriz Factores de riesgo en dispositivos.

4.7. Construcción de un entorno de simulación para la fase de pruebas y test de funcionalidad.

La fase de pruebas y test de la funcionalidad corresponde a una de las actividades propuestas en los objetivos Dos (2) y tres (3), es una de las Fases más relevantes en la actividad de desarrollo e implementación de un modelo de seguridad para entornos de IoT.

Dado que permite verificar de forma objetiva la capacidad que tiene el sistema para poder proteger a los dispositivos, detectar vulnerabilidades que no se han

considerado en el modelo inicial y reaccionar ante incidentes de ciberseguridad que surjan en esta fase.

Esta actividad tiene por objetivo verificar que los mecanismos de autenticación, de autorización, de cifrado de datos, de registro y de respuesta implementados durante el proceso de diseño del modelo funcionen correctamente frente a una puesta en práctica del modelo, como que la información esté en situación de alta disponibilidad, integridad y confidencialidad (ISO/IEC, 2022a).

En el entorno de las Smart Homes, donde una serie de dispositivos del Internet de las Cosas (IoT) están interconectados de forma continua a partir de redes domésticas, el proceso de pruebas tiene un rol más importante si cabe por la heterogeneidad de dispositivos y diversidad de protocolos de comunicación presentes, lo que pone de manifiesto que la norma ISO/IEC 27400: 2022.

Esta norma está centrada, sobre todo, en la seguridad y privacidad de los sistemas IoT, exige que la evaluación de un sistema tenga en cuenta tanto los aspectos técnicos como los riesgos relacionados con el funcionamiento del ecosistema, lo que incluye la identificación de amenazas, la protección de los datos personales o la resiliencia frente a ciberataques (ISO/IEC, 2022b).

En esta etapa, el modelo de seguridad desarrollado para tal fin deberá someterse a diversas validaciones del modelo de seguridad apoyándose en pruebas que permitan evaluar el comportamiento del modelo de seguridad en situaciones de uso normal y otras en condiciones adversas.

Se destacan las pruebas de autenticación de usuarios, dispositivos y aplicaciones o servicios; la validación de los mecanismos de control de acceso, entre ellos la

autorización tras la autenticación; la verificación del cifrado de las comunicaciones; la detección de intentos de acceso no autorizado; la calidad de la detección del modelo de seguridad para generar alertas en el caso de un evento sospechoso.

Las actividades explicadas son de gran utilidad para verificar si el modelo se ajusta a los requisitos de seguridad definidos en las etapas de análisis y diseño y también permite detectar mejoras que se pueden realizar antes o en la implementación del modelo de seguridad (ISO/IEC, 2022a).

De forma complementaria a las normas expuestas anteriormente, la familia de normas ISO/IEC 27001:2022 da lugar a la gestión de la seguridad de la información a partir de un enfoque basado en riesgos.

Si bien esta norma se refiere a los Sistemas de Gestión de Seguridad de la Información (SGSI), sus controles son el modelo de referencia para comprobar que nuestro modelo implemente maneras apropiadas para la gestión de activos, control de accesos, supervisión permanente o respuesta a incidentes de seguridad.

Por tanto, las pruebas funcionales deben verificar que cada uno de estos controles respete la manera en la que los controles se están ejecutando y al mismo tiempo contribuye a hacer que la superficie de ataque del entorno IoT disminuya.

De forma complementaria, el documento que hace referencia a la norma ISO/IEC 27002:2022 acompaña el proceso de validación mostrando buenas prácticas para la implantación de los controles de seguridad. Al llevar a cabo la validación, es también correcto incorporar las comprobaciones referidas a que los mecanismos utilizados en el modelo implementan principios de la autenticación robusta.

La gestión segura de las credenciales, la protección criptográfica, el login, la monitorización continua y la gestión de la vulnerabilidad. Dichas comprobaciones permiten no sólo validar el correcto funcionamiento del sistema, sino también la madurez de los controles implementados (ISO/IEC, 2022c).

4.7.1. Construcción de un entorno simulado para validar el modelo

Construcción inicial:

Para esta parte de la investigación se simulará un entorno controlado de una Smart home con su ecosistema de dispositivos conectados, para llevar a cabo el siguiente entorno controlado se utilizará el software Cisco Packet Tracer con el fin de simular un entorno base donde estos parámetros propuestos en el modelo inicial de cinco (5) capas planteado en la actividad número uno (1) del tercer objetivo en el cual se demostrará su desempeño y aplicación con el fin de corregir, estandarizar y optimizar dicho modelo para su versión final.

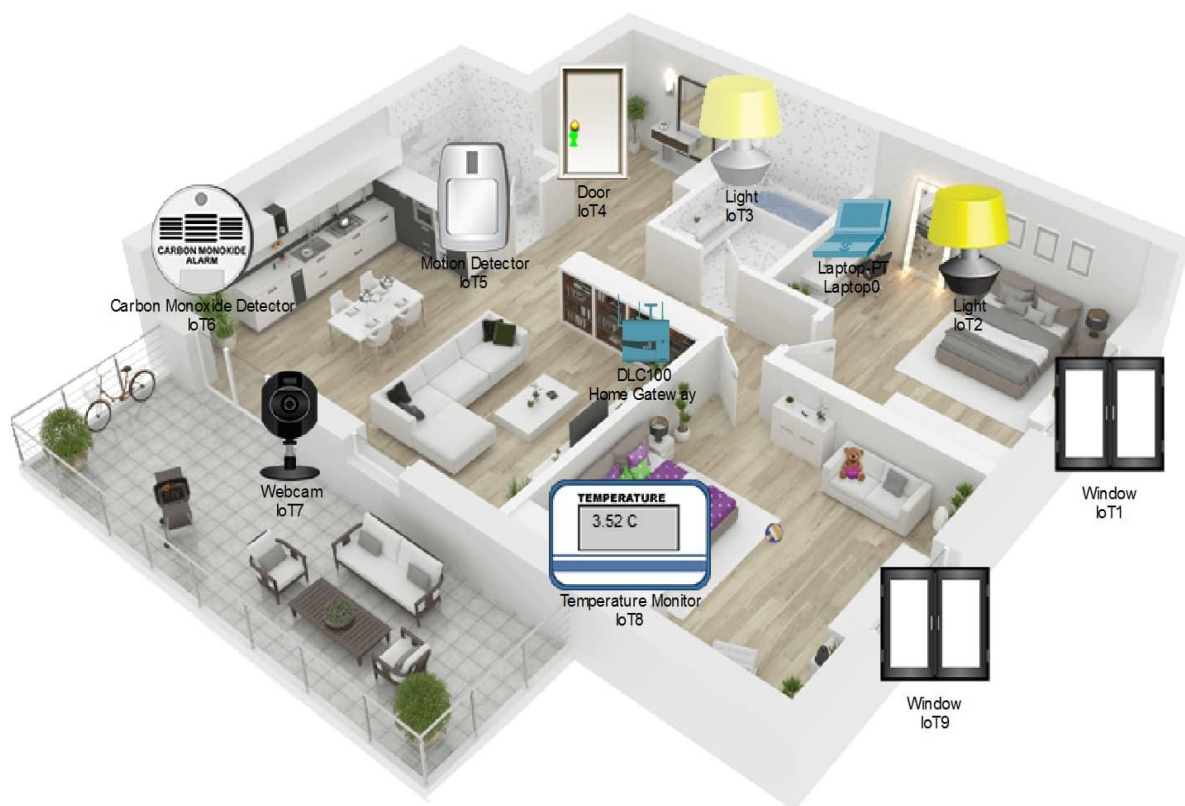
La validación del modelo empieza por crear una red de un hogar inteligente con los dispositivos planteados en el anexo de la matriz de riesgo de dispositivos comunes propuestos.

La red iniciara con dichos dispositivos en conjunto sin categorizar por jerarquías también se parte por simular un entorno de riesgo en el cual la red es conjunta para cada dispositivo conectado simulando uno de los riesgos más comunes que se han demostrado en esta investigación (Bitdefender, 2025).

Topología de la simulación:

La imagen muestra el plano 3D de un apartamento moderno donde se han instalado dispositivos simulados de Internet of Things (IoT) en Packet Tracer. Todos esos dispositivos están conectados a un Home Gateway (DLG100), que hace las veces de centro de la comunicación y control de la red Smart Home.

Figura 25. Topografía.



Fuente: Autor, Plano de fondo de vipreformas.

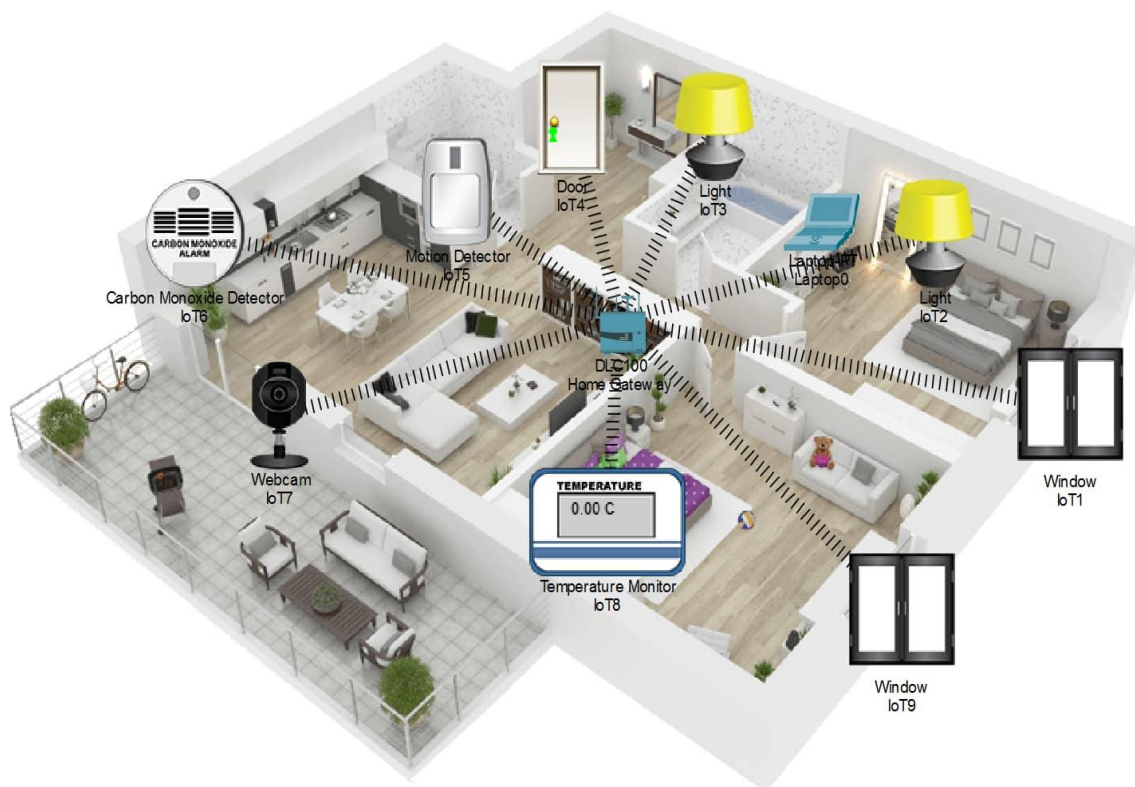
Con la topología ya estructurada el siguiente paso es configurara el dispositivo primario de control que viene siendo el DLC100 Home Gateway quien será el cerebro encargado de controlar los dispositivos se conecten al mismo, Iniciamos asignando un protocolo de seguridad y una contraseña básico así creando un dispositivo con parámetros de fabrica esenciales para la demostración simulada.

A continuación, se mostrará la configuración por defecto: contraseña por defecto de fabrica “admin”, nombre de la red “HomeGateway” el DHCP se dejará por defecto de la misma manera que los pasos anteriores sin la necesidad de configurar ya que cisco cuenta con directivas preestablecidas de IP asignación y reconocimiento de esta para los dispositivos enlazados.

Configurada la unidad central de mando el paso siguiente es enlazar cada dispositivo IoT con la unidad con el fin de establecer la comunicación con el home Gateway, para esto una vez ordenado y detallado cada dispositivo con un valor numérico con el fin de localizar a los mismos.

A continuación, se procederá a ingresar el nombre de la red acompañado de su respectiva contraseña por último asignando la opción IoT server a “home Gateway” aclarado de antemano los dispositivos también tendrán su configuración estándar diferente de los anteriores parámetros requeridos.

Figura 26. Conexión establecida.



Fuente: Autor, Plano de fondo de vipreformas.

Configuración del dispositivo de control:

Para el puesto de control se usará un equipo portátil, el cual tendrá la función de controlar y monitorear la red de dispositivos que se encuentran enlazados a la misma, el primer paso antes de monitorear y controlar la red es enlazar el equipo con el Home gateway mediante la misma red wifi, este paso respecto a los anteriores requiere que el computador cuente con módulo de conexión inalámbrico para ello hay que cambiar el módulo que esta por defecto ya que en la herramienta cisco el equipo portátil cuenta con un módulo distinto al esperado.

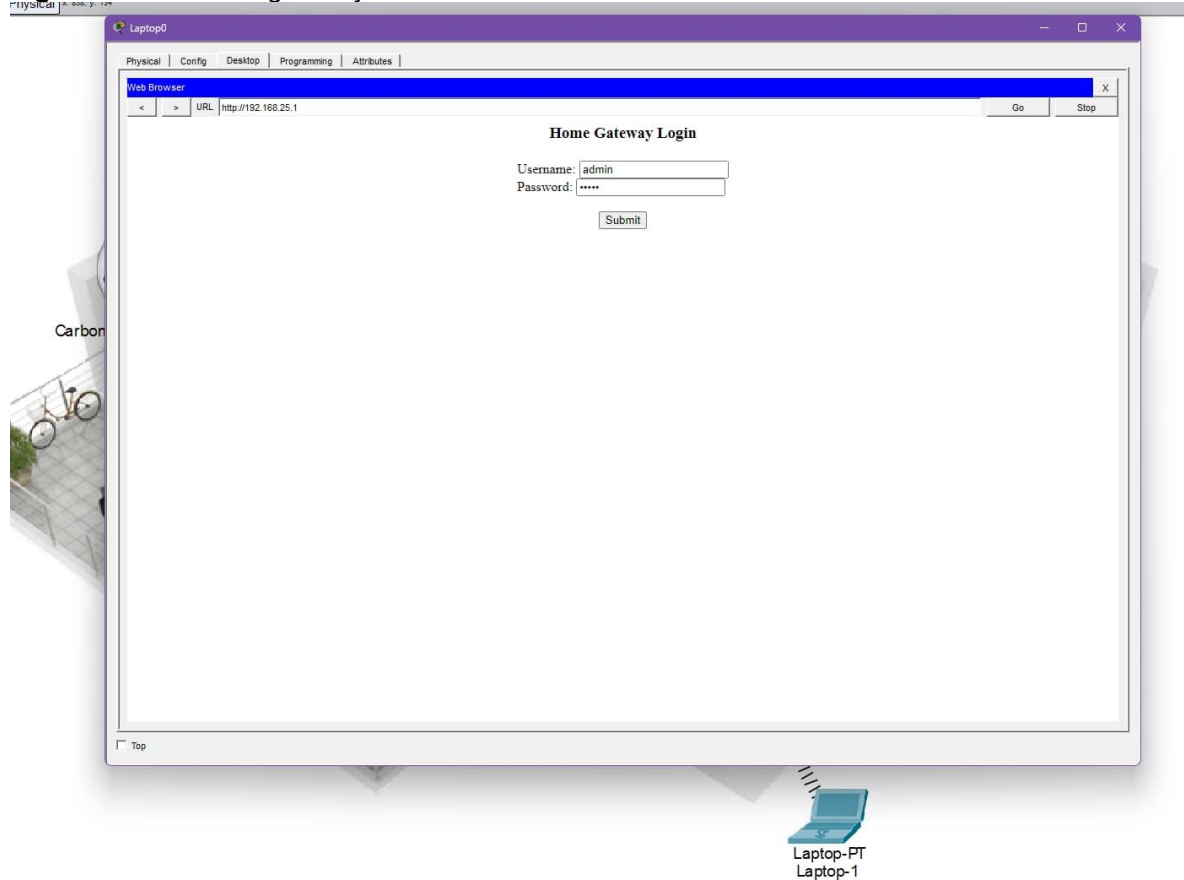
Figura 27. Conexión del computador y configuración.



Fuente: Autor, Plano de fondo de vipreformas.

Con la conexión establecida entre el computador y el gateway el siguiente paso a seguir para apreciar la red interna consiste en iniciar la interfaz del computador entrar al navegador introducir la dirección IP de gateway y lo siguiente que saldrá en pantalla es el inicio de sesión del dispositivo el cual al estar por defecto su usuario y contraseña será la palabra “admin” para ambos casos.

Figura 28. Acceso al gateway.



Fuente: Autor.

Iniciada la sección mediante el computador podemos apreciar los distintos dispositivos conectados a la red interna ordenado de acuerdo con el número que se les fue asignado al principio de la topografía inicial, desde este panel podremos apreciar y controlar los distintos dispositivos que conforman la smart home.

Con esto último la construcción inicial del simulador esta completa ahora el siguiente paso de la demostración a seguir es:

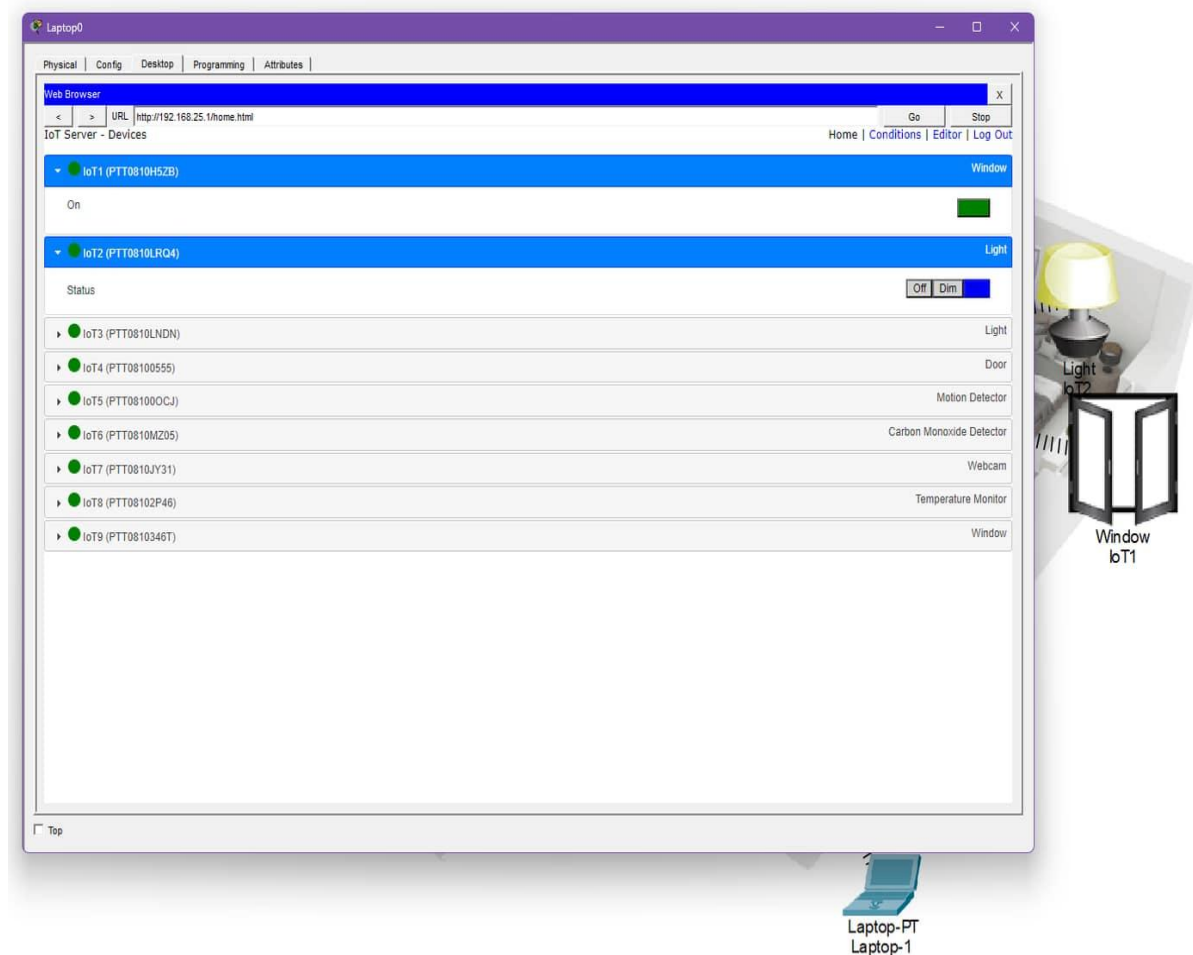
programar y ejecutar las vulnerabilidades mediante una serie de ataques que demuestren los riesgos asociados a los dispositivos presentes dando paso al anexo matriz de riesgo en los dispositivos desarrollada en el objetivo 1 de este proyecto a su vez también se contara con el anexo de la matriz de vulnerabilidad en los dispositivos desarrollado en el objetivo 2 y 3 de este proyecto.

Adicionalmente, las recomendaciones que son publicadas por el National Institute of Standards and Technology (NIST) a su vez contando también con las recomendaciones de la guía NISTIR 8259 se recoge un conjunto de capacidades fundamentales de la ciberseguridad que podrían adaptarse a los dispositivos IoT.

