MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE GRADUACIÓN

Sometido al Tribunal Examinador de Postgrados para optar por el grado de Maestría en Ciberseguridad

Título del Proyecto

Evaluación del dispositivo SafeLock como solución integral de ciberseguridad perimetral, orientado a proteger redes domésticas y de pymes frente a amenazas avanzadas y ataques persistentes.

AUTOR

Ing. Michael Corrales Oviedo, MS.c.

TUTOR: MS.c. Randall Artavia Delgado

LECTOR: MS.c. Irvin Argenis Sáenz Córdoba

Perez Zeledón, Costa Rica
Diciembre 2025

UNIVERSIDAD SAN ISIDRO DEL LABRADOR

MAESTRÍA EN CIBERSEGURIDAD

TRIBUNAL EXAMINADOR

Ing. Ruddy Rodríguez Acuña

Director de Maestría

Msc. Randall Artavia Delgado

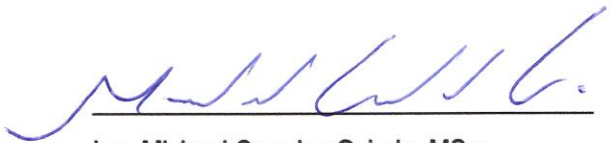
Tutor

Msc. Irvin Argenis Sáenz Córdoba

Lector

DECLARACIÓN JURADA

Yo, Michael Corrales Oviedo, mayor, casado(a), egresado(a) de la carrera de Maestría Profesional en Ciberseguridad de la Universidad San Isidro Labrador, domiciliado en la ciudad de San Isidro, Pérez Zeledón, portador(a) de la cédula de identidad número 1-1130-0124, en este acto, debidamente apercibido y entendido de las penas y consecuencias con las que se castiga, en el Código Penal, el delito del perjurio, ante quienes se constituyen en el Tribunal Examinador de mi Trabajo Final de Graduación para optar por el título de maestría, juro solemnemente que mi trabajo final de graduación titulado "**Evaluación del dispositivo SafeLock como solución integral de ciberseguridad perimetral, orientado a proteger redes domésticas y de pymes frente a amenazas avanzadas y ataques persistentes**", es una obra original que ha respetado todo lo preceptuado por las Leyes Penales así con la Ley de Derechos de Autor y Derechos Conexos, número 6683 de 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 de 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte: artículo 70°: Es permitido citar a un autor transcribiendo los pasajes pertinentes siempre que estos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor y de la obra original. Asimismo, quedo advertido que la Universidad San Isidro Labrador se reserva el derecho de protocolizar este documento ante Notario Público. En fe de lo anterior firmo en la ciudad de San isidro del General, al ser el 06 del mes de diciembre del año dos mil veinticinco.



Ing. Michael Corrales Oviedo, MS.c.

Cédula: 1-1130-0124

DEDICATORIA

A Dios, fuente de fortaleza, sabiduría y esperanza, por guiar cada paso de mi vida y permitirme culminar este proceso académico. A Él encomiendo este logro, pues sin su gracia, su dirección y su luz en los momentos de mayor dificultad, no habría sido posible perseverar hasta el final.

A mi madre, motor y razón de mi vida, quien con su ejemplo de esfuerzo, humildad y amor incondicional sembró en mí los valores que hoy me sostienen. Su partida durante el transcurso de esta maestría marcó uno de los momentos más difíciles de mi existencia, pero también se transformó en una fuente inagotable de fortaleza y motivación para culminar este camino académico en su memoria. Cada página de este trabajo es un homenaje a su legado, pues sin sus enseñanzas y su fe en mí, este logro no habría sido posible.

A mi esposa, compañera de vida y apoyo incondicional, cuyo amor, paciencia y comprensión han sido pilares esenciales en este proceso. Su presencia constante, sus palabras de ánimo y su confianza en mis capacidades me recordaron, aún en los momentos más duros, que juntos podemos superar cualquier desafío. Ella ha sido más que una compañera, ha sido mi complemento perfecto, llenando de equilibrio y esperanza los días de esfuerzo y estudio.

A mis hijos, Samuel e Ismael, que con su ternura, comprensión y sonrisas me han brindado la motivación diaria para seguir adelante. Ellos han aprendido a entender mis ausencias y sacrificios, regalándome su cariño y apoyo incondicional. Su alegría ha sido la chispa que encendió mi compromiso de perseverar, recordándome siempre que este logro también les pertenece, porque ha sido construido con su paciencia, amor y comprensión.