Como son la identificación del dispositivo, la configuración segura, la protección de los datos, la actualización del software y la auditoría (entendida como el registro de los eventos de seguridad).

Por ello, al propio proceso de pruebas le corresponde validar que el modelo implementado sea capaz de alcanzar esas capacidades obligatorias e imprescindibles de manera que se garantice que los dispositivos puedan mantenerse protegidos en el ciclo de vida de este (NIST, 2020).

Figura 29. Dispositivos en la red.



Fuente: Autor.

4.8. Fase de demostración de vulnerabilidades.

La fase de demostración de vulnerabilidades y ataque tiene como finalidad la validación de la capacidad del modelo de seguridad para la detección, mitigación y respuesta ante amenazas reales existentes en dispositivos IoT.

Esta fase, a diferencia de las pruebas funcionales, intenta reproducir escenarios de ataque, ya documentados en las normativas de estándares internacionales,

ELABORADO POR:
Docencia

REVISADO POR:
Sistema Integrado de Gestión

APROBADO POR: Líder del Sistema Integrado de Gestión
FECHA APROBACIÓN: Octubre de 2023

artículos y textos literatura científica anteriormente citados a lo largo de este proyecto, de este modo permitiendo comprobar que los mecanismos de protección implementados son eficaces.

En el caso de las viviendas inteligentes, en donde cámaras, asistentes virtuales, sensores y dispositivos de automatismo van intercambiando continuamente información, las vulnerabilidades respecto de credenciales por defecto.

Comunicaciones sin cifrar y actualizaciones inseguras de firmware suponen algunos de los vectores de ataque más usuales y con un mayor impacto sobre la seguridad del ecosistema IoT (ISO/IEC, 2022; ETSI, 2020).

Demostración de vulnerabilidades mediante credenciales por defecto.

Como uno de los ataques más típicos podemos encontrar el uso de credenciales predeterminadas o muy débiles (combinaciones como admin/admin, admin/password o directamente las credenciales codificadas por el fabricante) que ha sido responsable de algunos de los principales incidentes con dispositivos IoT durante la última década.

Uno de los ejemplos más representativos es el caso del malware conocido como Mirai (detectado en 2016), el cual comprometía, entre otros dispositivos, cámaras IP, grabadores digitales (DVR) y routers domésticos a través de un recopilado de credenciales predeterminadas que venían almacenadas en el propio código malicioso.

Una vez comprometido un dispositivo, este era incorporado a una botnet (red de bots) que permitía realizar ataques distribuidos de denegación de servicio (DDoS), como la botnet utilizada en el ataque contra el proveedor Dyn.

Un ataque que afectó a múltiples servicios de Internet de carácter mundial. Diferentes estudios posteriores continúan la senda de Mirai para verificar cómo las credenciales por defecto continúan siendo uno de los principales componentes de la amenaza a los dispositivos IoT.

En este contexto, la prueba del modelo de seguridad consiste en poner en marcha dispositivos inicialmente configurados con credenciales de acceso predeterminadas y verificar que el sistema reconozca dicha condición como un riesgo asociado a la seguridad.

A continuación, se comprueba si el modelo contiene las políticas necesarias para indicar al usuario final la importancia del cambio de credenciales (contraseña) de acceso predeterminadas por defecto en los dispositivos.

Prevenir accesos no permitidos y registrar los intentos de autenticación abusivos del sistema. Esta validación, por tanto, da fe de la eficacia del modelo para afrontar el problema relacionado con el vector de ataque más utilizado en entornos IoT.

La relevancia de esta validación encuentra su base en la norma ETSI EN 303 645, que señala expresamente que, dentro de los dispositivos de consumo IoT, no se deberían establecer contraseñas universales predeterminadas.

Es recomendando que cada dispositivo debiera disponer de credenciales de acceso únicas o requerir que el usuario establezca credenciales seguras a través del proceso de configuración inicial (ETSI, 2024).

Complementariamente, la norma ISO/IEC 27400 recomienda establecer mecanismos de autenticación robustos y gestionar la identidad para reducir el riesgo de accesos no autorizados a dispositivos por parte de un tercero que ya cuente con acceso a la red en la cual ya se encuentran dichos dispositivos (Fagan et al., 2020).

Demostración de vulnerabilidades mediante transmisión de datos sin cifrar.

Un segundo escenario crítico es que, al comunicarse sin un mecanismo de cifrado, una buena cantidad de sensores IoT transmitirían información sobre las condiciones ambientales, información de presencia, estados de los actuadores o incluso credenciales utilizando algún protocolo sin cifrado (ISO, 2022);

de este modo, sería posible que un posible atacante conectado a la misma red pudiera leer el tráfico utilizando alguna técnica de análisis de paquetes (packet sniffing).

La literatura científica ha identificado la comunicación sin cifrar como una de las vulnerabilidades más frecuentes en dispositivos IoT asequibles, dado que este comportamiento se manifiesta especialmente entre dispositivos que utilizan protocolos HTTP, Telnet o comunicaciones TCP sin TLS (Fagan et al., 2020).

Con estos protocolos, sería posible que un atacante pudiera capturar, alterar o reutilizar la información para comprometer otros elementos del sistema. Investigaciones de seguridad en el ámbito de hogar inteligente han mostrado que la comunicación sin cifrar pone en peligro la seguridad y la privacidad de sus usuarios, facilitando ataques de espionaje, robo de información o manipulación de sensores inteligentes críticos.

En el transcurso de la demostración del modelo de seguridad, la vulnerabilidad se puede explotar consiguiendo que uno o más de los sensores manden mensajes de datos no cifrados de forma controlada en un entorno de pruebas.

A continuación, utilizando herramientas de análisis de tráfico, se comprueba que el modelo genera alertas cuando se detectan comunicaciones no seguras, es decir, cuando se detectan protocolos no cifrados o cuando hay intercambio de información sensible en texto plano.

El resultado deseado consiste en demostrar que el sistema es capaz de distinguir correctamente las comunicaciones protegidas por TLS de las que representan un riesgo para la privacidad e integridad de la información.

Estas pruebas corresponden a las recomendaciones de ISO/IEC 27400, puesto que esta norma establecía que cualquier información sensible que se envíe desde el dispositivo IoT debería ser cifrada.

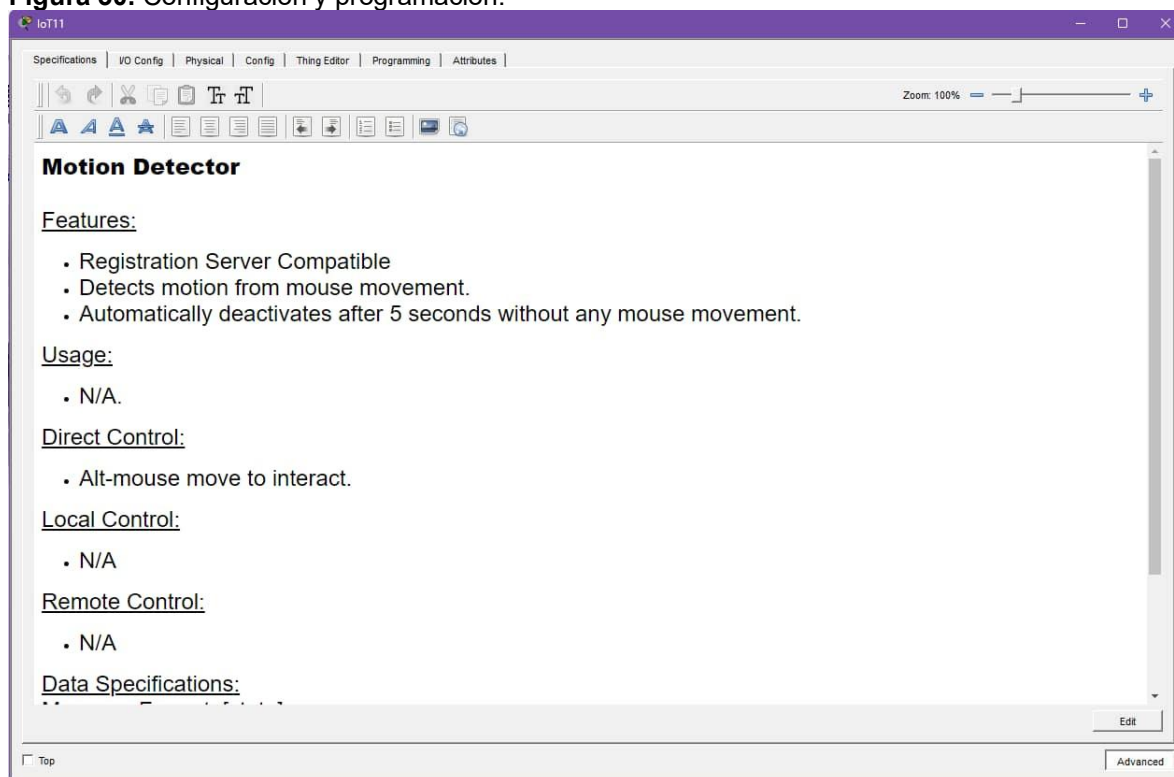
De la misma forma, la recomendación de NIST SP 800-213 aconseja que los dispositivos IoT doten de capacidades de protección de datos del almacenamiento y de la información en tránsito para minimizar la exposición frente a ataques de interceptación.

Construcción del escenario.

Para la construcción de este escenario tomaremos el sensor de movimiento “Motion Detector IoT5” el código con el que el dispositivo cuenta solo tendrá una modificación adicional al mismo ya que lo que queremos buscar es que el dispositivo no solo detecte el movimiento e indique que existe.

Sino también que la simulación actúe como lo haría un dispositivo IoT moderno el cual indica con un mensaje que sea transmitido al usuario que hay o no movimiento mediante un mensaje enviado desde el propio dispositivo.

Figura 30. Configuración y programación.



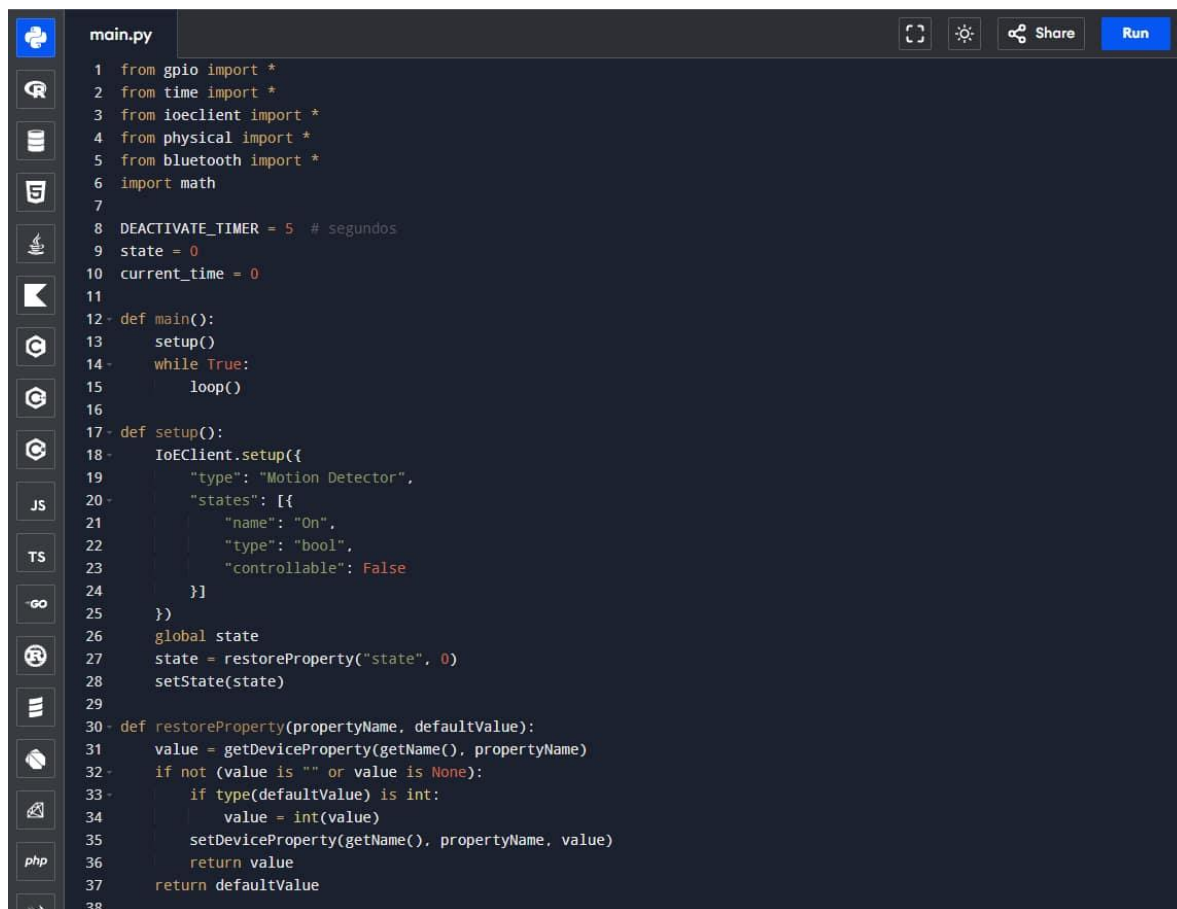
Fuente: Autor.

Seleccionaremos el dispositivo una vez dentro del panel de control del dispositivo es necesario activar las opciones avanzadas para así tener acceso al módulo de programación seleccionamos el lenguaje de programación que utilizaremos los cuales son JavaScript o Python que son los dos lenguajes que ofrece cisco packet tracer para la simulación.

Para mayor comodidad usaremos el lenguaje Python y mediante el uso de comentarios se resaltarán las partes editadas del código y el también del código adicionado.

Programación:

Figura 31. Programación 1.



```

main.py
1 from gpio import *
2 from time import *
3 from ioeclient import *
4 from physical import *
5 from bluetooth import *
6 import math
7
8 DEACTIVATE_TIMER = 5 # segundos
9 state = 0
10 current_time = 0
11
12 def main():
13     setup()
14     while True:
15         loop()
16
17 def setup():
18     IoEClient.setup({
19         "type": "Motion Detector",
20         "states": [{
21             "name": "On",
22             "type": "bool",
23             "controllable": False
24         }]
25 })
26 global state
27 state = restoreProperty("state", 0)
28 setState(state)
29
30 def restoreProperty(propertyName, defaultValue):
31     value = getDeviceProperty(getName(), propertyName)
32     if not (value is "" or value is None):
33         if type(defaultValue) is int:
34             value = int(value)
35         setDeviceProperty(getName(), propertyName, value)
36     return value
37     return defaultValue
38
  
```

Fuente: Autor.

En esta parte del código las variables se dejarán asignadas por defecto sin la necesidad de agregar nuevas ya que solo usaremos la detención como parámetro por defecto agregando solo como adicional en la estructura del código que se envié un mensaje en texto plano.

Figura 32. Programación 1.1.

```

39- def mouseEvent(pressed, x, y, firstPress):
40     # Cuando el mouse pasa sobre el sensor con ALT presionado
41     setState(1)
42     # 🚩 VULNERABILIDAD: Envía mensaje en texto plano
43     customWrite(0, "MOVIMIENTO_DETECTADO")
44     print("🔴 MOVIMIENTO_DETECTADO (texto plano)")
45
46- def loop():
47     global state
48     global current_time
49     if state == 1:
50         current_time = current_time - 1
51         if current_time <= 0:
52             setState(0)
53             # 🚩 VULNERABILIDAD: Envía mensaje en texto plano al desactivarse
54             customWrite(0, "SIN_MOVIMIENTO")
55             print("🟢 SIN_MOVIMIENTO (texto plano)")
56         sleep(1)
57
58- def setState(newState):
59     global state
60     global DEACTIVATE_TIMER
61     global current_time
62     state = newState
63
64     if state == 0:
65         digitalWrite(1, LOW)
66     else:
67         digitalWrite(1, HIGH)
68         current_time = DEACTIVATE_TIMER
69
70     IoEClient.reportStates(state)
71     setDeviceProperty(getName(), "state", state)
72
73- if __name__ == "__main__":
74     main()

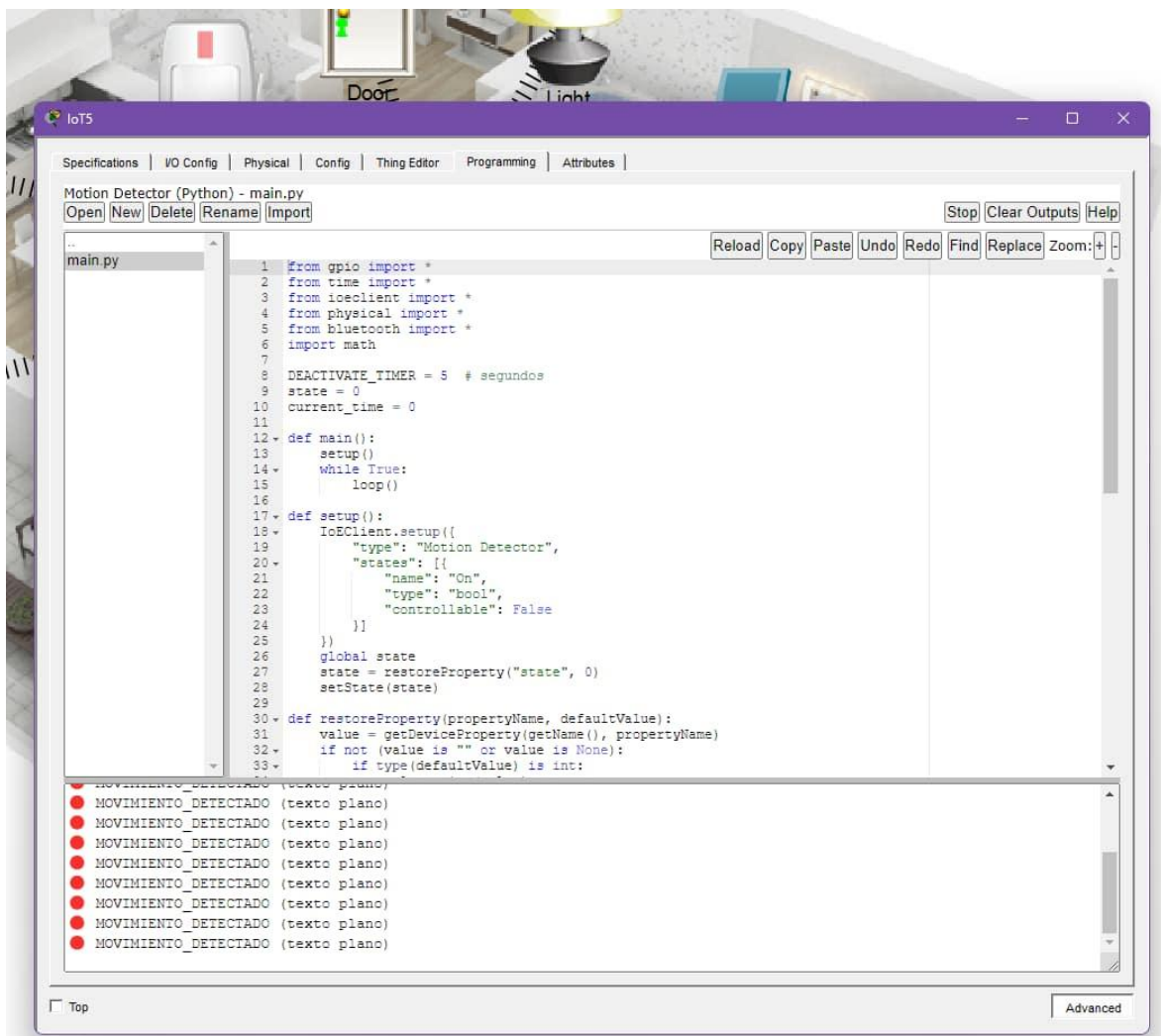
```

Fuente: Autor.

Después de que el evento sea activado por el sensor dentro del mismo se define el loop de evento relacionado al mensaje y la cantidad de este cada segundo que sea detectado el movimiento, en cuanto el dispositivo deja de detectar movimiento este se desactiva enviando un único mensaje que indica sin movimiento.

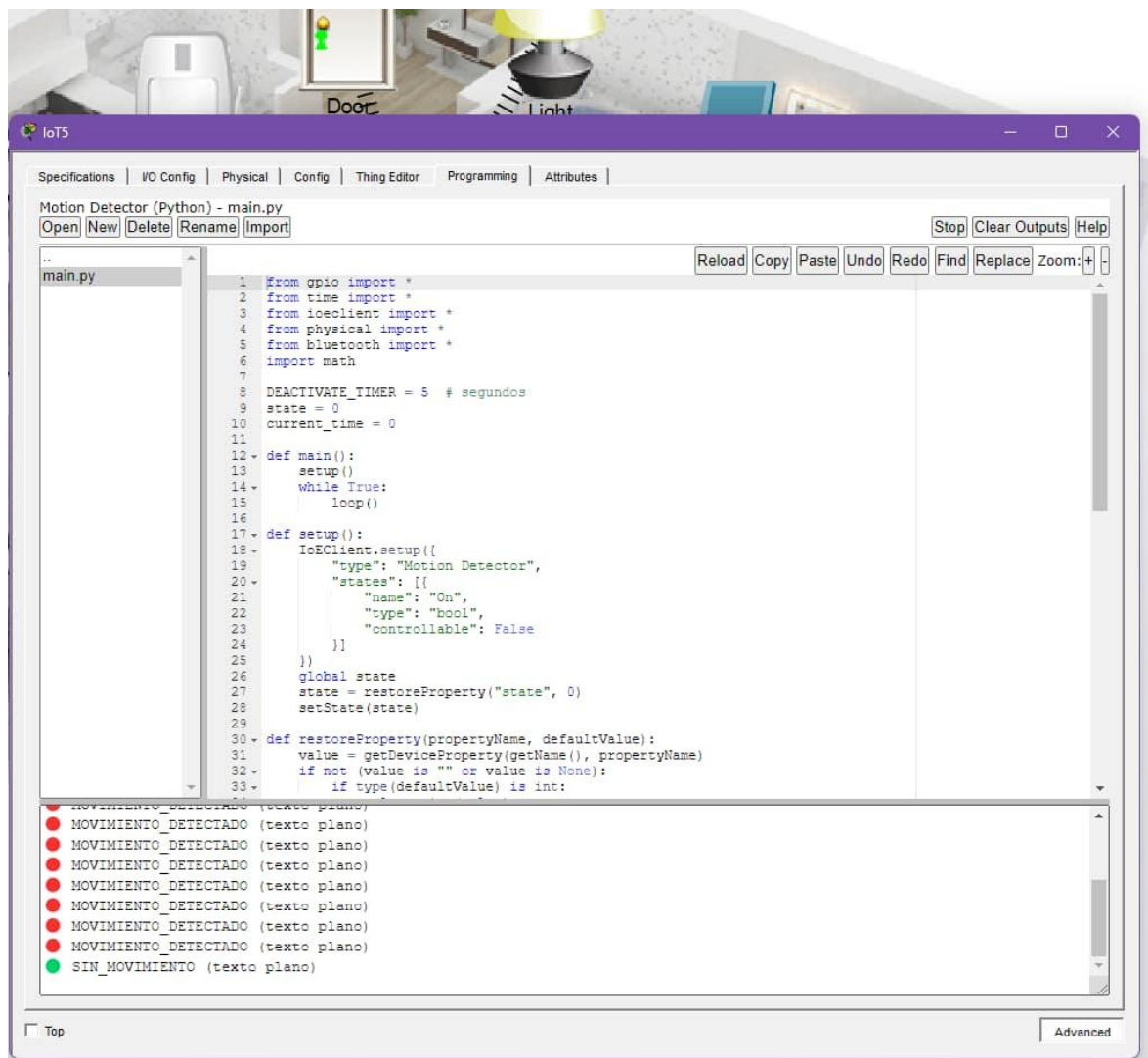
De este modo así se ha simulado un dispositivo moderno, pero con una de las vulnerabilidades más grave evaluadas dentro de la matriz, siendo este el envío de texto plano sin cifrar mediante la red.

Figura 33. Muestra de funcionalidad No.1.



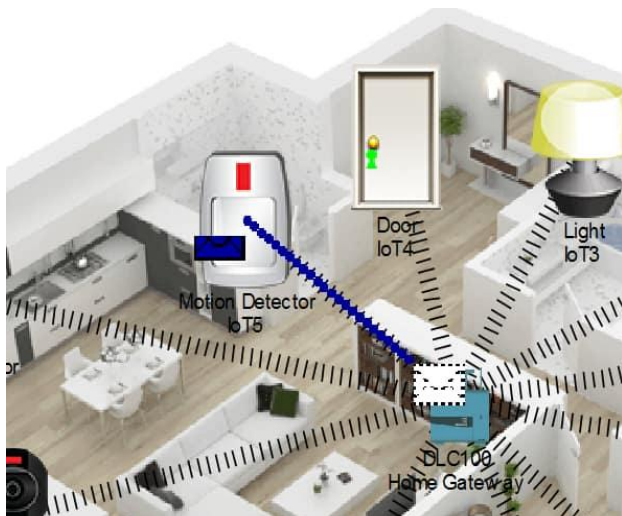
Fuente: Autor.

Figura 34. Muestra de funcionalidad No.2 tras 5 segundos de inactividad.



Fuente: Autor.

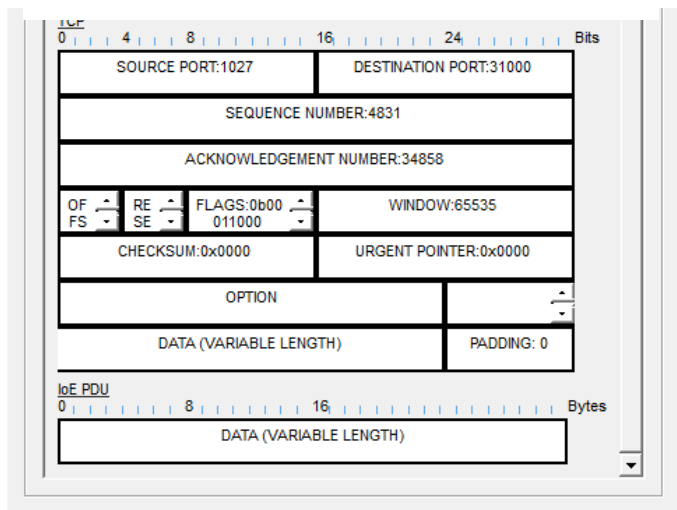
Figura 35. Muestra de funcionalidad No.3.



Fuente: Autor.

En la siguiente muestra de funcionalidad se valida el envío del paquete del detector de movimiento hacia el DLC Home Gateway este paquete para utilidad de la demostración primero viajara en texto plano como se demuestra en la consola del anexo muestra de funcionalidad No.1 y No.2.

Figura 36. Muestra de funcionalidad No.4.



Fuente: Autor.

En esta muestra de funcionalidad se aparecía que el home Gateway ha recibido el paquete de manera satisfactoria indicando de ese modo que cualquier persona en la red puede interceptar dicho mensaje cuándo es transmitido.

Demostración del caso seguro:

Demostrado en caso grave en el que un dispositivo envía información sin cifrar, ahora se presentara como un dispositivo debe de actuar de manera correcta corrigiendo el problema de esta vulnerabilidad o directamente remplazar el dispositivo por uno el cual cumpla con los parámetros de seguridad.

Siguiendo la simulación se procede a realizar el cambio del código para que el dispositivo envíe los datos, pero esta vez cumpliendo con el parámetro de cifrado para evitar que un atacante pueda interceptar dicha información.

Figura 37. Programación 1.2.

```
1 from gpio import *
2 from time import *
3 from ioecclient import *
4 from physical import *
5 from bluetooth import *
6 import math
7
8 DEACTIVATE_TIMER = 5
9 state = 0
10 current_time = 0
11
12 # Funcion de cifrado (Cesar +1)
13 def cifrar(mensaje):
14     mensaje_cifrado = ""
15     for c in mensaje:
16         # Desplaza cada caracter en +1
17         mensaje_cifrado += chr(ord(c) + 1)
18     return mensaje_cifrado
19
20 def main():
21     setup()
22     while True:
23         loop()
24
25 def setup():
26     IoEClient.setup({
27         "type": "Motion Detector",
28         "states": [{
29             "name": "On",
30             "type": "bool",
31             "controllable": False
32         }]
33     })
34     global state
35     state = restoreProperty("state", 0)
36     setState(state)
37
38 def restoreProperty(propertyName, defaultValue):
39     value = getDeviceProperty(getName(), propertyName)
40     if not (value is "" or value is None):
41         if type(defaultValue) is int:
42             value = int(value)
43         setDeviceProperty(getName(), propertyName, value)
44     return value
45     return defaultValue
46
47 def mouseEvent(pressed, x, y, firstPress):
48     setState(1)
49     mensaje_original = "MOVIMIENTO DETECTADO"
50     mensaje_cifrado = cifrar(mensaje_original)
51     customWrite(0, mensaje_cifrado)
52     # Reemplazo de f-string por concatenación clásica
53     print("[Cifrado] " + mensaje_original + " -> " + mensaje_cifrado)
```

Fuente: Autor.

Figura 38. Programación 1.2.1

```
55- def loop():
56-     global state
57-     global current_time
58-     if state == 1:
59-         current_time = current_time - 1
60-         if current_time <= 0:
61-             setState(0)
62-             mensaje_original = "SIN_MOVIMIENTO"
63-             mensaje_cifrado = cifrar(mensaje_original)
64-             customWrite(0, mensaje_cifrado)
65-             # Reemplazo de f-string por concatenación clásica
66-             print("[Cifrado] " + mensaje_original + " -> " + mensaje_cifrado)
67-         sleep(1)
68-
69- def setState(newState):
70-     global state
71-     global DEACTIVATE_TIMER
72-     global current_time
73-     state = newState
74-
75-     if state == 0:
76-         digitalWrite(1, LOW)
77-     else:
78-         digitalWrite(1, HIGH)
79-         current_time = DEACTIVATE_TIMER
80-
81-     IoEClient.reportStates(state)
82-     setDeviceProperty(getName(), "state", state)
83-
84- if __name__ == "__main__":
85-     main()
```

Fuente: Autor.

Con el nuevo código el dispositivo es parcheado solventando la vulnerabilidad, envió de datos en texto plano pasando a un estado más seguro en el cual antes de enviar la información el dispositivo la cifra y envía los datos ya seguros.

Nota: En la parte superior del código se puede observar la función de cifrar agregada que solventara el gran agujero de seguridad, por prácticas de funcionalidad y demostración no se agrega un código complejo que genere claves de cifrado esto con el fin meramente demostrativo.

Figura 39. Demostración de funcionalidad No.3.

```

54
55 def loop():
56     global state
57     global current_time
58     if state == 1:
59         current_time = current_time - 1
60         if current_time <= 0:
61             setState(0)
62             mensaje_original = "SIN_MOVIMIENTO"
63             mensaje_cifrado = cifrar(mensaje_original)
64             customWrite(0, mensaje_cifrado)
65             # Reemplazo de f-string por concatenación clásica
66             print("[Cifrado] " + mensaje_original + " -> " + mensaje_cifrado)
67         sleep(1)
68
69 def setState(newState):
70     global state
71     global DEACTIVATE_TIMER
72     global current_time
73     state = newState
74
75     if state == 0:
76         digitalWrite(1, LOW)
77     else:
78         digitalWrite(1, HIGH)
79         current_time = DEACTIVATE_TIMER
80
81     IoEClient.reportStates(state)
82     setDeviceProperty(getName(), "state", state)
83
84 if __name__ == "__main__":
85     main()

```

Starting Motion Detector (Python)...

```

[Cifrado] MOVIMIENTO_DETECTADO -> NPWJNJFOUP`EFUFDUBEP
[Cifrado] MOVIMIENTO_DETECTADO -> NPWJNJFOUP`EFUFDUBEP
[Cifrado] MOVIMIENTO_DETECTADO -> NPWJNJFOUP`EFUFDUBEP
[Cifrado] SIN_MOVIMIENTO -> TJO`NPWJNJFOUP

```

Fuente: Autor.

Figura 40. El antes y el ahora cifrado.

Antes.			Ahora.	
●	MOVIMIENTO_DETECTADO	(texto plano)	[Cifrado]	MOVIMIENTO_DETECTADO -> NPWJNJFOUP`EFUFDUBEP
●	MOVIMIENTO_DETECTADO	(texto plano)	[Cifrado]	MOVIMIENTO_DETECTADO -> NPWJNJFOUP`EFUFDUBEP
●	MOVIMIENTO_DETECTADO	(texto plano)	[Cifrado]	MOVIMIENTO_DETECTADO -> NPWJNJFOUP`EFUFDUBEP
●	MOVIMIENTO_DETECTADO	(texto plano)	[Cifrado]	MOVIMIENTO_DETECTADO -> NPWJNJFOUP`EFUFDUBEP
●	MOVIMIENTO_DETECTADO	(texto plano)	[Cifrado]	MOVIMIENTO_DETECTADO -> NPWJNJFOUP`EFUFDUBEP
●	MOVIMIENTO_DETECTADO	(texto plano)	[Cifrado]	MOVIMIENTO_DETECTADO -> NPWJNJFOUP`EFUFDUBEP
●	MOVIMIENTO_DETECTADO	(texto plano)	[Cifrado]	MOVIMIENTO_DETECTADO -> NPWJNJFOUP`EFUFDUBEP
●	SIN_MOVIMIENTO	(texto plano)	[Cifrado]	SIN_MOVIMIENTO -> TJO`NPWJNJFOUP

Fuente: Autor.

ELABORADO POR:
Docencia

REVISADO POR:
Sistema Integrado de Gestión

APROBADO POR: Líder del Sistema Integrado de Gestión
FECHA APROBACIÓN: Octubre de 2023

Demostración de vulnerabilidades mediante actualizaciones inseguras del firmware.

El tercer escenario de ataque hace referencia a los riesgos relacionados con la gestión del firmware del dispositivo. El firmware es el software que permite la correcta operación del hardware por parte del mismo, de manera que cualquier vulneración del firmware puede permitir que el dispositivo sea comprometido de forma completa.

Diferentes investigaciones recientes sobre la ingeniería inversa de firmware IoT han puesto de manifiesto que muchos dispositivos de hogar no implementan mecanismos adecuados de verificación de autenticidad de las actualizaciones o utilizan funciones inseguras durante su proceso de desarrollo o hasta posibilitan el despliegue de las mismas actualizaciones modificadas y sin validación criptográfica (NIST, 2020).

Estas debilidades hacen que el código malicioso sea más fácil de incluir, así como que la persistencia del atacante y el control permanente del dispositivo sean una realidad.

La demostración práctica consiste en evaluar si el modelo de seguridad verifica la integridad del firmware antes de permitir su instalación. Para ello, pueden simularse intentos de actualización utilizando versiones alteradas o no firmadas digitalmente, comprobando si el sistema rechaza dichas instalaciones y genera los registros correspondientes (Fagan et al., 2020).

Asimismo, se valida que el modelo supervise la existencia de nuevas versiones oficiales y mantenga un historial de actualizaciones realizadas sobre cada dispositivo.

Este tipo de pruebas cumplen las recomendaciones fijadas mediante ETSI EN 303 645 y por parte de NIST, que consideran que los dispositivos IoT tienen que tener capacidades para realizar actualizaciones de procesos seguros, validación criptográfica de firmware y mecanismos para la autenticidad del software instalado durante el ciclo vital del dispositivo (ISO/IEC, 2022; ETSI, 2020).

En conjunto, la demostración de estos tres escenarios permite comprobar que el modelo de seguridad desarrollado protege el entorno IoT frente a amenazas ampliamente documentadas en la literatura especializada.

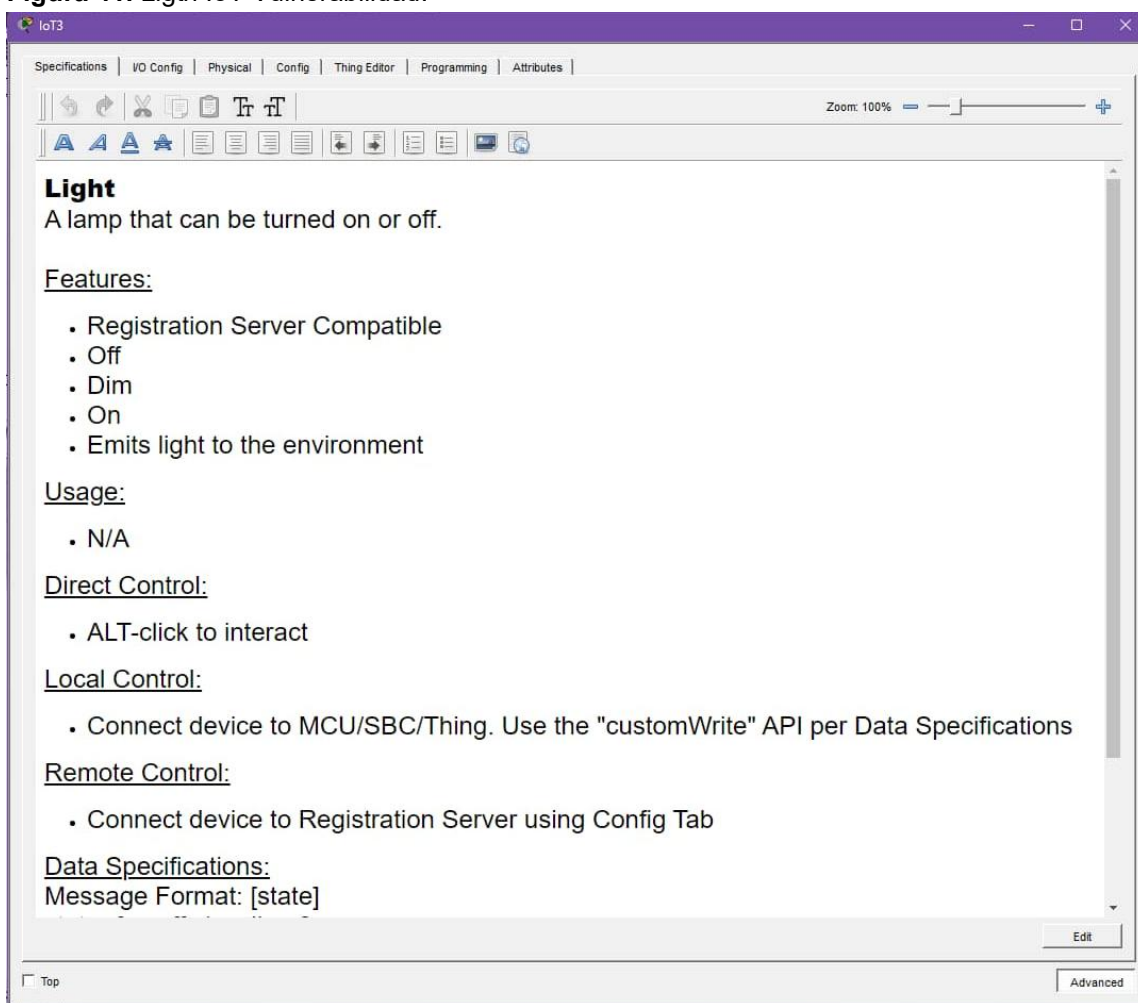
La utilización de credenciales robustas, el cifrado de las comunicaciones y la validación segura del firmware constituyen controles fundamentales para reducir la superficie de ataque de una vivienda inteligente y se encuentran respaldados por las principales normas y organismos internacionales dedicados a la ciberseguridad de dispositivos IoT.

Construcción del escenario.

Para la construcción del escenario tomaremos el dispositivo de iluminación “light IoT3”. En este caso si tendremos que modificar el código completo para hacer la demostración de descarga de actualización automática por defecto del dispositivo mediante un servidor Http sin verificar la firma digital. Un atacante en la misma red

podría interceptar la descarga (Man-in-the-Middle) y reemplazar el firmware legítimo por uno malicioso.

Figura 41. Ligth IoT Vulnerabilidad.



Fuente: Autor.

Como en el ejemplo anterior se programa el dispositivo con el fin de que realice comprobaciones de actualización de firmware siguiendo los anteriores pasos llevados a cabo en la vulnerabilidad de cifrado y de ese modo programar el dispositivo.