Finalmente, a mis familiares más cercanos, quienes han estado presentes en cada etapa de este proceso, acompañándome con su interés, oraciones, consejos y gestos de apoyo sincero. Su compañía silenciosa pero firme me ha recordado que los logros nunca son individuales, sino el resultado de la unión y el cariño de quienes nos rodean. A todos ellos, mi más profundo agradecimiento por haber sido parte fundamental de este recorrido.

AGRADECIMIENTOS

A Dios, fuente de todo, por darme la fortaleza, la sabiduría y la salud necesarias para llegar hasta este momento. A Él encomiendo este logro, pues ha sido su guía, su luz y su infinita misericordia las que me han sostenido en cada dificultad, mostrándome que con fe y perseverancia es posible alcanzar las metas más grandes.

Al Ing. Ruddy Rodríguez Acuña, por toda su ayuda, confianza y colaboración en calidad de cabeza de la Escuela de Ingeniería. Su liderazgo, visión académica y disposición constante han permitido que los estudiantes encontremos en la universidad un espacio de crecimiento integral. Su apoyo ha sido fundamental para que esta maestría se desarrolle con excelencia y para que cada uno de nosotros tengamos la oportunidad de alcanzar nuestras metas profesionales.

Al MS.c. Randall Artavia Delgado, profesor y guía invaluable durante este proceso, por su paciencia, orientación y compromiso en cada etapa de la elaboración de este Trabajo Final de Graduación. Su disposición para aclarar dudas, su capacidad para motivar en los momentos de mayor cansancio y su exigencia académica fueron pilares para mantener la disciplina y la constancia necesarias en la culminación de este proyecto.

A la Universidad Internacional San Isidro Labrador (UISIL), por abrir las puertas a la formación de profesionales en ciberseguridad y promover una visión innovadora que responde a las demandas actuales de la sociedad. Esta institución ha sido un espacio de crecimiento, no solo académico, sino también humano, que nos motiva a asumir con responsabilidad los retos del mundo digital. El esfuerzo de la universidad por ofrecer programas de tan alto nivel es un reflejo del compromiso con el país y con la región en la construcción de un futuro más seguro e inclusivo.

A mi madre, por toda su guía, apoyo y amor incondicional durante el tiempo que estuvo conmigo en este mundo y ahora desde donde se encuentra. Su ejemplo de fortaleza, entrega y sacrificio sigue vivo en mí y se refleja en cada paso que doy. Este trabajo es también suyo, porque fue su inspiración y sus enseñanzas las que me impulsaron a no rendirme y a terminar lo que juntos alguna vez soñamos.

A mi esposa e hijos, quienes han sido los pilares fundamentales de este proceso. A mi esposa, por su amor, paciencia y apoyo constante, siempre dispuesta a comprender mis ausencias y a darme palabras de ánimo en los momentos más duros. A mis hijos Samuel e Ismael, por su alegría, ternura y comprensión, que se convirtieron en la motivación diaria para no detenerme y culminar este sueño. Ellos son la razón principal de mis esfuerzos y la inspiración más grande para seguir construyendo un mejor futuro.

Finalmente, a mis compañeros de maestría, por su apoyo, generosidad y compañerismo en cada etapa del camino. Compartir este proceso con ellos ha sido un verdadero privilegio, ya que más allá de las aulas virtuales se formó un vínculo de amistad y solidaridad que enriqueció la experiencia académica. Cada intercambio de ideas, cada trabajo en equipo y cada gesto de apoyo mutuo fueron esenciales para mantener el entusiasmo y la confianza de que juntos lograríamos culminar este desafío.

CARTA DE AUTORIZACIÓN DEL TUTOR

Pérez Zeledón, 06 de diciembre de 2025

Licenciado
Ruddy Rodríguez Acuña
Coordinador de la Escuela de Informática
Universidad Internacional San Isidro Labrador

Estimado señor director:

Yo, Randall Mauricio Artavia Delgado, mayor, Ingeniero en informática, con domicilio en la Trinidad de Moravia San José, portador de la cédula de identidad número **205740823**, en mi condición de tutor del Proyecto de Graduación titulado: Evaluación del dispositivo SafeLock como solución integral de ciberseguridad perimetral, orientado a proteger redes domésticas y de pymes frente a amenazas avanzadas y ataques persistentes**,** propuesta por el estudiante **Michael Corrales Oviedo**, manifiesto lo siguiente:

1. Que el proceso de trabajo final de graduación culmina satisfactoriamente.
2. Que se ha incorporado en el documento final las sugerencias hechas por el Tribunal Examinador.
3. Que he cumplido con el acompañamiento encomendado por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,

MATI Randall Mauricio Artavia Delgado
Tutor

CARTA DE APROBACIÓN DEL LECTOR

Pérez Zeledón, 06 de diciembre de 2025

Licenciado
Ruddy Rodríguez Acuña
Coordinador de la Escuela de Informática
Universidad Internacional San Isidro Labrador

Estimado señor director:

Yo, Irvin Sáenz Córdoba, mayor, divorciado, analista de ciberseguridad L2, vecino de Guápiles, portador de la cédula de identidad número 7-0197-0839, en mi condición de lector del Proyecto de Graduación titulado: Evaluación del dispositivo SafeLock como solución integral de ciberseguridad perimetral, orientado a proteger redes domésticas y de pymes frente a amenazas avanzadas y ataques persistentes, propuesta por el estudiante Michael Corrales Oviedo, manifiesto lo siguiente:

1. Que la lectura del trabajo final de graduación concluye satisfactoriamente.
2. Que he leído el documento final y he hecho mis observaciones en el mismo.
3. Que he cumplido con las labores de lector encomendadas por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,

Máster Irvin Sáenz Córdoba
Lector

TABLA DE CONTENIDOS

DEDICATORIA iv
AGRADECIMIENTOS v
TABLA DE CONTENIDOS ix
ÍNDICE DE TABLAS xii
ÍNDICE DE GRÁFICOS, FIGURAS E ILUSTRACIONES xiii
LISTA DE PALABRAS CLAVES xiv
RESUMEN EJECUTIVO xv
CAPÍTULO I. INTRODUCCIÓN 17
1.1 Planteamiento del tema de estudio 18
1.2 Antecedentes del tema 19
1.3 Justificación 21
1.4 Objetivos 24
1.4.1 Objetivo general 24
1.4.2 Objetivos específicos 24
1.5 Alcances 24
Elementos fuera del alcance 26
1.6 Limitaciones 28
1.7 Cronograma de actividades 30
1.8 Producto esperado del TFG 31
CAPÍTULO II. MARCO TEÓRICO 33
Marco Teórico 34
1. Ciberseguridad perimetral 34
Definición y evolución del concepto 34
Importancia de la seguridad en el perímetro de red frente a amenazas externas 35
Comparación entre seguridad perimetral tradicional y modelos actuales basados en hardware inteligente 36
2. Redes domésticas y de PyMEs 37
Características particulares de estas redes 37
Riesgos específicos en entornos residenciales y PyME 38
Impacto económico y operativo de los incidentes de seguridad 39
3. Amenazas avanzadas persistentes (APT) 40

Definición, ciclo de vida y fases de una APT 40
Técnicas comunes utilizadas por los actores maliciosos 41
Relación entre APTs y la necesidad de protección perimetral inteligente 42
4. Dispositivos IoT y su impacto en la superficie de ataque 42
Concepto y tipos de dispositivos IoT 43
Vulnerabilidades típicas en entornos IoT 44
Papel del firewall perimetral en la protección de dispositivos inteligentes 45
4. Firewalls de nueva generación (NGFW) 46
Características diferenciales frente a los firewalls tradicionales 46
Funciones integradas 47
Comparativa entre NGFW comerciales y soluciones adaptadas como SafeLock 49
5. Sistemas de detección y respuesta 50
Definición y diferencia entre sistemas de detección y prevención 50
Enfoque perimetral vs. enfoque endpoint 50
Aplicabilidad en entornos pequeños con recursos limitados 50
6. Aprendizaje automático aplicado a ciberseguridad 51
Concepto de machine learning en la detección de amenazas 51
Aplicaciones comunes en clasificación de tráfico y detección de anomalías 51
Ventajas y desafíos de usar modelos ML en dispositivos embebidos 51
7. Arquitectura de dispositivos de seguridad embebida 52
Componentes físicos y lógicos 52
Principios de diseño seguro 52
Ejemplos de arquitecturas similares 52
8. Soberanía tecnológica y soluciones locales 53
Importancia del desarrollo regional de tecnologías 53
Limitaciones de soluciones importadas 53
Valor estratégico de SafeLock en América Latina 53
9. Ciberresiliencia 54
Concepto de ciberresiliencia en organizaciones y usuarios 54
Contribución de dispositivos perimetrales a la respuesta ante incidentes 54
Indicadores para medir ciberresiliencia 54
CAPITULO III. MARCO METODOLÓGICO 56
3.1 Tipo de investigación 57
3.1.1 Finalidad 57
3.2 Administración y abordaje del proyecto objeto 61