Programación:

Figura 42. Programación 2.

```

1 from gpio import *
2 from time import *
3
4 # Simula la descarga del firmware desde un servidor HTTP
5 def descargar_firmware():
6     # En una implementación real, sería una solicitud HTTP GET
7     print("[Vulnerable] Descargando firmware desde http://servidor/firmware.bin")
8     # Simulamos que la descarga es exitosa
9     return "firmware_data"
10
11 def instalar_firmware(firmware):
12     # No se verifica la firma
13     print("[Vulnerable] Instalando firmware sin verificar firma...")
14     print("[Vulnerable] Firmware instalado correctamente.")
15
16 def loop():
17     print("[Vulnerable] Verificando actualizaciones...")
18     firmware = descargar_firmware()
19     instalar_firmware(firmware)
20     sleep(10)
21
22 def main():
23     print("[Vulnerable] Lámpara iniciada. Buscando actualizaciones...")
24     while True:
25         loop()
26
27 if __name__ == "__main__":
28     main()

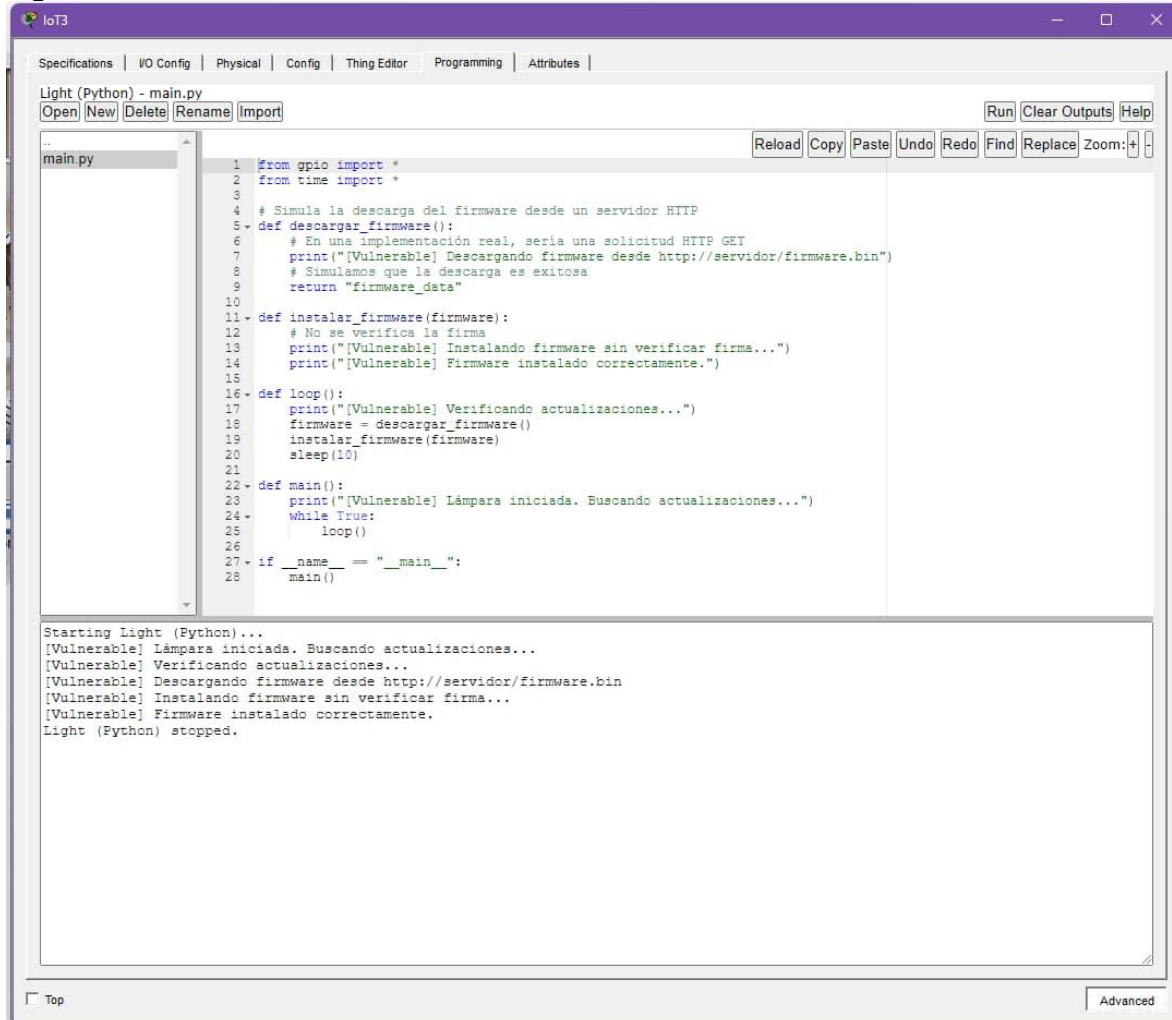
```

Fuente: Autor.

En el siguiente código se creará un “loop” de eventos para que el dispositivo compruebe actualizaciones cada cierto tiempo, en la primera parte y siguiendo los comentarios dentro del mismo, se realizara la descarga del firmware que se mostrara incluso como mensaje sin cifrar.

Con lo anterior y verificado que existe actualización el código instalara las actualizaciones sin importar si el servidor usa protocolos seguros, si está cifrado o si la misma actualización está firmada digitalmente y cuya firma sea legítima.

Figura 43. Muestra de funcionalidad No.4.



```

Light (Python) - main.py
Open New Delete Rename Import Run Clear Outputs Help

main.py
1 from gpio import *
2 from time import *
3
4 # Simula la descarga del firmware desde un servidor HTTP
5 def descargar_firmware():
6     # En una implementación real, sería una solicitud HTTP GET
7     print("[Vulnerable] Descargando firmware desde http://servidor/firmware.bin")
8     # Simulamos que la descarga es exitosa
9     return "firmware_data"
10
11 def instalar_firmware(firmware):
12     # No se verifica la firma
13     print("[Vulnerable] Instalando firmware sin verificar firma...")
14     print("[Vulnerable] Firmware instalado correctamente.")
15
16 def loop():
17     print("[Vulnerable] Verificando actualizaciones...")
18     firmware = descargar_firmware()
19     instalar_firmware(firmware)
20     sleep(10)
21
22 def main():
23     print("[Vulnerable] Lámpara iniciada. Buscando actualizaciones...")
24     while True:
25         loop()
26
27 if __name__ == "__main__":
28     main()

Starting Light (Python)...
[Vulnerable] Lámpara iniciada. Buscando actualizaciones...
[Vulnerable] Verificando actualizaciones...
[Vulnerable] Descargando firmware desde http://servidor/firmware.bin
[Vulnerable] Instalando firmware sin verificar firma...
[Vulnerable] Firmware instalado correctamente.
Light (Python) stopped.
Top Advanced

```

Fuente: Autor.

Iniciada la simulación continuaremos con el ataque al dispositivo, primero mediante un equipo que simulara ser el atacante pasara lo siguiente: El atacante (Laptop-1) está en la misma red y tiene acceso usando credenciales por defecto admin/admin en el Home Gateway demostrado en la primera vulnerabilidad el siguiente paso.

El atacante configura un servidor HTTP malicioso en su laptop (simulado) haciéndose pasar por el servicio oficial y el cual el mismo ofrece un firmware con código malicioso.

El atacante redirige el tráfico de la lámpara hacia su servidor (mediante ARP Spoofing o modificando la configuración DNS). La lámpara descarga el firmware malicioso desde <http://laptop-atacante/firmware.bin> en lugar del servidor legítimo así la lámpara instala el firmware sin verificar firma, quedando comprometida.

Aunque en Packet Tracer este limitado y no pueda ejecutar un ataque MITM real, la evidencia está en el hecho de que la descarga es por HTTP y no hay verificación de firma, lo que permite este tipo de ataque en un entorno real.

Demostración del caso seguro:

Demostrado en caso grave en el que un dispositivo descarga las actualizaciones de entornos no seguros, sin validar la legitimidad o estado de la firma, ahora se presentara como un dispositivo debe de actuar de manera correcta ya sea mediante una actualización que corrige el problema de esta vulnerabilidad o remplazando el dispositivo inseguro.

Siguiendo la simulación: el fabricante opta por lanzar un parche masivo que actualiza los dispositivos con esta vulnerabilidad a continuación, representada en el siguiente código.

Figura 44. Programación 2.1.

```

1 from gpio import *
2 from time import *
3
4 # --- Configuración ---
5 FIRMA_ESPERADA = "firma_valida_123" # Firma que consideramos válida
6
7 # --- Función de hash simple (simulación) ---
8 def calcular_hash(texto):
9     total = 0
10    for c in texto:
11        total += ord(c)
12    return hex(total)
13
14 # --- Verificación de firma ---
15 def verificar_firma(firmware, firma_recibida):
16    print("[Seguro] Verificando firma del firmware...")
17    hash_calculado = calcular_hash(firmware)
18    print("[Seguro] Hash calculado: " + hash_calculado)
19    print("[Seguro] Firma recibida: " + firma_recibida)
20
21    if firma_recibida == FIRMA_ESPERADA:
22        print("[Seguro] FIRMA VERIFICADA CON EXITO")
23        return True
24    else:
25        print("[Seguro] FIRMA INVALIDA - Actualizacion rechazada")
26        return False
27
28 # --- Descarga segura (HTTPS) ---
29 def descargar_firmware():
30    print("[Seguro] Descargando firmware desde https://servidor/firmware.bin")
31    firmware = "contenido_del_firmware_seguro"
32    firma = FIRMA_ESPERADA # Firma válida
33    return firmware, firma
34
35 # --- Instalación segura ---
36 def instalar_firmware(firmware, firma):
37    if verificar_firma(firmware, firma):
38        print("[Seguro] Instalando firmware...")
39        print("[Seguro] Firmware instalado correctamente.")
40    else:
41        print("[Seguro] Instalacion cancelada por firma invalida.")
42
43 # --- Bucle principal ---
44 def loop():
45    print("[Seguro] Verificando actualizaciones...")
46    firmware, firma = descargar_firmware()
47    instalar_firmware(firmware, firma)
48    sleep(10)
49
50 def main():
51    print("[Seguro] Lampara iniciada. Buscando actualizaciones...")
52    while True:
53        loop()
54
55 if __name__ == "__main__":
56    main()

```

Fuente: Autor.

Con el código de actualización que corrige esta vulnerabilidad ahora el dispositivo cuando detecte una actualización validara la firma del fabricante y el servicio de donde se descargara la actualización si la comprobación pasa todas las pruebas de seguridad y la firma es legítima el dispositivo se actualizara de manera satisfactoria.

Nota: Como uso practico y con el fin demostrativo no se implementa un código complejo que se conecte mediante API para ser valida la firma de la actualización, la misma se toma como validación local.

Figura 45. Muestra de funcionalidad No5. Firma valida.

The screenshot shows the IoT3 IDE interface. The top menu bar includes 'Specifications', 'I/O Config', 'Physical', 'Config', 'Thing Editor', 'Programming', and 'Attributes'. The main editor displays a Python script named 'main.py' with the following code:

```

25     print("[Seguro] FIRMA INVALIDA - Actualizacion rechazada")
26     return False
27
28 # --- Descarga segura (HTTPS) ---
29 def descargar_firmware():
30     print("[Seguro] Descargando firmware desde https://servidor/firmware.bin")
31     firmware = "contenido_del_firmware_seguro"
32     firma = FIRMA_ESPERADA # Firma valida
33     return firmware, firma
34
35 # --- Instalación segura ---
36 def instalar_firmware(firmware, firma):
37     if verificar_firma(firmware, firma):
38         print("[Seguro] Instalando firmware...")
39         print("[Seguro] Firmware instalado correctamente.")
40     else:
41         print("[Seguro] Instalacion cancelada por firma invalida.")
42
43 # --- Bucle principal ---
44 def loop():
45     print("[Seguro] Verificando actualizaciones...")
46     firmware, firma = descargar_firmware()
47     instalar_firmware(firmware, firma)
48     sleep(10)
49
50 def main():
51     print("[Seguro] Lampara iniciada. Buscando actualizaciones...")
52     while True:
53         loop()
54
55 if __name__ == "__main__":
56     main()

```

Below the code editor, the output console shows the execution results:

```

Light (Python) stopped.
Starting Light (Python)...
[Seguro] Lampara iniciada. Buscando actualizaciones...
[Seguro] Verificando actualizaciones...
[Seguro] Descargando firmware desde https://servidor/firmware.bin
[Seguro] Verificando firma del firmware...
[Seguro] Hash calculado: 0xc07
[Seguro] Firma recibida: firma valida_123
[Seguro] FIRMA VERIFICADA CON EXITO
[Seguro] Instalando firmware...
[Seguro] Firmware instalado correctamente.

```

Fuente: Autor.

ELABORADO POR:
Docencia

REVISADO POR:
Sistema Integrado de Gestión

APROBADO POR: Líder del Sistema Integrado de Gestión
FECHA APROBACIÓN: Octubre de 2023

Figura 46. Muestra de funcionalidad No5. Firma no valida.

```

1 from gpio import *
2 from time import *
3
4 # --- Configuración ---
5 FIRMA_ESPERADA = "firma_valida_123" # Firma que consideramos válida
6
7 # --- Función de hash simple (simulación) ---
8 def calcular_hash(texto):
9     total = 0
10    for c in texto:
11        total += ord(c)
12    return hex(total)
13
14 # --- Verificación de firma ---
15 def verificar_firma(firmware, firma_recibida):
16     print("[Seguro] Verificando firma del firmware...")
17     hash_calculado = calcular_hash(firmware)
18     print("[Seguro] Hash calculado: " + hash_calculado)
19     print("[Seguro] Firma recibida: " + firma_recibida)
20
21     if firma_recibida == FIRMA_ESPERADA:
22         print("[Seguro] FIRMA VERIFICADA CON EXITO")
23         return True
24     else:
25         print("[Seguro] FIRMA INVALIDA - Actualizacion rechazada")
26         return False
27
28 # --- Descarga segura (HTTPS) ---
29 def descargar_firmware():
30     print("[Seguro] Descargando firmware desde https://servidor/firmware.bin")
31     firmware = "contenido_del_firmware_seguro"

```

Light (Python) stopped.
Starting Light (Python)...

```

[Seguro] Lámpara iniciada. Buscando actualizaciones...
[Seguro] Verificando actualizaciones...
[Seguro] Descargando firmware desde https://servidor/firmware.bin
[Seguro] Verificando firma del firmware...
[Seguro] Hash calculado: 0xc07
[Seguro] Firma recibida: firma_invalida_xyz
[Seguro] FIRMA INVALIDA - Actualizacion rechazada
[Seguro] Instalacion cancelada por firma invalida.

```

Fuente: Autor.

Figura 47. El antes y el ahora, firmas.

Antes	Ahora
Starting Light (Python)... [Vulnerable] Lámpara iniciada. Buscando actualizaciones... [Vulnerable] Verificando actualizaciones... [Vulnerable] Descargando firmware desde http://servidor/firmware.bin [Vulnerable] Instalando firmware sin verificar firma... [Vulnerable] Firmware instalado correctamente. Light (Python) stopped.	Light (Python) stopped. Starting Light (Python)... [Seguro] Lámpara iniciada. Buscando actualizaciones... [Seguro] Verificando actualizaciones... [Seguro] Descargando firmware desde https://servidor/firmware.bin [Seguro] Verificando firma del firmware... [Seguro] Hash calculado: 0xc07 [Seguro] Firma recibida: firma_valida_123 [Seguro] FIRMA VERIFICADA CON EXITO [Seguro] Instalando firmware... [Seguro] Firmware instalado correctamente.

Fuente: Autor.

ELABORADO POR:
Docencia

REVISADO POR:
Sistema Integrado de Gestión

APROBADO POR: Líder del Sistema Integrado de Gestión
FECHA APROBACIÓN: Octubre de 2023

4.9. Modelo final.

4.9.1. Un modelo de protección por capas para dispositivos IoT, redes IoT, información y usuarios.

Introducción al modelo:

La transformación de una vivienda normal o convencional en un hogar inteligente ha generado un ecosistema digital compuesto por dispositivos físicos, sensores, apps “aplicaciones de teléfono celular”, servicios en la nube, redes inalámbricas y mecanismos de automatización.

Una cámara de seguridad, un televisor inteligente, una cerradura electrónica, un asistente de voz, un sensor de movimiento o una bombilla conectada dejan de funcionar como elementos completamente independientes cuando se incorporan a una misma infraestructura de comunicaciones.

En consecuencia, una vulnerabilidad presente en uno de estos elementos puede convertirse en un punto de entrada hacia otros componentes del hogar. Esta característica puede diferenciar a los sistemas IOT (Internet of Things, Internet de las cosas) de muchos sistemas informáticos tradicionales. En una vivienda conectada, los dispositivos poseen una relación directa con el entorno físico.

Un sensor puede detectar movimiento, una cámara puede observar un espacio privado, una cerradura puede controlar un acceso físico y un actuador puede modificar determinadas condiciones del hogar.

Por tanto, un incidente de ciberseguridad no necesariamente termina en la pérdida de información digital, sino que puede afectar la privacidad, la seguridad física y el funcionamiento cotidiano de la vivienda (Wang et al., 2022).

La literatura especializada ha identificado desde hace años que la seguridad debe analizarse considerando el hogar como un ecosistema y no únicamente como un conjunto de dispositivos aislados.

Un análisis de riesgos sobre sistemas de automatización residencial encontró múltiples riesgos vinculados con componentes de software y comportamiento humano, concluyendo que la seguridad y la privacidad deben integrarse desde las primeras etapas del diseño del sistema (Sadeghi et al., 2015).

De manera semejante, estudios sobre arquitecturas de hogares inteligentes han señalado que la heterogeneidad de dispositivos, protocolos y servicios dificulta establecer una estrategia de seguridad uniforme, por lo que resulta necesario analizar las diferentes superficies de ataque del ecosistema completo (Kearney et al., 2018).

El presente modelo propone una arquitectura de ciberseguridad basada en cinco capas: hardware, software, red, factor humano y gobernanza “toma de decisiones”. La estructura se conserva del modelo inicial.

Pero se amplía para incorporar una metodología de gestión de riesgos, controles técnicos y factor humano, mecanismos de detección y respuesta, indicadores de evaluación y un proceso de mejora continua. De esta manera, el modelo deja de ser solamente una lista de recomendaciones y se convierte en un sistema organizado de protección.

4.9.2. Fundamentación del modelo, heredado de la investigación modelo inicial.

El modelo se fundamenta principalmente en cuatro referencias complementarias:

En primera referencia, ISO/IEC 27400:2022 proporciona directrices específicas para abordar riesgos, principios y controles relacionados con la seguridad y privacidad de soluciones IoT. Esta norma resulta especialmente pertinente porque considera el ecosistema IoT y no solamente el dispositivo individual (International Organization for Standardization [ISO], 2022a).

En segunda referencia, ISO/IEC 27402:2023 establece requisitos básicos de seguridad y privacidad para dispositivos IoT. Esta referencia permite trasladar el modelo desde una perspectiva puramente organizacional hacia características concretas que deberían poseer los dispositivos utilizados dentro de la vivienda (ISO, 2023).

En tercera referencia, NISTIR 8259A define siete capacidades técnicas fundamentales para dispositivos IoT: identificación del dispositivo, configuración, protección de datos, control lógico de acceso a interfaces, actualización de software, conocimiento del estado de ciberseguridad y seguridad del dispositivo. Estas capacidades permiten establecer una base técnica para evaluar si un dispositivo puede ser administrado y protegido adecuadamente durante su ciclo de vida (Fagan et al., 2020).

En cuarta referencia, NIST Cybersecurity Framework 2.0 (CSF 2.0) proporciona una estructura general para gestionar riesgos de ciberseguridad mediante seis funciones: Govern, Identify, Protect, Detect, Respond y Recover. La incorporación

de Govern es particularmente importante para una vivienda inteligente porque permite relacionar la tecnología con políticas, responsabilidades, criterios de adquisición, tolerancia al riesgo y toma de decisiones (Pascoe et al., 2024).

Adicionalmente, ETSI EN 303 645 proporciona requisitos de referencia para dispositivos IoT de consumo. Entre otros aspectos, establece que no deben mantenerse contraseñas universales predeterminadas y aborda la integridad del software y los mecanismos de actualización segura (ETSI, 2024).

Por último, ISO/IEC 27001:2022 e ISO/IEC 27002:2022 aportan una perspectiva de gestión de riesgos, controles y mejora continua. Es importante aclarar que ISO/IEC 27001 no es una norma específica para dispositivos IoT ni significa que un hogar pueda considerarse automáticamente certificado por aplicar este modelo.

Su valor en este contexto consiste en aportar principios de gestión y control que pueden adaptarse al entorno residencial (ISO, 2022b, 2022c).

Citando el objetivo general de esta investigación:

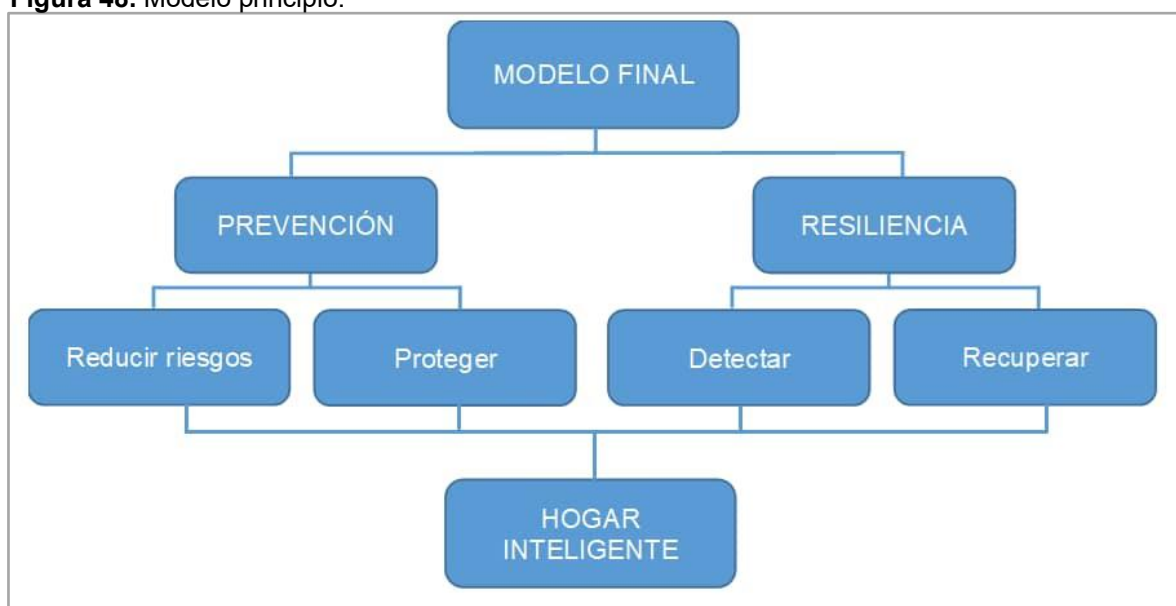
“Proteger los sistemas y dispositivos de casas IoT automatizadas mediante un modelo que asegure la defensa ante amenazas cibernéticas y la continuidad de los servicios en caso de incidentes.”

El objetivo general del modelo es proporcionar una metodología práctica y escalable donde se asegura la defensa ante amenazas cibernéticas para este fin el modelo final: identifica, evalúa, detecta, previene, responder y recupera de amenazas de ciberseguridad que puedan afectar a los dispositivos y servicios IoT utilizados dentro de una vivienda inteligente entonces;

El modelo pretende que la seguridad no dependa de una única herramienta. En lugar de asumir que un antivirus, un router, persona o una contraseña pueden proteger por sí solos todo el hogar, se establece una estrategia de defensa en profundidad.

Este principio puede representarse de la siguiente manera:

Figura 48. Modelo principio.



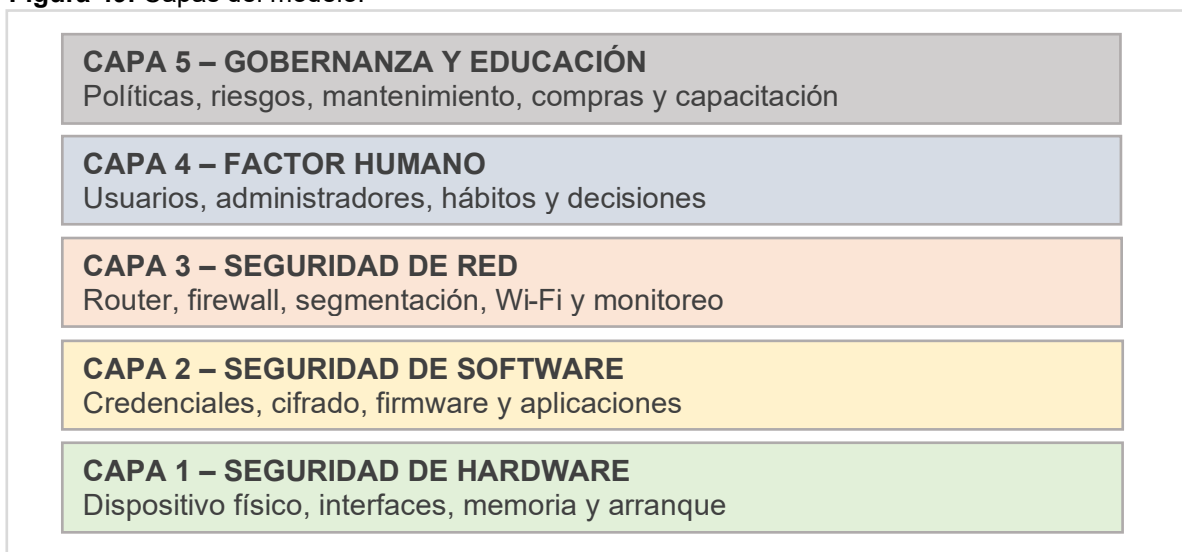
Fuente: Autor.

La finalidad no consiste en afirmar que un hogar puede ser completamente invulnerable. Ningún modelo de ciberseguridad puede garantizar la ausencia absoluta de incidentes. Su finalidad es reducir la probabilidad de compromiso, limitar el impacto cuando ocurre un incidente y aumentar la capacidad de recuperación.

4.9.3. Arquitectura general de cinco capas modelo final.

La arquitectura conserva la estructura original del modelo:

Figura 49. Capas del modelo.



Fuente: Autor.

La idea fundamental es que cada capa reduzca la posibilidad de que una vulnerabilidad localizada en otra capa pueda convertirse en un riesgo que comprometa por completo el hogar.

Por ejemplo, si una cámara tiene una contraseña débil, la capa de software debería impedir el acceso no autorizado. Si este control falla, la segmentación de red debería impedir que la cámara pueda comunicarse libremente con los equipos personales.

Si también fallara este mecanismo, el monitoreo debería detectar el comportamiento anómalo. Finalmente, la gobernanza debería disponer de procedimientos para retirar, actualizar o reemplazar el dispositivo.

Este enfoque coincide con investigaciones recientes que destacan la conveniencia de utilizar arquitecturas por capas y separación de responsabilidades para

administrar sistemas domésticos complejos (Kearney et al., 2018; Radovanovic et al., 2026).

Capa 1: Seguridad de hardware.

Concepto: El hardware representa la base física del ecosistema. Comprende cámaras, sensores, televisores, routers, cerraduras, enchufes, asistentes de voz, microcontroladores, hubs y cualquier otro elemento conectado.

Aunque gran parte de las vulnerabilidades visibles se encuentran en el software, el hardware determina qué mecanismos de protección pueden implementarse. Un dispositivo sin mecanismos adecuados de almacenamiento seguro de claves, sin protección del proceso de arranque o con interfaces de depuración accesibles puede presentar una superficie de ataque considerablemente mayor.

La seguridad del hardware, por lo tanto, debe considerarse desde el proceso de selección y adquisición del dispositivo.

Elementos que deben evaluarse.

El modelo propone evaluar cinco (5) elementos principales:

Identidad del dispositivo. Cada dispositivo debería poder identificarse de forma única. NIST incluye la identificación del dispositivo como una capacidad básica de ciberseguridad para IoT (Fagan et al., 2020).

Protección de credenciales y claves. Las claves criptográficas no deberían mantenerse de forma innecesariamente expuesta en memoria accesible o en mecanismos fácilmente extraíbles.

Arranque seguro. El proceso de arranque debe permitir verificar que el software utilizado para iniciar el dispositivo sea legítimo. ETSI EN 303 645 recomienda mecanismos de secure boot como medio para verificar la integridad del software (ETSI, 2025).

Interfaces de depuración. Interfaces como UART, JTAG u otros mecanismos de mantenimiento deben estar protegidos o deshabilitados cuando no sean necesarios.

Resistencia física. El dispositivo debe considerar escenarios donde una persona pueda acceder físicamente al equipo, especialmente cuando se trata de cámaras, routers, hubs o controladores instalados en lugares accesibles.

Función dentro del modelo.

La función de esta capa consiste en impedir que el atacante pueda obtener una ventaja desde el nivel físico. En términos sencillos: El dispositivo debe comenzar su funcionamiento desde un estado confiable. Esto no significa que el hardware sea perfecto, sino que proporciona una base de confianza sobre la cual pueden funcionar las capas superiores.

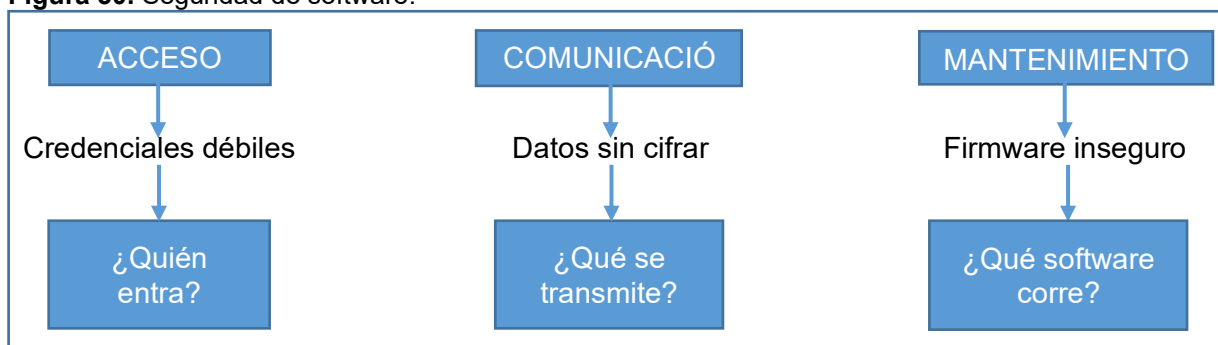
Capa 2: Seguridad de software.

La capa de software constituye uno de los componentes centrales del modelo debido a que concentra mecanismos de autenticación, comunicación, almacenamiento de información, procesamiento de datos y actualización.

El modelo original identificaba tres vulnerabilidades prioritarias: credenciales predeterminadas, comunicaciones sin cifrado y actualizaciones inseguras de

firmware. Estas tres categorías se mantienen porque permiten representar tres momentos fundamentales del riesgo:

Figura 50. Seguridad de software.



Fuente: Autor.

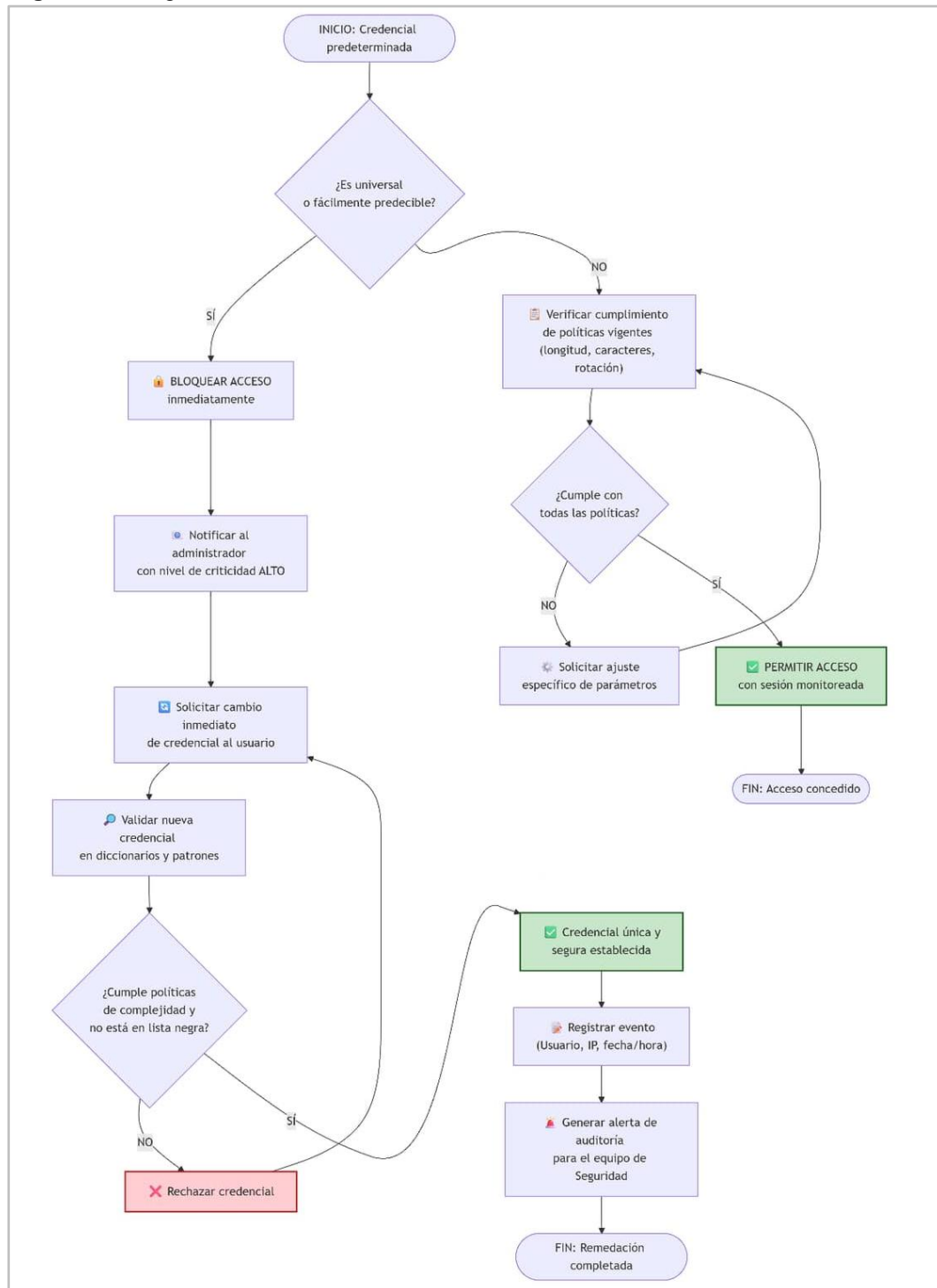
Credenciales por defecto.

Los dispositivos IoT históricamente han sido afectados por contraseñas universales o fáciles de adivinar. El caso de Mirai constituye uno de los ejemplos más conocidos. Antonakakis et al. (2017) analizaron la botnet Mirai y documentaron cómo esta logró comprometer cientos de miles de dispositivos IoT, evidenciando la fragilidad de numerosos equipos conectados.

(ETSI EN 303 645), aborda directamente este problema. Su disposición sobre contraseñas establece que, fuera del estado de fábrica, las contraseñas utilizadas por dispositivos IoT de consumo deben ser únicas por dispositivo o definidas por el usuario; además, la norma menciona expresamente las combinaciones universales como admin/admin como una práctica que debe eliminarse (ETSI, 2024).

Por ello, el modelo establece los siguientes controles:

Figura 51. Diagrama de credenciales.



Fuente: Autor.

El modelo también debe considerar la posibilidad de utilizar mecanismos distintos de contraseña cuando la arquitectura del dispositivo lo permita. ETSI contempla, por ejemplo, identidades únicas, certificados y autenticación multifactorial como mecanismos que pueden aumentar la seguridad (ETSI, 2024).

Comunicaciones sin cifrar.

La segunda vulnerabilidad se relaciona con la protección de la información durante su transmisión. Un sensor de movimiento puede producir un dato aparentemente simple:

MOVIMIENTO = DETECTADO

Sin embargo, desde una perspectiva de privacidad, este dato puede revelar que una persona está dentro de la vivienda. La investigación sobre privacidad en hogares inteligentes ha demostrado que incluso patrones de tráfico pueden permitir inferir actividades de los usuarios.

En un estudio sobre tráfico de dispositivos domésticos, los investigadores mostraron que determinados patrones permiten inferir el estado de dispositivos y, por extensión, información sobre las actividades de las personas (Liu et al., 2023).

Por esta razón, el modelo debe evaluar tanto la confidencialidad del contenido como la exposición derivada del comportamiento de la red, no basta simplemente mantener un entorno cerrado si no también contar con que el dispositivo cuente con los protocolos de protección de la información que este envía a través de la red.

Para esto la protección de la comunicación debe contemplar, según las capacidades del dispositivo y protocolo son las siguientes:

- TLS para comunicaciones basadas en TCP.
- DTLS para determinados protocolos orientados a datagramas.
- HTTPS en interfaces web.
- Mecanismos de cifrado proporcionados por los protocolos inalámbricos.
- Autenticación mutua cuando el escenario lo requiera.

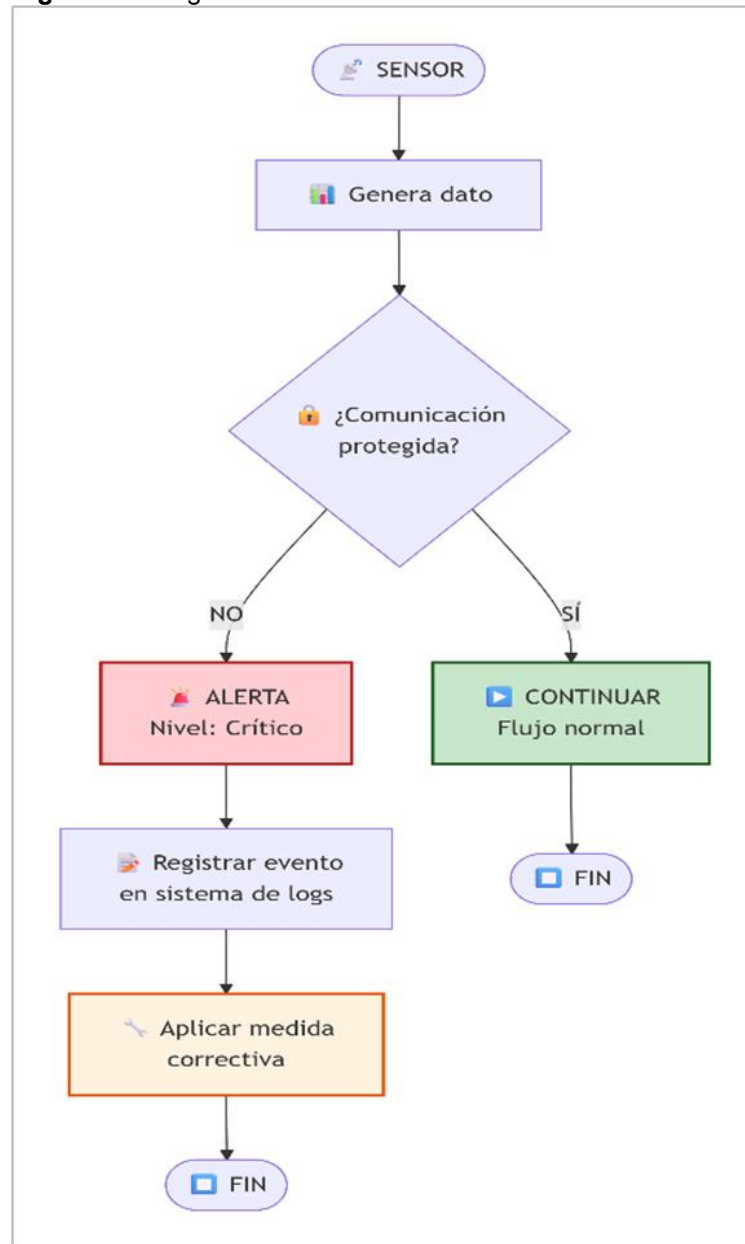
La literatura reciente confirma que TLS y DTLS constituyen mecanismos centrales para proteger comunicaciones IoT, mientras que protocolos como MQTT deben utilizarse con configuraciones de seguridad apropiadas cuando transmiten información sensible (Radovanovic et al., 2026).

Asimismo, la seguridad en el envío de la información por parte de dichos dispositivos debe complementarse de ser estrictamente necesario si se trata de entornos IoT aplicados a oficinas en casa o áreas de trabajo comunes en el hogar ya que de ser así es fundamental contar con mecanismos más robustos.

Como el control de acceso y autenticación a nivel de aplicación, integrando estándares como OAuth 2.0 o JSON Web Tokens (JWT) para garantizar la trazabilidad y la integridad de los datos en todo el ecosistema conectado (Seitz, H., Selander, G., & Erdtman, S. 2022).

La evaluación del modelo puede resumirse:

Figura 52. Diagrama de sensor básico.



Fuente: Autor.

Actualización segura del firmware.

La tercera vulnerabilidad crítica corresponde a las actualizaciones inseguras, un dispositivo IoT necesita actualizaciones porque con el tiempo se descubren vulnerabilidades nuevas.

Sin embargo, actualizar no significa automáticamente estar seguro. Si un atacante puede reemplazar una actualización legítima por una versión manipulada, el mecanismo diseñado para proteger el dispositivo puede transformarse en un mecanismo de ataque.

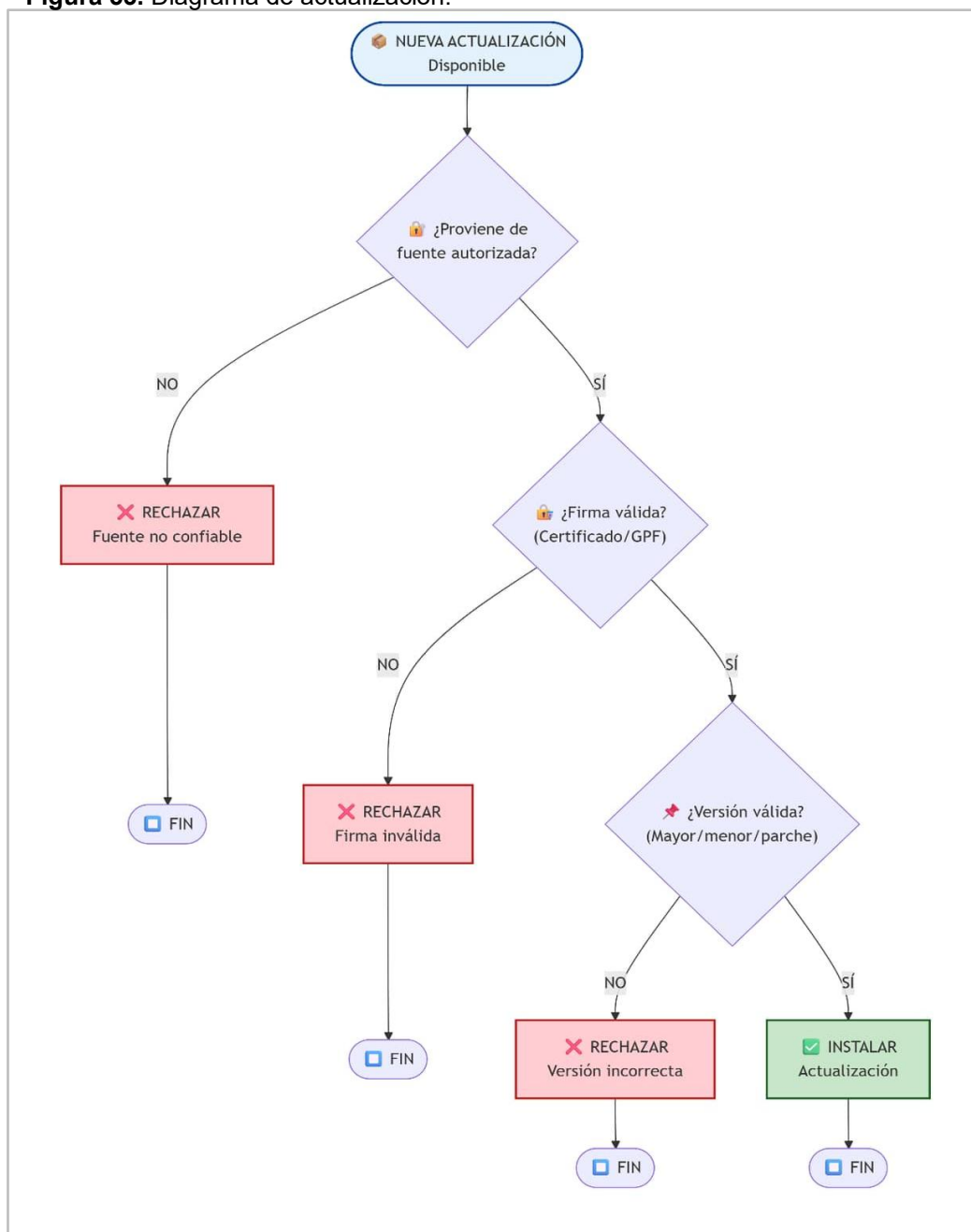
Una revisión especializada sobre actualizaciones OTA de firmware IoT identifica precisamente la autenticidad de la imagen, la integridad, la cadena de confianza y la heterogeneidad de dispositivos como problemas fundamentales para la seguridad del proceso de actualización (Karimian et al., 2022).