3.2.1 Descripción de supuestos 62
3.2.2 Restricciones y riesgos 62
3.3 Sujetos y fuentes de información 63
3.3.1 Sujetos de Información 63
3.3.2 Fuentes de información 63
3.4 Muestreo 63
3.4.1 Población y muestreo 63
3.4.2 Tipo de muestreo 64
3.5 Diseño de técnicas e instrumentos para recolectar información 64
3.5.1 Detalle de técnica e instrumentos de aplicación 64
3.5.2 Detalle de la aplicación de técnicas e instrumentos 64
3.6 Determinación de variables 65
3.6.1 Clasificación 65
3.6.2 Definición 65
3.6.3 Cuadro o matriz de las variables 65
CAPÍTULO IV. ANÁLISIS DE RESULTADOS 67
4.1 Introducción al análisis 68
4.2 Resultados 69
4.2.1 Descripción de la muestra y línea base 69
4.2.2 Métricas técnicas y rendimiento operativo 71
..... 75
4.2.3 Evaluación de usabilidad (SUS) 76
4.2.4 Incidencias de soporte y retroalimentación cualitativa 79
4.2.5 Comparativa de SafeLock frente a soluciones comerciales 82
4.2.6 Brechas y plan de mejora post-piloto 85
4.3 Conclusión general del análisis 87
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES 89
5.1 Conclusiones 90
5.2 Recomendaciones 91
Conclusión general del capítulo 93
BIBLIOGRAFÍA 95
ANEXOS 98
Anexo 1. Instrumento de Evaluación de Usabilidad del Dispositivo SafeLock (SUS) 99
Anexo 2. Registro de Incidencias de Soporte 100
Anexo 3. Comentarios Cualitativos de los Usuarios 101

ÍNDICE DE TABLAS

Tabla 1. Comparativa de características entre SafeLock y productos similares. 20

Tabla 2. Factores que aumentan la superficie de ataque en redes con IoT 45

Tabla 3. Comparación entre firewalls tradicionales y firewalls de nueva generación (NGFW) 48

Tabla 4. Componentes clave de la ciberseguridad perimetral en redes domésticas y PyMEs 55

Tabla 5. Tabla comparativa de finalidades 58

Tabla 6. Tabla comparativa de enfoques sistemáticos 59

Tabla 7. Tabla comparativa de naturaleza 60

Tabla 8. Tabla comparativa de carácter 61

Tabla 9. Matriz de Variables 65

Tabla 10. Porcentaje de vulnerabilidades detectadas en los entornos evaluados antes de la instalación de SafeLock 76

Tabla 11. Resultados de las métricas técnicas del dispositivo SafeLock durante las pruebas piloto 78

Tabla 12. Resultados del puntaje de usabilidad SUS del dispositivo SafeLock en entornos domésticos y empresariales 82

Tabla 13. Registro de incidencias de soporte técnico durante las pruebas piloto del dispositivo SafeLock 85

Tabla 14. Comentarios cualitativos de los usuarios y su interpretación durante las pruebas del dispositivo SafeLock 86

Tabla 15. Comparativa del dispositivo SafeLock frente a soluciones comerciales de referencia 89

Tabla 16. Plan de mejora del dispositivo SafeLock posterior a las pruebas piloto 91

ÍNDICE DE GRÁFICOS, FIGURAS E ILUSTRACIONES

Figura 1. Distribución estimada de ciberataques por tipo de objetivo. 20

Figura 2. Alcance del Proyecto 28

Ilustración 1. Distribución porcentual de vulnerabilidades iniciales (puertos abiertos, contraseñas por defecto y dispositivos IoT desactualizados). 72

Ilustración 2. Comparativo de métricas técnicas del dispositivo SafeLock 73

Ilustración 3-2A. Interfaz del panel de monitoreo de amenazas bloqueadas del dispositivo SafeLock. 74

Ilustración 4-2B. Interfaz del panel principal de SafeLock con métricas de consultas, bloqueos y dominios supervisados 75

Ilustración 5. Comparación de resultados SUS entre hogares y PyMEs. 78

Ilustración 6. Clasificación de incidencias reportadas 80

Ilustración 7. Retroalimentación de usuarios sobre la experiencia de uso del dispositivo SafeLock 82

Ilustración 8. Posición comparativa del dispositivo SafeLock respecto a soluciones comerciales de referencia 85