ETSI EN 303 645 recomienda que los dispositivos puedan verificar la integridad del software mediante mecanismos como secure boot y que, cuando se detecte una modificación no autorizada, el dispositivo pueda alertar al usuario o administrador y limitar su conectividad mientras se recupera de un estado conocido como seguro (ETSI, 2025). La seguridad de la actualización debe entenderse, por tanto, como una cadena:

**servidor confiable → comunicación protegida → imagen auténtica →
integridad comprobada → instalación autorizada → arranque seguro.**

Si uno de esos elementos desaparece, la confianza del proceso puede verse comprometida. El modelo propone que una actualización atraviese al menos cuatro verificaciones conceptuales.

Figura 53. Diagrama de actualización.



Fuente: Autor.

ELABORADO POR:
Docencia

REVISADO POR:
Sistema Integrado de Gestión

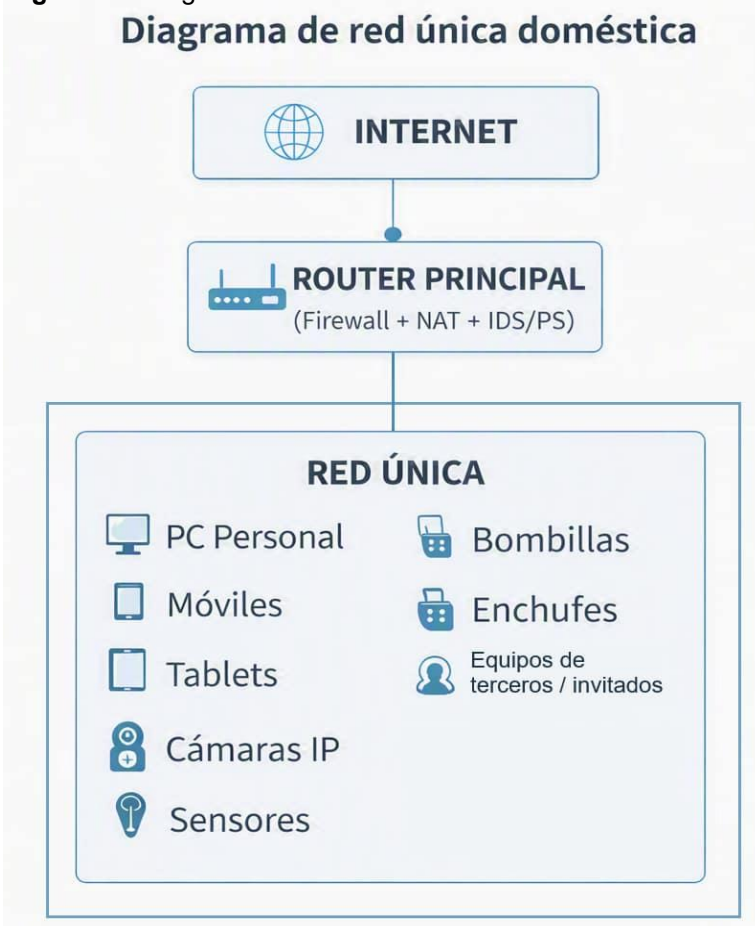
APROBADO POR: Líder del Sistema Integrado de Gestión
FECHA APROBACIÓN: Octubre de 2023

Capa 3: Seguridad de red.

La red representa el entorno por el cual circula la información entre los dispositivos. El modelo original identifica correctamente un problema frecuente: la denominada red plana, en la cual los computadores, teléfonos, cámaras, sensores y otros dispositivos utilizan la misma red de forma plana sin separación por secciones dedicadas.

El problema puede visualizarse así:

Figura 54. Diagrama de red única.

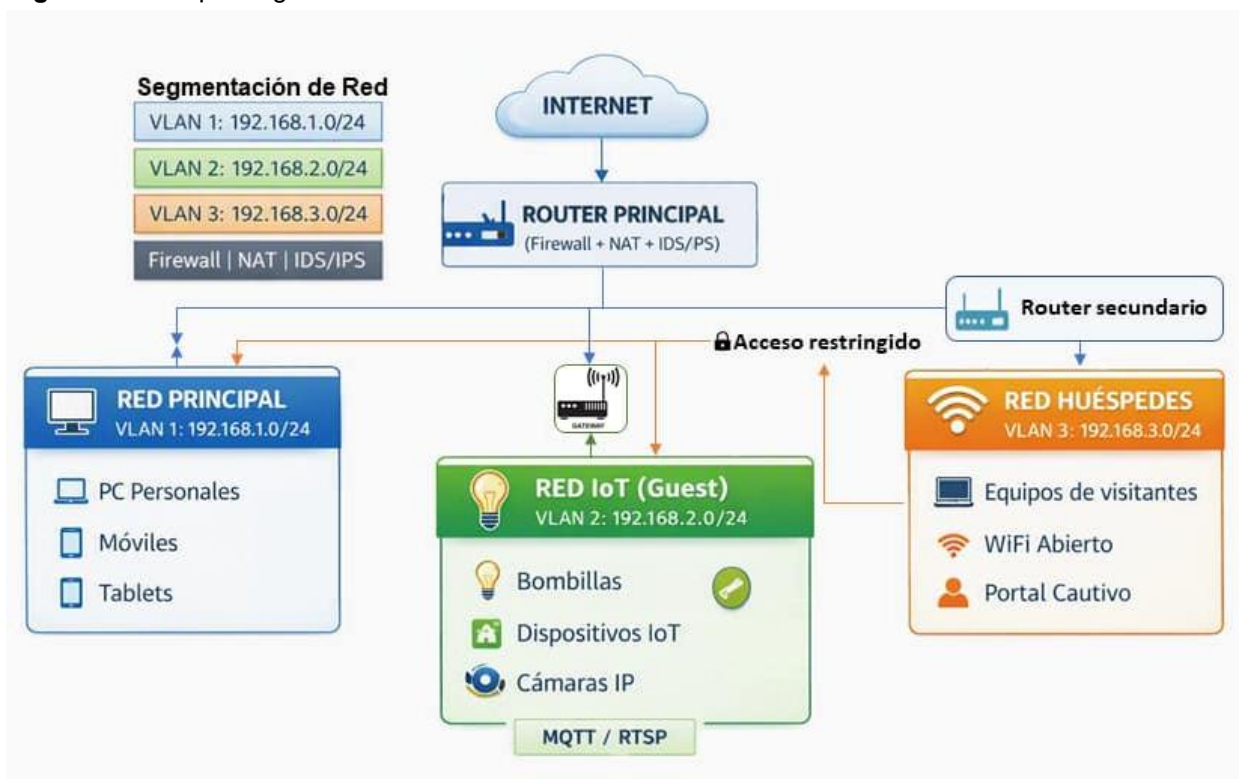


Nota: Un dispositivo comprometido puede intentar comunicarse con otros dispositivos.

Fuente: Autor.

Una arquitectura segmentada busca reducir la posibilidad de un atacante para ello el siguiente ejemplo muestra la representación de una red segmentada:

Figura 55. Red por segmentos.



Fuente: Autor.

Para dispositivos lot:

MQTT: es un protocolo de mensajería ligero y eficiente basado en el modelo de publicación y suscripción, diseñado especialmente para la comunicación entre dispositivos del Internet de las Cosas (IoT) con recursos o ancho de banda limitados.

RTSP: (Real Time Streaming Protocol o Protocolo de Transmisión en Tiempo Real) es un protocolo de red diseñado para controlar la entrega de datos multimedia en tiempo real, como audio y video. Ejemplos (Control remoto universal, Cámaras IP)

Red segmentada su funcionalidad antes ataques.

En una implementación avanzada puede incorporarse aislamiento entre clientes, VLAN, reglas de firewall y políticas que restrinjan qué dispositivos pueden comunicarse entre sí. La segmentación no elimina una vulnerabilidad. Su función es limitar el alcance del daño.

Si una bombilla es comprometida, el objetivo es que el atacante encuentre una barrera al intentar comunicarse con un ordenador personal. Este principio es especialmente importante debido a la naturaleza heterogénea de los hogares inteligentes.

Las investigaciones sobre sistemas de automatización doméstica muestran que la coexistencia de múltiples tecnologías y componentes genera numerosas superficies de ataque, por lo que proteger solamente el dispositivo final es insuficiente (Wang et al., 2022).

Router como punto de control.

El router debe considerarse una pieza estratégica del modelo porque conecta la vivienda con redes externas y dependiendo de la configuración, puede constituir uno de los principales puntos de concentración del tráfico entre dispositivos y la salida a internet.

En redes domesticas es normal encontrarnos con un solo dispositivo router el cual acompañado del centro de control para dispositivos IoT o Smart Hub es un complemento más que suficiente para mantener un control de seguridad estricto y

confiable siempre y cuando se apliquen las normas de seguridad y los parámetros seguros de ambos dispositivos.

Si bien los router otorgados temporalmente o comprados a las empresas de servicio de internet ya suelen venir configurados con estándares de seguridad, generalmente el usuario no tiene acceso a su dispositivo sin la opción de “restablecer de fábrica”.

Ya que esto si bien recuperaría el acceso del usuario también restablecería los parámetros de la empresa prestadora del servicio y con la posibilidad de dejar sin conexión a internet del usuario.

Por este motivo de ser requerido una segmentación de red para mayor seguridad el camino más fácil a seguir es adquirir un dispositivo router adicional con el cual el usuario tendrá mayor control de su red en el hogar.

Adicionalmente. No debe interpretarse, por ejemplo, la configuración de seguridad inalámbrica WPA2 o WPA3 que resuelven todos los problemas de seguridad del hogar. El cifrado del enlace inalámbrico protege determinadas comunicaciones, pero no sustituye el cifrado aplicado por las propias aplicaciones o protocolos.

Además, investigaciones recientes muestran que incluso el tráfico cifrado puede revelar información mediante patrones y metadatos (Li et al., 2023; Radovanovic et al., 2026).

A continuación, y para una configuración de seguridad en la siguiente tabla se da a conocer los parámetros para su configuración. Los controles mínimos y avanzados propuestos son:

Tabla 18. controles de configuración y descripción.

Control	Función
Contraseña administrativa única	Evitar acceso a la configuración
WPA2/WPA3	Proteger el acceso inalámbrico
Firmware actualizado	Reducir vulnerabilidades conocidas
Firewall	Controlar tráfico no autorizado
Segmentación	Aislar grupos de dispositivos
Desactivación de funciones innecesarias	Reducir superficie de ataque
Registro de eventos	Facilitar investigación
Controles avanzados	Función
Autenticación multifactor (MFA)	Aumentar seguridad en accesos críticos
Listas de control de acceso (ACLs)	Definir qué dispositivos/usuarios pueden comunicarse
VPN para acceso remoto	Cifrar y proteger conexiones externas
IDS/IPS (detección y prevención de intrusos)	Identificar y bloquear ataques en tiempo real
Actualización automática de parches	Minimizar exposición a exploits recientes
Cifrado de datos en tránsito (TLS/SSL)	Proteger información sensible en comunicaciones
Monitoreo continuo	Detectar anomalías y comportamientos sospechosos
Políticas de respaldo	Garantizar recuperación ante incidentes

Notas prácticas: Tabla elaborada por el autor;

- En entornos domésticos, lo más realista es aplicar MFA, VPN y firmware actualizado.
- En entornos corporativos, se vuelve crítico añadir IDS/IPS, ACLs y monitoreo continuo.
- El respaldo suele olvidarse, pero es clave para resiliencia frente a ransomware o fallos.

Capa 4: Factor humano.

Una arquitectura de seguridad técnicamente sólida puede fallar si las personas que utilizan el sistema toman decisiones inseguras. El usuario realiza acciones que afectan directamente a la seguridad:

- instala dispositivos.
- establece contraseñas.
- acepta permisos.
- conecta equipos desconocidos.
- ignora advertencias.
- decide cuándo actualizar.
- determina si un dispositivo antiguo continúa conectado.

Por tanto, el usuario no debe considerarse simplemente "el eslabón débil", también puede convertirse en un componente activo de defensa.

Una investigación sobre dispositivos IoT de consumo encontró que la información proporcionada en manuales y páginas de soporte no siempre ofrece orientación suficiente sobre prácticas de seguridad para consumidores, destacando la necesidad de mejorar la comunicación de la seguridad al usuario final (Ur et al., 2019).

Transformación del usuario; el modelo propone pasar de: Usuario = posible fuente de error a: el Usuario Identifica dispositivos, Cambia credenciales, Instala actualizaciones, Reconoce alertas, Revisa permisos, Reporta anomalías dando como resultado Usuario = control de seguridad. Siempre y cuando se cumplan las normas.

Principio de decisión sencilla.

Las recomendaciones deben poder comprenderse sin conocimientos de redes o instalaciones y usos complejas. Por ejemplo, de un problema muy común: "El dispositivo utiliza la contraseña admin/admin."

Explicación técnica: "Existe una credencial universal predeterminada susceptible de ataques automatizados.", para personal especializado en la rama técnica y tecnológica esta descripción es lo más normal del caso, pero para un usuario normal no termina de entender a que se referirá con credencial universal predeterminada.

La simple palabra de "credencial" ya es suficiente para agobiar a una persona que no dispone de conocimientos en jerga técnica de tal manera un manual debe de ser lo más claro y sencillo respecto a usuarios sin conocimientos especializados.

Explicación para el usuario: "La misma contraseña puede ser conocida por un atacante. Debes cambiarla." Este principio de traducción es fundamental para que el modelo resulte aplicable en hogares donde no existe personal especializado.

Ya que la gran brecha de vulnerabilidad o riesgo no se da por una mayor complejidad y determinación de un atacante para encontrarla y llevarla a cabo, si no la falta de simplicidad para con el usuario final el cual puede no entender de jerga técnica y complejidad de los manuales.

En resumen, la explicación para un usuario final en un manual debe ser clara, sencilla y directa y de ser necesario acompañada de apoyo visual, evitando tecnicismos innecesarios para que cualquier persona pueda entender y usar el producto sin frustración.

Capa 5: Gobernanza y educación.

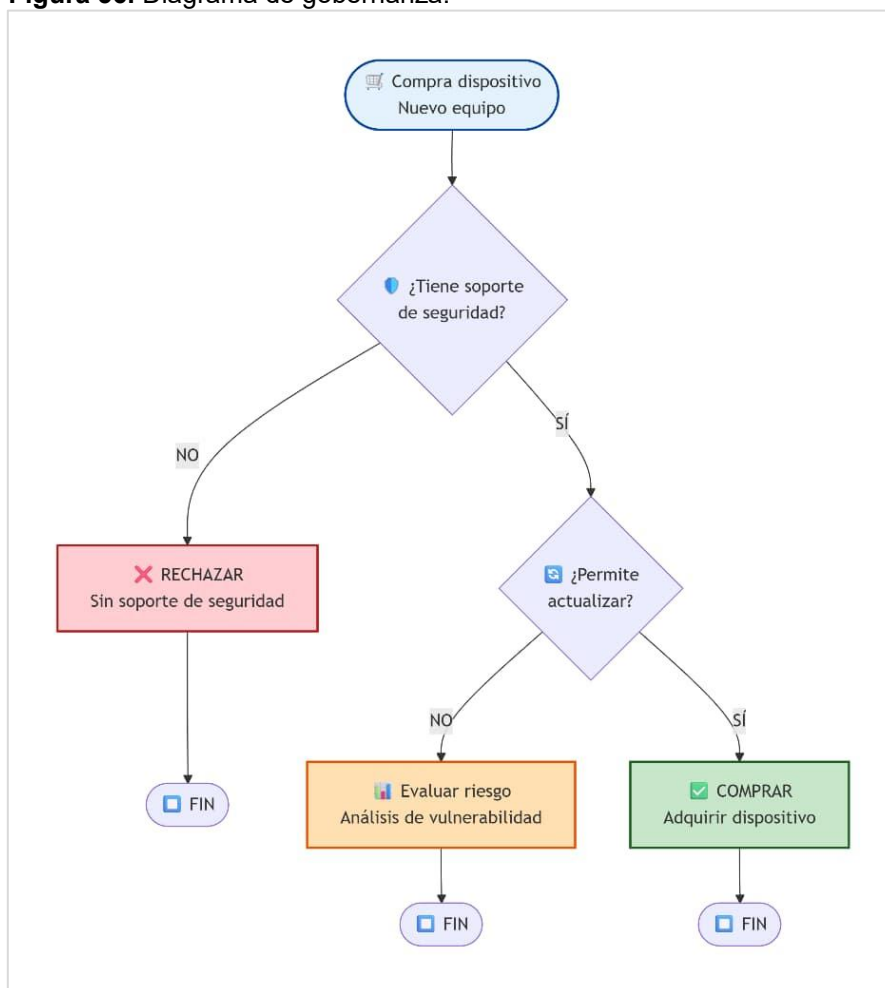
La quinta capa funciona como elemento transversal, su función consiste en establecer y preguntarse:

- quién administra los dispositivos: ¿quién es la persona o grupo de personas encargada de administrar dichos dispositivos en el hogar?
- qué dispositivos pueden incorporarse: ¿qué dispositivos son relevantes para el hogar y cuales merecen mayor atención y cuáles no?
- qué requisitos deben cumplir: ¿qué normativas de seguridad cumplen estos dispositivos?
- cuando deben actualizarse: ¿cómo y cada cuanto hay actualizaciones en los dispositivos?
- qué hacer cuando un dispositivo deja de recibir soporte: ¿cuál es el tiempo de soporte y actualizaciones de seguridad de los dispositivos?
- cómo registrar incidentes: ¿el fabricante cuenta con línea de soporte para incidentes?
- cuando reemplazar un equipo: No solo se reemplaza cuando el dispositivo presenta fallas, si el dispositivo es parte de las funciones de seguridad o de si es comprometido y el fabricante no brinda soporte al mismo para su solución de inseguridad.

Aquí resulta especialmente útil NIST CSF 2.0 porque incorpora Govern como función formal. Esta función aborda la estrategia, las políticas, los roles, las responsabilidades y la supervisión del riesgo (Pascoe et al., 2024). La gobernanza evita que la seguridad dependa únicamente de decisiones improvisadas.

Por ejemplo: el siguiente diagrama de muestra.

Figura 56. Diagrama de gobernanza.



Fuente: Autor.

Este mecanismo puede ampliarse hasta convertirse en una pequeña política de adquisición de tecnología para el hogar.

4.9.4. Gestión de dispositivos y sus riesgos dentro del modelo.

Una de las principales mejoras propuestas respecto al modelo inicial consiste en incorporar formalmente la gestión de riesgos complementando la matriz inicial de

factores de riesgo en hardware y software, no todos los dispositivos tienen el mismo impacto.

Por ejemplo: “véase Tabla 16. Matriz de Factores de riesgo. Pag 89” adicional como complemento para la siguiente tabla:

Tabla 19. Factores de riesgo tabla adicional.

Dispositivo	Probabilidad	Impacto	Riesgo aproximado
 Bombilla inteligente	Media	Bajo	Medio-bajo
 Sensor de temperatura	Media	Bajo	Medio-bajo
 Smart TV	Media	Medio	Medio
 Cámara IP	Alta	Alto	Alto
 Cerradura inteligente	Media	Muy alto	Alto
 Router	Alta	Muy alto	Critico

Nota: Tabla elaborada por el autor.

La clasificación no pretende establecer un valor universal para todos los hogares este debe de adaptarse al contexto. Una cámara puede tener un impacto superior al de una bombilla porque puede afectar directamente la privacidad, una cerradura inteligente puede presentar un impacto aún mayor porque su compromiso puede relacionarse con el acceso físico a una vivienda.

La investigación sobre riesgos de hogares inteligentes confirma que los sistemas IoT pueden generar consecuencias que trascienden la pérdida de información y afectan la privacidad y seguridad física de los residentes (Sadeghi et al., 2015).

Inventario y gestión de dispositivos: Antes de proteger un sistema, es necesario conocer qué se está protegiendo y cuantos dispositivos hay en el hogar, para esto el modelo presente propone mantener un inventario de los dispositivos y una gestión limpia de los mismos, aquí un ejemplo de gestión:

Figura 57. Ejemplo de gestión de dispositivo.

Campo	Ejemplo
Dispositivo	Cámara frontal
Fabricante	Fabricante X
Modelo	CAM-01
Dirección/IP	192.168.50.20
Red	IoT
Función	Videovigilancia
Datos manejados	Imagen/video
Usuario administrador	Sí
Última actualización	Fecha
Estado	Activo
Nivel de riesgo	Alto

Fuente: Autor.

Este inventario permite identificar rápidamente dispositivos olvidados, equipos antiguos o componentes que continúan utilizando configuraciones inseguras. NISTIR 8425 establece precisamente una línea de referencia orientada a productos

IoT de consumo y sus capacidades de ciberseguridad, lo cual resulta adecuado para construir criterios de inventario, gestión y evaluación dentro del hogar (Megs et al., 2022).

4.9.5. Motor de evaluación del modelo.

Para hacer que el modelo pueda ser evaluable, se propone asignar a cada dispositivo una puntuación de seguridad proponiendo una formula conceptual, Formula conceptual propuesta $[R = P \times I]$ donde:

(R) =es nivel de riesgo;

(P) = es probabilidad de explotación;

(I) =es impacto sobre el hogar.

Ambos factores se evaluarán en una escala de 1 a 5. Por ejemplo: $R = [4 \times 5 = 20]$

Podemos clasificar entonces que si: $R = 20$ entonces el riesgo es critico

Tabla 20. Matriz Evaluativa.

Probabilidad:	Impacto:	Matriz de evaluación.	
1 = Muy baja 2 = Baja 3 = Media 4 = Alta 5 = Muy alta	1 = Muy bajo 2 = Bajo 3 = Medio 4 = Alto 5 = Crítico	$P \times I$	Clasificación
		1 – 4	Bajo
		5 – 9	Medio
		10 – 15	Alto
		16 – 25	Crítico

Nota: Tabla elaborada por el autor. Esta clasificación constituye una herramienta metodológica para el desarrollo de este modelo propuesto y no debe presentarse como una escala establecida por ISO o NIST. El motor de evaluación calcula y decide el nivel de riesgo de una vulnerabilidad.

4.9.6. Integración con NIST CSF 2.0.

Las cinco capas de este modelo y las seis funciones del NIST CSF 2.0 no deben considerarse estructuras rivales La principal ventaja de esta integración es que el modelo deja de considerar la seguridad como una acción puntual.

- Las capas responden a: ¿Dónde aplicamos seguridad?
- Las funciones responden a: ¿Qué hacemos con el riesgo?

Esto convierte el modelo en un ciclo, la integración propuesta es:

Tabla 21. Integración NIST con el modelo propuesto.

NIST CSF 2.0	Aplicación en el modelo
Govern (gobernanza)	Políticas, responsables y criterios.
Identify (Identificar)	Inventario y análisis de riesgos.
Protect (Proteger)	Controles de hardware, software y red.
Detect (Detectar)	Monitoreo y detección de anomalías.
Respond (Responder)	Contención y gestión del incidente.
Recover (Recuperar)	Restauración y aprendizaje.

Nota: Tabla elaborada por el autor.

Sistema de detección de intrusiones doméstico.

Una evolución natural del modelo consiste en incorporar un sistema de detección de intrusiones o IDS doméstico. “Un IDS doméstico (Sistema de Detección de Intrusos, por sus siglas en inglés)” es un software o dispositivo diseñado para monitorear el tráfico de la red en el hogar y alertar sobre actividades sospechosas o maliciosas.

A diferencia de un firewall, que bloquea el tráfico basándose en reglas, el IDS actúa como una cámara de seguridad: analiza lo que pasa y da la alarma si detecta comportamientos extraños o ataques informáticos conocidos. De ese modo el IDS puede observar:

- dispositivos nuevos.
- cambios de comportamiento.
- intentos repetidos de autenticación.

- comunicaciones hacia destinos inesperados.
- protocolos inseguros.
- tráfico anómalo.
- actividad fuera del patrón normal.

No necesariamente debe analizar todo el contenido de las comunicaciones. Su objetivo principal puede ser identificar: "Esto no se comporta como debería comportarse este dispositivo."

respuesta ante incidentes: La protección no termina cuando se detecta un ataque el modelo propuesto y acompañado de la integrado con el NIST, propone cinco pasos simplificados:

Figura 58. Pasos simplificados.

Detección: Determinar que existe un comportamiento potencialmente anómalo.

Verificación: Comprobar que el evento no constituye simplemente un comportamiento legítimo.

Contención: Aislar el dispositivo o limitar su comunicación.

Recuperación: Restaurar el dispositivo a un estado confiable, mediante actualización, reinstalación o restauración.

Aprendizaje: Registrar qué ocurrió y modificar los controles para reducir la posibilidad de repetición.

Fuente: Autor.

Esta filosofía coincide con la orientación general de NIST CSF 2.0 hacia detectar, responder y recuperar, evitando que la seguridad se limite exclusivamente a la prevención (Pascoe et al., 2024).

4.9.7. Indicadores para evaluar el modelo final.

Para demostrar experimentalmente que el modelo funciona, es necesario utilizar indicadores medibles. A continuación, se proponen los siguientes:

Porcentaje de dispositivos correctamente identificados “PCI”: $PCI = \frac{R}{D} \times 100$ donde:

- R = dispositivos registrados
- D = dispositivos detectados

Un resultado cercano al 100% indica que el inventario refleja de forma adecuada la infraestructura existente.

Tasa de detección “TD”: $TD = \frac{Vp}{Vp+Fn} \times 100$ donde:

- Vp = verdaderos positivos;
- Fn = falsos negativos.

Tasa de falsos positivos “TFP”: $TFP = \frac{FP}{FP+Vn} \times 100$ donde:

- FP = Falsos positivos
- Vn = Verdaderos negativos

Esto es importante porque un sistema que genera demasiadas alertas falsas puede terminar siendo ignorado por el usuario.

Tiempo de detección “TDD”: $TDD = T_{deteccion} - T_{inicio}$ donde:

- T_d = Tiempo de detección

- T_i = Tiempo de inicio

Permite conocer cuánto tiempo tarda el modelo en reconocer un comportamiento anómalo.

Tiempo de respuesta “TTR”: $TDD = T_{mitigacion} - T_{deteccion}$ donde:

- T_m = Tiempo de mitigación
- T_d = Tiempo de detección

Para que el modelo sea eficiente debería reducir este intervalo.

Casos de prueba del modelo.

La arquitectura propuesta permite definir casos concretos. Esta matriz de caso puede utilizarse posteriormente para construir la sección experimental del proyecto:

Tabla 22. Matriz de caso.

Caso “Cs”	Condición	Respuesta esperada
Cs-01	Credencial predeterminada	Alerta y solicitud de cambio
Cs-02	Intentos repetitivos de autenticación	Detección y bloqueo/limitación
Cs-03	Comunicación sin protección	Alerta de protocolo inseguro
Cs-04	Firmware no confiable	Rechazo de instalación
Cs-05	Dispositivo desconocido	Alerta y clasificación
Cs-06	Dispositivo IoT intenta acceder a red principal	Bloqueo o alerta
Cs-07	Cambio inesperado de comportamiento	Generación de evento
Cs-08	Dispositivo comprometido	Aislamiento
Cs-09	Recuperación a firmware conocido	Restauración
Cs-10	Dispositivo sin soporte	Clasificación como riesgo elevado

Nota: Tabla elaborada por el autor. Los indicadores miden qué tan bien está funcionando el modelo final, la matriz de casos se usa como complemento para la respuesta esperada de los resultados en los indicadores de evaluación.

Relación entre las vulnerabilidades y los controles.

La ventaja de este planteamiento es que una misma amenaza puede ser mitigada por más de una capa. Las tres vulnerabilidades principales estudiadas con anterioridad en la etapa: 4.7 página 92 título “Construcción de un entorno de simulación para la fase de pruebas y test de funcionalidad”, pueden integrarse de la siguiente forma:

Tabla 23. Tabla de resultados de vulnerabilidad.

Vulnerabilidad	Capa principal	Controles
Credenciales predeterminadas	Software / Humano	Cambio obligatorio, autenticación robusta, registro
Datos sin cifrar	Software / Red	TLS/DTLS, protocolos seguros, monitoreo
Firmware inseguro	Software / Hardware	Firma, integridad, secure boot, recuperación

Nota: Tabla elaborada por el autor.

Por ejemplo, una credencial comprometida puede encontrarse con:

- autenticación fortalecida.
- segmentación de red.
- detección de comportamiento.
- alerta al usuario.
- procedimiento de respuesta.

Esto constituye defensa en profundidad.

4.9.8. Seguridad durante todo el ciclo de vida del dispositivo.

Figura 59. Ciclo de vida.



Fuente: Autor.

Una mejora importante respecto al modelo inicial consiste en considerar que un dispositivo no es seguro únicamente el día de su instalación.

Su ciclo puede representarse así: “Figura 59”

NIST ha desarrollado precisamente una serie de publicaciones para abordar las actividades de ciberseguridad de los fabricantes durante la concepción, desarrollo, prueba, comercialización y soporte de productos IoT (Fagan et al., 2026).

Esto significa que el modelo propuesto debe preguntarse continuamente:

- ¿El dispositivo sigue siendo seguro hoy?

y no solamente:

- ¿Era seguro cuando lo compré?

Fin de soporte y dispositivos obsoletos: Una de las amenazas menos visibles para el usuario es el dispositivo que continúa funcionando correctamente, pero ya no recibe actualizaciones, desde la perspectiva funcional puede parecer que no existe ningún problema.

Ejemplo: **Cámara** → funciona, **TV** → funciona, **Router** → funciona, **Sensor** → funciona

Sin embargo, desde la perspectiva de seguridad puede ocurrir.

Ejemplo: **Cámara → funciona + vulnerabilidad sin parche, TV → funciona + firmware antiguo, Router → funciona + vulnerabilidad conocida.**

En consecuencia, el modelo debe diferenciar entre funcionalidad y seguridad, un dispositivo puede funcionar perfectamente y, simultáneamente, representar un riesgo elevado.

El informe 2025 de Bitdefender y NETGEAR, por ejemplo, reportó 22 dispositivos conectados por hogar y aproximadamente 29 ataques diarios promedio sobre hogares monitorizados, además de señalar que 99,4 % de los intentos de explotación observados estaban dirigidos a vulnerabilidades ya conocidas y corregidas.

Estas cifras deben interpretarse como telemetría de un proveedor de seguridad, no como una medición universal de todos los hogares del mundo; aun así, son útiles para ilustrar la importancia de mantener los dispositivos actualizados (Bitdefender, 2025).

Etiquetado y adquisición segura: Otra mejora consiste en convertir la seguridad en un criterio de compra para ello el comprador debería conocer antes de adquirir un dispositivo.

- cuánto tiempo recibirá actualizaciones.
- cómo se realizan las actualizaciones.
- cómo se protegen las comunicaciones.
- qué mecanismos de autenticación utiliza.

- qué información recopila.
- qué soporte ofrece el fabricante.
- cómo se reportan vulnerabilidades.

ISO/IEC 27404:2025 establece un marco internacional para programas de etiquetado de ciberseguridad para productos IoT de consumo. El estándar incluye aspectos relacionados con riesgos y amenazas, responsabilidades, evaluación de conformidad, emisión y mantenimiento del etiquetado (ISO, 2025). Por ello, el etiquetado puede integrarse en el modelo como un mecanismo de decisión previo a la adquisición.

Gestión de vulnerabilidades y comunicación con fabricantes: El modelo Final no debería considerar que el descubrimiento de una vulnerabilidad representa el final del proceso si no que a su vez estas vulnerabilidades puedan ser reportadas.

Según la normativa ISO/IEC 29147:2018 proporciona orientación sobre divulgación de vulnerabilidades, mientras que ISO/IEC 30111:2019 aborda los procesos para gestionar y remediar vulnerabilidades reportadas en productos o servicios (ISO, 2018, 2019).

Estas normas pueden ser especialmente útiles para ampliar el modelo en contextos donde participen integradores, fabricantes o proveedores de servicios.

4.9.9. Principios fundamentales del modelo.

A partir de la arquitectura desarrollada en este modelo, se establecen diez (10) principios:

Tabla 24. Principios

Principio 1. Conocer antes de proteger	No puede protegerse adecuadamente un dispositivo que no se conoce o que no figura en el inventario.
Principio 2. Seguridad desde el origen	Las características de seguridad deben evaluarse antes de adquirir el dispositivo, no únicamente después de sufrir un incidente.
Principio 3. No confiar en credenciales universales	Una contraseña de fábrica predecible debe considerarse una condición insegura.
Principio 4. Proteger la información durante su transmisión	Los datos sensibles deben transmitirse mediante mecanismos de protección adecuados al dispositivo y protocolo.
Principio 5. Mantener el software actualizado de forma segura	Una actualización solamente aumenta la seguridad cuando su origen, integridad y proceso de instalación pueden confiarse.
Principio 6. Separar los dispositivos	Un dispositivo IoT no debería tener automáticamente el mismo nivel de acceso que un ordenador personal.
Principio 7. Detectar, no solamente prevenir	La seguridad debe asumir que eventualmente puede producirse un fallo o compromiso.
Principio 8. Limitar el impacto	Cuando un dispositivo se compromete, la arquitectura debe dificultar que el atacante se desplace hacia otros equipos.
Principio 9. Preparar la recuperación	Todo modelo de seguridad debe contemplar cómo volver a un estado confiable.
Principio 10. Mejorar continuamente	Los riesgos cambian, aparecen vulnerabilidades nuevas y los dispositivos envejecen; por tanto, el modelo debe reevaluarse periódicamente.

Nota: Tabla elaborada por el autor.

5. RESULTADOS

Síntesis de resultados.

Los principales resultados obtenidos durante el desarrollo conceptual y técnico del modelo pueden ser evidenciados en las etapas de construcción de dichos modelos como el modelo inicial y modelo final dentro del mismo desarrollo de este documento de ese modo los resultados obtenidos pueden sintetizarse así:

La combinación de estos resultados permite concluir que la propuesta supera el enfoque de una lista de recomendaciones independientes y presenta una estructura que puede ser implementada, evaluada y posteriormente mejorada.

Para dar paso a la síntesis de dichos resultados consulte la tabla Numero (25) “Resultado, Evidencia y fundamento” donde se evidenciarán los resultados, la evidencia que respalda a los mismos y su fundamento. Los resultados más relevantes o concluyentes se encontrarán justo debajo de la tabla.

Tabla 25. Resultado, evidencia y fundamento.

Resultado	Evidencia o fundamento
Arquitectura de cinco capas	Modelo integral desarrollado
Identificación de credenciales por defecto como riesgo	ETSI EN 303 645 + caso Mirai
Protección de comunicaciones	NISTIR 8259A + literatura smart home
Actualización segura del firmware	NISTIR 8259A + ETSI
Segmentación de red	Arquitectura defensiva + perfil NIST de routers
Evaluación mediante riesgo	Motor ($R=P \times I$)
Detección y respuesta	NIST CSF 2.0
Gestión durante el ciclo de vida	NISTIR 8259 Rev. 1
Participación del usuario	NIST y literatura sobre smart homes
Necesidad de mantenimiento continuo	Evidencia de telemetría 2025

Nota: Tabla elaborada por el autor.

Resultado general del desarrollo del modelo.

Como resultado del desarrollo del Modelo Integral de Ciberseguridad para el Hogar Inteligente, se obtuvo una propuesta de protección estructurada en cinco capas: seguridad de hardware, seguridad de software, seguridad de red, factor humano y gobernanza y educación.

Esta arquitectura permite abordar la seguridad del hogar inteligente desde diferentes puntos de vista, evitando que la protección dependa exclusivamente de un único mecanismo técnico. La estructura inicial del modelo ya planteaba estas cinco capas como una estrategia de defensa en profundidad.

El principal resultado de esta arquitectura es que una vulnerabilidad existente en un componente no implica necesariamente el compromiso inmediato de todo el sistema. Por ejemplo, si un sensor presenta una configuración insegura, la segmentación de red puede limitar sus comunicaciones;

Sí una credencial es comprometida, la autenticación y el monitoreo pueden detectar el comportamiento; y si un dispositivo deja de recibir actualizaciones, la gobernanza puede conducir a su aislamiento o sustitución.

Esta característica constituye uno de los aportes centrales del modelo: la seguridad se concibe como un conjunto de controles complementarios y no como una única barrera de protección.

La propuesta además puede relacionarse con el enfoque del NIST Cybersecurity Framework 2.0, que organiza la gestión del riesgo mediante las funciones Govern, Identify, Protect, Detect, Respond y Recover (Pascoe et al., 2024).

NIST señala que estas funciones deben entenderse como actividades continuas y concurrentes, proporcionando una perspectiva de ciclo de vida para la gestión del riesgo. Por lo tanto, el modelo desarrollado puede interpretarse mediante dos dimensiones complementarias:

Las cinco capas responden dónde se debe proteger; las funciones del NIST CSF 2.0 responden qué debe hacerse con el riesgo.

Resultado de la integración de normas y marcos de referencia.

Uno de los resultados más importantes fue la posibilidad de relacionar cada componente del modelo con estándares y marcos internacionales específicos. La ISO/IEC 27400:2022 proporciona directrices relacionadas con riesgos, principios y controles de seguridad y privacidad aplicables a soluciones IoT (ISO, 2022a).

A su vez, ISO/IEC 27402:2023 proporciona requisitos básicos de seguridad y privacidad para dispositivos IoT, permitiendo utilizar un referente específicamente orientado al componente físico y lógico del dispositivo (ISO, 2023).

El modelo también se relaciona con NISTIR 8259A, que establece capacidades técnicas para dispositivos IoT, entre ellas identificación del dispositivo, configuración, protección de datos, control de acceso lógico, actualización de software, conocimiento del estado de ciberseguridad y seguridad del dispositivo (Fagan et al., 2020).

Finalmente, ETSI EN 303 645 proporciona requisitos particularmente relevantes para IoT de consumo. Por ejemplo, establece que, fuera del estado de fábrica, las contraseñas utilizadas por dispositivos IoT deben ser únicas por dispositivo o definidas por el usuario, eliminando la práctica de utilizar contraseñas universales como admin/admin (ETSI, 2024).

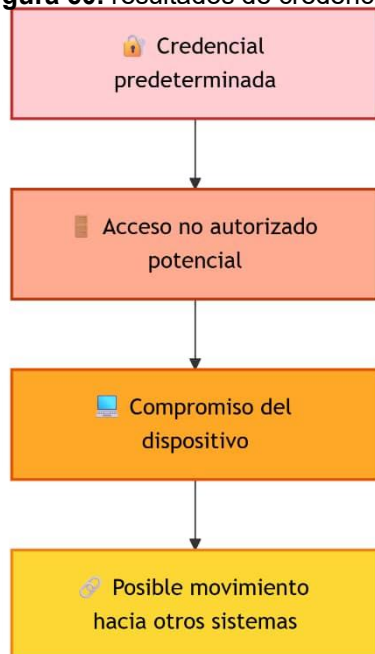
Como resultado, el modelo no se queda únicamente en fundamentos con recomendaciones generales, sino que cuenta con referencias y seguimiento a estándares internacionales reconocidos.

Resultado sobre las credenciales predeterminadas.

Uno de los primeros resultados obtenidos fue la identificación de las credenciales predeterminadas o débiles como una vulnerabilidad prioritaria.

El modelo establece que un dispositivo que conserve credenciales universales o fácilmente predecibles debe ser considerado inseguro hasta que se modifique dicha configuración. Esta decisión encuentra respaldo directo en ETSI EN 303 645, que establece la prohibición de contraseñas universales predeterminadas para dispositivos IoT de consumo y menciona explícitamente ejemplos como admin/admin (ETSI, 2024).

Figura 60. resultados de credenciales.



Fuente: Autor.

La relevancia de este control no es exclusivamente teórica. Antonakakis et al. (2017), al analizar la botnet Mirai, documentaron cómo el uso de credenciales conocidas permitió a esta infraestructura comprometer un gran número de dispositivos IoT. El caso demostró que una debilidad aparentemente simple puede convertirse en un mecanismo de compromiso automatizado a gran escala.

El resultado de esta parte del modelo es la incorporación de un control preventivo obligatorio: comprobar las credenciales durante la configuración inicial y exigir su modificación cuando corresponda.

Resultado sobre la protección de las comunicaciones.

El segundo resultado corresponde a la incorporación de la protección de los datos transmitidos entre dispositivos.

El modelo identificó que no basta con proteger el dispositivo individual. También debe protegerse la información mientras circula por la red. Esto resulta especialmente relevante en los hogares inteligentes, donde sensores y dispositivos intercambian constantemente datos sobre movimiento, temperatura, presencia, actividad y otros elementos del entorno doméstico.

La investigación reciente confirma que la seguridad de las comunicaciones sigue siendo un componente fundamental de los sistemas smart home. Una revisión sistemática de la seguridad de hogares inteligentes analizó (233) fuentes publicadas entre 2018 y mayo de 2025 y concluyó que la protección escalable del hogar requiere abordar simultáneamente los siguientes parámetros.

Como protocolos, privacidad, detección y mecanismos de defensa, en lugar de depender de una única solución técnica (Radovanovic et al., 2026).

Como resultado, el modelo establece la necesidad de identificar comunicaciones inseguras y, cuando el protocolo y las características del dispositivo lo permitan, utilizar mecanismos adecuados de protección criptográfica.

La protección también se relaciona con NISTIR 8259A, que incorpora la protección de datos como una de las capacidades técnicas fundamentales de un dispositivo IoT (Fagan et al., 2020).

La conclusión obtenida es que la seguridad del hogar no puede evaluarse solamente preguntando: "¿El dispositivo tiene contraseña?" También debe preguntarse: "¿Qué ocurre con la información después de que el usuario se autentica?".

Resultado sobre las actualizaciones y el firmware.

El tercer resultado importante fue la identificación de la actualización segura del firmware como condición necesaria para conservar la seguridad a lo largo del tiempo. El modelo estableció que la actualización debe comprenderse como un proceso completo, no simplemente como la descarga de un archivo.

La cadena de confianza propuesta es: véase “**Figura53**. Diagrama de actualización pagina 138”

Esta estructura coincide con la orientación de NIST, que considera la actualización de software una de las capacidades técnicas fundamentales de los dispositivos IoT (Fagan et al., 2020).

También coincide con la evolución de las recomendaciones dirigidas a fabricantes. La versión actual de la serie NISTIR 8259, NISTIR 8259 Rev. 1, publicada en abril de 2026, sustituye la edición anterior de NISTIR 8259 y señala que los fabricantes deben mejorar la capacidad de sus productos para que los clientes puedan mitigar sus riesgos de ciberseguridad (Fagan et al., 2026).

En consecuencia, el modelo identifica una condición importante: un dispositivo que funciona correctamente no necesariamente es un dispositivo seguro. Si dejó de

recibir actualizaciones o contiene vulnerabilidades conocidas sin corregir, su funcionamiento normal no elimina el riesgo.

Resultado frente al escenario actual de amenazas.

Los datos actuales muestran que la protección de los hogares inteligentes no constituye una preocupación puramente hipotética.

Bitdefender y NETGEAR reportaron en 2025, a partir de telemetría de millones de hogares inteligentes en varios continentes, un promedio de 22 dispositivos conectados por hogar y aproximadamente 29 ataques IoT diarios, frente a 10 ataques diarios reportados el año anterior. El mismo informe indicó que el 99,4 % de las explotaciones observadas estaban dirigidas contra CVE ya conocidas y corregidas (Bitdefender, 2025).

Estas cifras no deben interpretarse como si todos los hogares del mundo recibieran exactamente 29 ataques diarios, ya que corresponden a la telemetría utilizada en ese estudio. Sin embargo, sí proporcionan evidencia de que existe una exposición considerable y que una parte importante de los ataques está relacionada con problemas que ya cuentan con soluciones disponibles.

Este resultado respalda uno de los principios fundamentales del modelo:

la gestión continua de dispositivos y la aplicación oportuna de actualizaciones no son actividades opcionales, sino componentes centrales de la reducción del riesgo.

6. CONCLUSIONES

El hogar inteligente debe entenderse como un sistema interconectado y no como una colección de aparatos independientes. Esta característica proporciona beneficios importantes en términos de automatización, comodidad y control, pero también genera una superficie de ataque distribuida que puede abarcar desde el hardware del dispositivo hasta las decisiones del usuario.

El modelo integral desarrollado aborda esta problemática mediante cinco capas de seguridad: hardware, software, red, factor humano y gobernanza. Estas capas se complementan con un ciclo de gestión compuesto por gobernar, identificar, proteger, detectar, responder y recuperar, tomando como referencia el NIST Cybersecurity Framework 2.0 (Pascoe et al., 2024).

El análisis realizado demuestra además que las vulnerabilidades seleccionadas inicialmente tales como credenciales predeterminadas, comunicaciones sin protección y actualizaciones inseguras estas vulnerabilidades poseen precedentes y correspondencia directa con problemas reconocidos por estándares y organismos especializados.

ETSI EN 303 645 establece requisitos específicos para eliminar las contraseñas universales predeterminadas; NISTIR 8259A establece capacidades técnicas fundamentales para dispositivos IoT; ISO/IEC 27400 proporciona directrices sobre seguridad y privacidad de soluciones IoT; y ISO/IEC 27402 proporciona requisitos básicos específicos para dispositivos IoT (ETSI, 2024; Fagan et al., 2020; ISO, 2022a, 2023).

La importancia de estos controles está respaldada por estándares especializados como ISO/IEC 27400:2022, ISO/IEC 27402:2023 y ETSI EN 303 645, así como por las capacidades técnicas establecidas por NISTIR 8259A (ISO, 2022a, 2023; Fagan et al., 2020; ETSI, 2024).

Los datos recientes sobre el panorama de amenazas refuerzan la necesidad de esta arquitectura. El informe conjunto de Bitdefender y NETGEAR de 2025 registró 22 dispositivos conectados por hogar y una media de 29 ataques IoT diarios en la telemetría analizada, además de indicar que el 99,4 % de los exploits observados se dirigía a vulnerabilidades ya conocidas y corregidas (Bitdefender, 2025).

A partir de estos resultados, la recomendación principal es abandonar el enfoque de seguridad basado exclusivamente en la instalación inicial del dispositivo. Un hogar inteligente requiere una estrategia continua que contemple inventario, configuración, autenticación, protección de comunicaciones, actualizaciones, segmentación, monitoreo, respuesta y reemplazo de equipos que hayan alcanzado el final de su ciclo de soporte.

Una característica fundamental de la propuesta es que no busca garantizar una seguridad absoluta, sino establecer defensa en profundidad y resiliencia. En consecuencia, cuando un control falla, los demás deben reducir la probabilidad de que el incidente alcance otros componentes y facilitar la recuperación.

El resultado es un modelo que puede utilizarse tanto como guía práctica para una vivienda inteligente como marco conceptual para el desarrollo de pruebas experimentales. Su estructura permite asociar cada vulnerabilidad con un control, cada control con una capa de seguridad y cada capa con un mecanismo de evaluación.

Esto facilita posteriormente demostrar mediante pruebas funcionales y escenarios controlados si el modelo propuesto consigue detectar las vulnerabilidades, generar alertas, aplicar medidas de mitigación y recuperar el sistema después de un incidente.

En este sentido, la seguridad deja de considerarse una condición estática y pasa a entenderse como un proceso continuo de evaluación, protección, detección, respuesta y mejora.

7. RECOMENDACIONES

7.1. Recomendaciones para fabricantes e integradores.

Los resultados también muestran que la seguridad no puede trasladarse completamente al usuario.

NISTIR 8259 Rev. 1 señala que los fabricantes deben realizar actividades de ciberseguridad durante el desarrollo del producto para aumentar la capacidad de los dispositivos de ser protegidos y reducir el esfuerzo que posteriormente recae sobre los clientes (Fagan et al., 2026).

Por ello se recomienda a los fabricantes:

- eliminar credenciales universales.
- incorporar mecanismos seguros de actualización.
- proporcionar soporte durante un periodo definido.
- documentar las capacidades de seguridad.
- facilitar la notificación de vulnerabilidades.
- proporcionar información clara al consumidor.
- implementar mecanismos de protección de datos.

También resulta conveniente adoptar procesos coordinados de divulgación y gestión de vulnerabilidades. ETSI ha destacado que disponer de un mecanismo de divulgación coordinada de vulnerabilidades es importante para mantener la seguridad después de que el producto llega al mercado.

7.2. Recomendación sobre dispositivos sin soporte.

Debe establecerse una política de reemplazo para dispositivos que ya no reciben actualizaciones de seguridad. El hecho de que un dispositivo todavía funcione no significa que continúe ofreciendo un nivel de seguridad aceptable.

El crecimiento de la cantidad de dispositivos conectados y la observación de ataques contra vulnerabilidades ya conocidas refuerzan esta recomendación. El informe Bitdefender/NETGEAR de 2025 encontró que la gran mayoría de los exploits observados apuntaba a vulnerabilidades conocidas y corregidas (Bitdefender, 2025).

Por ello: “Dispositivo funcional + sin soporte de seguridad $\neq$ dispositivo seguro.”

7.3. Recomendación para las actualizaciones

Las actualizaciones deben realizarse de manera periódica, pero también deben ser seguras, no basta con preguntar:

"¿El dispositivo tiene actualizaciones?"

También debe preguntarse:

"¿Cómo sabe el dispositivo que la actualización es legítima?"

"¿La actualización es oficial del fabricante o un tercero asociado?"

La actualización segura debe incorporar, según el diseño del dispositivo:

- fuente confiable.
- comunicación protegida.
- autenticidad.
- integridad.
- control de versiones.
- mecanismos de recuperación.
- arranque desde software confiable.

La reciente NISTIR 8259 Rev. 1 refuerza la importancia de que los fabricantes proporcionen productos suficientemente seguros para que los usuarios puedan gestionar sus riesgos durante el ciclo de vida (Fagan et al., 2026).

7.4. Recomendación para eliminar credenciales predeterminadas

Debe establecerse como política que ningún dispositivo permanezca con credenciales universales de fábrica después de la configuración inicial. Esta recomendación posee respaldo especialmente fuerte en ETSI EN 303 645, que prohíbe el uso continuado de contraseñas universales predeterminadas en dispositivos IoT de consumo (ETSI, 2024).

Se recomienda:

- 1 cambiar la contraseña durante la instalación.
- 2 utilizar credenciales únicas.
- 3 evitar reutilizar la misma contraseña entre dispositivos.

4 utilizar MFA cuando esté disponible.

5 deshabilitar mecanismos de acceso remoto que no sean necesarios.

7.5. Recomendaciones para futuras versiones del modelo

El modelo desarrollado puede continuar evolucionando mediante la incorporación de nuevas capacidades, la primera evolución recomendable es convertir el inventario en un sistema automatizado capaz de detectar dispositivos nuevos.

La segunda consiste en implementar un IDS doméstico que analice el comportamiento de los dispositivos, la tercera consiste en incorporar una base de datos de vulnerabilidades para relacionar automáticamente dispositivos y versiones de firmware con vulnerabilidades conocidas.

La cuarta consiste en integrar el motor de riesgo con el sistema de alertas para que una vulnerabilidad crítica produzca una respuesta prioritaria. La revisión sistemática reciente de seguridad de smart homes también apunta hacia mecanismos de detección en gateways, ciclos de actualización exigibles y análisis locales que preserven la privacidad como líneas de evolución relevantes para la seguridad doméstica (Radovanovic et al., 2026).

8. REFERENCIAS BIBLIOGRÁFICAS

Arteaga, F., & Alonso Lecuit, J. (2024, 17 de junio). La ciberresiliencia: Entre la ciberseguridad y la resiliencia. Real Instituto Elcano. <https://www.realinstitutoelcano.org/analisis/la-ciberresiliencia-entre-la-ciberseguridad-y-la-resiliencia/>

Asociación Colombiana de Ingenieros de Sistemas. (2019). Ciberriesgos: Un riesgo sistémico. Sistemas, (148), 12–41. <https://www.acis.org.co/>

Comisión de Regulación de Comunicaciones. (2025, 23 de diciembre). Análisis prospectivo en materia de ciberseguridad. CRC. Documento oficial de la CRC. <https://www.crcm.gov.co/system/files/Biblioteca%20Virtual/An%C3%A1lisis%20prospectivo%20en%20materia%20de%20ciberseguridad/analisis-prospectivo-ciberseguridad-261225.pdf>

Gómez Mendoza, E. J. (2024, 5 de agosto). Ciberseguridad del Internet de las cosas (IoT) en el sector doméstico y estado actual en Colombia [Trabajo de grado, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional UNAD. Repositorio UNAD. <https://repository.unad.edu.co/bitstream/handle/10596/63551/ejgomezmen.pdf>

International Organization for Standardization, & International Electrotechnical Commission. (2019). IEC 31010:2019: Risk management—Risk assessment techniques. International Organization for Standardization. ISO 31010:2019. <https://www.iso.org/standard/72140.html?>

Kaspersky. (2019, 28 de agosto). Kaspersky registra 45 ataques por segundo en América Latina. Kaspersky. <https://latam.kaspersky.com/blog/kaspersky-registra-45-ataques-por-segundo-en-america-latina/15274/>

Ministerio de Tecnologías de la Información y las Comunicaciones. (2025, 3 de junio). Modelo de Seguridad y Privacidad de la Información (MSPI). Gobierno Digital. Modelo de Seguridad y Privacidad de la Información. https://gobiernodigital.mintic.gov.co/692/w3-multipropertyvalues-533221-533236.html?__noredirect=1

National Institute of Standards and Technology. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST Special Publication 800-61 Revision 3). U.S. Department of Commerce. NIST SP 800-61 Rev. <https://csrc.nist.gov/pubs/sp/800/61/r3/final>

Romero, J. C. (2021). Ciberseguridad: Evolución y tendencias. Dialnet. <https://dialnet.unirioja.es/servlet/articulo?codigo=8175398&utm>

Toala Pilay, M. A., & Gutiérrez Tubay, M. A. (2024, 20 de marzo). [Trabajo relacionado con infraestructura IoT, ZigBee y control inteligente] [Trabajo de grado, Universidad Estatal del Sur de Manabí]. Repositorio Digital UNESUM. Repositorio Digital UNESUM. <http://repositorio.unesum.edu.ec/handle/53000/6368?utm>

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). Understanding the Mirai botnet. Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), 1093–1110. <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis>

Bitdefender. (2025, October 29). New Bitdefender and NETGEAR report reveals rising threats across the connected home landscape [Press release]. <https://www.bitdefender.com/en-us/news/new-bitdefender-and-netgear-report-reveals-rising-threats-across-the-connected-home-landscape>

Bitdefender. (2025, August 6). Mejores prácticas para proteger tu hogar inteligente con IoT. Bitdefender Hot for Security. <https://www.bitdefender.com/es-es/blog/hotforsecurity/mejores-practicas-para-proteger-tu-hogar-inteligente-con-iot>

Cloudflare. (s. f.). ¿Qué es la seguridad de IoT? Cloudflare Learning Center. <https://www.cloudflare.com/es-es/learning/security/glossary/iot-security/>

Domínguez Waisbrod, S. (2024, February 9). Las 10 contraseñas débiles más utilizadas en dispositivos IoT durante 2023. WeLiveSecurity. <https://www.welivesecurity.com/es/seguridad-iot/10-contrasenas-debiles-comunes-dispositivos-iot-2023/>

ETSI. (2024, September). ETSI EN 303 645 V3.1.3: Cyber security for consumer Internet of Things: Baseline requirements. European Telecommunications Standards Institute. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

Fagan, M., Megas, K., Cuthill, B., Marron, J., & Hoehn, B. (2026). Foundational cybersecurity activities for IoT product manufacturers (NISTIR 8259 Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8259r1>

Fagan, M., Megas, K., Scarfone, K., & Smith, M. (2020). IoT device cybersecurity capability core baseline (NISTIR 8259A). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8259A>

Fagan, M., Megas, K., Watrobski, P., Marron, J., Cuthill, B., Lemire, D., Hoehn, B., & Evans, C. (2024). Recommended cybersecurity requirements for consumer-grade router products (NISTIR 8425A). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8425A>

Gálvez Cisneros, X. A. (2025). Ciberseguridad en los dispositivos IoT de uso doméstico: Una revisión sistemática de la literatura. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 140–170.

Ghirardello, K., Maple, C., Ng, D., & Kearney, P. (2018). Cyber security of smart homes: Development of a reference architecture for attack surface analysis. In *Living in the Internet of Things: Cybersecurity of the IoT*. <https://doi.org/10.1049/cp.2018.0045>

International Organization for Standardization. (2018). ISO/IEC 29147:2018: Information technology — Security techniques — Vulnerability disclosure. <https://www.iso.org/standard/72311.html>

International Organization for Standardization. (2019). ISO/IEC 30111:2019: Information technology — Security techniques — Vulnerability handling processes. <https://www.iso.org/standard/69725.html>

International Organization for Standardization. (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information

F-DC-125

INFORME FINAL DE TRABAJO DE GRADO EN MODALIDAD DE
PROYECTO DE INVESTIGACIÓN, DESARROLLO TECNOLÓGICO,
MONOGRAFÍA, EMPRENDIMIENTO Y SEMINARIO

VERSIÓN: 2.0

security management systems — Requirements.
<https://www.iso.org/standard/27001>

International Organization for Standardization. (2022). ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls. <https://www.iso.org/standard/75652.html>

International Organization for Standardization. (2022). ISO/IEC 27005:2022: Information security, cybersecurity and privacy protection — Guidance on managing information security risks. <https://www.iso.org/standard/80585.html>

International Organization for Standardization. (2022). ISO/IEC 27400:2022: Cybersecurity — IoT security and privacy — Guidelines. <https://www.iso.org/standard/44373.html>

International Organization for Standardization. (2023). ISO/IEC 27402:2023: Cybersecurity — IoT security and privacy — Device baseline requirements. <https://www.iso.org/standard/80136.html>

International Organization for Standardization. (2025). ISO/IEC 27404:2025: Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT. <https://www.iso.org/standard/80138.html>

Jia, Y., Song, Y., Liu, Z., Tan, Q., Song, Y., Zhang, Y., & Liu, Z. (2026). Analyzing consumer IoT traffic from security and privacy perspectives: A comprehensive survey. *Frontiers of Computer Science*, 20(7), 2007809. <https://doi.org/10.1007/s11704-025-41155-0>

Keyfactor. (2020, October 28). Top 10 IoT vulnerabilities in your devices. <https://www.keyfactor.com/blog/top-10-iot-vulnerabilities-in-your-devices/>

Karimian, A., et al. (2022). Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions. Internet of Things, 18, 100508. <https://doi.org/10.1016/j.iot.2022.100508>

Kumar, V. (2025). Enhancing home IoT network security. Discover Applied Sciences, 7, 1085. <https://doi.org/10.1007/s42452-025-07270-0>

Li, Y., et al. (2023). ZPA: A smart home privacy analysis system based on ZigBee encrypted traffic. Wireless Communications and Mobile Computing, 2023, 6731783. <https://doi.org/10.1155/2023/6731783>

Megas, K. N., Fagan, M., Marron, J., Watrobski, P., & Cuthill, B. (2022). Profile of the IoT core baseline for consumer IoT products (NISTIR 8425). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8425>

National Institute of Standards and Technology. (2025). Mitigating cybersecurity and privacy risks in telehealth smart home integration (NIST Cybersecurity White Paper CSWP 34). <https://csrc.nist.gov/pubs/cswp/34/mitigating-cybersecurity-and-privacy-risks-in-tele/final>

Pardo Vergara, R. D., & Herrera Herrera, H. M. (2025). Propuesta de estrategias de ciberseguridad doméstica basadas en ISO/IEC 27001: Guía de controles prácticos. Apuntes de Ciencia e Ingeniería, 4(2). <https://doi.org/10.37511/apuntesci.v4n2a6>

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper CSWP 29). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.CSWP.29>

Radovanovic, D., Savanovic, N., Janackovic, J., & Kresoja, P. (2026). A systematic review of smart home IoT security: Applications, threat taxonomy, privacy risks, and emerging defensive solutions. *Big Data and Cognitive Computing*, 10(8), 252. <https://doi.org/10.3390/bdcc10080252>

Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial Internet of Things. *Proceedings of the 52nd Annual Design Automation Conference*, 1–6. <https://doi.org/10.1145/2744769.2747942>

Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., & Tschofenig, H. (2022, August). Authentication and authorization for constrained environments using the OAuth 2.0 framework (ACE-OAuth) (RFC 9200). RFC Editor. <https://doi.org/10.17487/RFC9200>

SentinelOne. (2025, July 23). Top 10 IoT security risks and how to mitigate them. <https://www.sentinelone.com/cybersecurity-101/data-and-ai/iot-security-risks/>

Total Defense. (2026, March 21). Hidden security risks inside smart home hubs and routers (and how to protect yourself). <https://www.totaldefense.com/security-blog/hidden-security-risks-inside-smart-home-hubs-and-routers-and-how-to-protect-yourself/>

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2019). What security features and crime prevention advice is communicated in consumer IoT

device manuals and support pages? Journal of Cybersecurity, 5(1), tyz005.
<https://doi.org/10.1093/cybsec/tyz005>

Wang, Z., Liu, D., Sun, Y., Pang, X., Sun, P., Lin, F., Lui, J. C. S., & Ren, K. (2022). A survey on IoT-enabled home automation systems: Attacks and defenses. IEEE Communications Surveys & Tutorials, 24(4), 2292–2328.
<https://doi.org/10.1109/COMST.2022.3201557>

Khadka, B., Shah, A. K., Shah, R. K., & Yadav, R. K. (2025). An investigation of security risks regarding the user awareness of IoT devices in the home. AIP Conference Proceedings, 3297(1), 030015.
<https://doi.org/10.1063/5.0287403>

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K., Nadeau, E., O'Rourke, D. G., Piccarreta, B., & Scarfone, K. (2019). Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks (NISTIR 8228). National Institute of Standards and Technology.
<https://doi.org/10.6028/NIST.IR.8228>

Cybersecurity and Infrastructure Security Agency. (2016, 14 de octubre). Heightened DDoS threat posed by Mirai and other botnets (Alert TA16-288A). U.S. Department of Homeland Security. <https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets>

Hernandez, G., Arias, O., Buentello, D., & Jin, Y. (2014). Smart Nest Thermostat: A smart spy in your home [Documento de conferencia]. Black Hat USA.
<https://blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf>

Microsoft Security. (2021, 19 de agosto). How to proactively defend against Mozi IoT botnet. Microsoft. <https://www.microsoft.com/en-us/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/>

European Union Agency for Cybersecurity. (2017, 20 de noviembre). Baseline security recommendations for Internet of Things in the context of critical information infrastructures. <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>

FIRST.org, Inc. (2019). Common vulnerability scoring system version 3.1: Specification document. <https://www.first.org/cvss/v3.1/specification-document>

OWASP Foundation. (2018). OWASP Internet of Things Top 10. <https://owasp.org/www-project-internet-of-things/>