LISTA DE PALABRAS CLAVES

- Amenazas persistentes avanzadas (APT)
- Aprendizaje automático aplicado a ciberseguridad
- Arquitectura de red segura
- Ciberresiliencia
- Ciberseguridad perimetral
- Control de acceso
- Defensa en profundidad
- Dispositivos IoT
- Evaluación de usabilidad
- Experiencia del usuario
- Firewalls de nueva generación (NGFW)
- Gestión de vulnerabilidades
- Innovación tecnológica costarricense
- Inteligencia artificial en seguridad
- Pequeñas y medianas empresas (PyMEs)
- Protección de datos
- Redes domésticas
- SafeLock
- Seguridad informática en Costa Rica
- Transformación digital

RESUMEN EJECUTIVO

Este Trabajo Final de Graduación evalúa la eficacia del dispositivo SafeLock como solución integral de ciberseguridad perimetral para redes domésticas y de pequeñas y medianas empresas (PyMEs) en Costa Rica, con el propósito de determinar su aplicabilidad frente a amenazas avanzadas y ataques persistentes durante 2025. El objetivo general orienta la investigación hacia la validación técnica y de usabilidad del dispositivo en entornos reales y simulados, así como a la formulación de recomendaciones para su adopción en el contexto nacional.

El enfoque metodológico considera acciones centrales: caracterización del contexto costarricense de ciberseguridad, diagnóstico de necesidades, implementación de pruebas piloto con SafeLock, evaluación de desempeño técnico (seguridad y eficiencia), análisis comparativo con alternativas de mercado y elaboración de recomendaciones.

La muestra de la fase aplicada comprendió 10 participantes: 6 hogares y 4 PyMEs del sector comercio y servicios, con topologías de red representativas del entorno objetivo (router básico residencial y switch administrable en PyME).

El diagnóstico de línea base evidenció exposición inicial elevada: 70 % de redes domésticas y 50 % de PyMEs con puertos abiertos de administración remota, así como 40 % de uso de contraseñas por defecto en routers. En hogares se identificó en promedio 4 dispositivos IoT, con 30 % de firmware desactualizado; además, en entornos PyME se registró un promedio semanal de 3 intentos de intrusión y 2 alertas de malware antes de instalar el dispositivo. Estos hallazgos confirman la pertinencia de una defensa perimetral accesible y efectiva.

Durante las pruebas, SafeLock mostró desempeño técnico consistente: TBR 94 %, TPR 92 %, FPR 1.8 %, latencia p95 = 42 ms, throughput 93 % y uptime 99.4 %, resultados que evidencian equilibrio entre protección, estabilidad y transparencia operativa en el uso cotidiano.

En términos de experiencia de usuario, la evaluación SUS arrojó un promedio general de 97.25/100 (hogares 97.50; PyMEs 96.88), muy por encima del umbral de excelencia, lo que confirma la alta usabilidad del modelo plug-and-protect incluso para usuarios con escasa formación técnica.

La evidencia empírica respalda que SafeLock reduce significativamente la superficie de ataque (al controlar puertos expuestos y credenciales débiles, y mitigar riesgos IoT) y

mejora la ciberresiliencia de hogares y PyMEs sin introducir fricción perceptible en el desempeño de la red. Asimismo, el análisis comparativo sugiere ventajas de accesibilidad y adecuación contextual frente a soluciones importadas, en línea con los objetivos y alcances del estudio.

Como resultado, se formulan recomendaciones técnicas (interfaz con métricas visibles, fortalecimiento del sistema de actualización OTA, segmentación de perfiles hogar/PyME), operativas (capacitación básica y mantenimiento preventivo) y estratégicas (alianzas con instituciones, y evaluación para certificaciones) con el fin de consolidar la adopción y evolución del dispositivo en el ecosistema local. Estas recomendaciones se alinean con los productos esperados y la proyección de transferencia de conocimiento del proyecto.

En síntesis, los resultados confirman que es posible, desde Costa Rica, desarrollar y validar una solución de ciberseguridad perimetral avanzada, usable y sostenible, capaz de cerrar brechas de protección en entornos históricamente desatendidos y de fortalecer la competitividad tecnológica nacional.

CAPITULO I. INTRODUCCIÓN

1.1 Planteamiento del tema de estudio

En el actual panorama de amenazas cibernéticas, las redes domésticas y de pequeñas empresas enfrentan riesgos crecientes sin contar con soluciones de seguridad perimetral adecuadas, accesibles y adaptadas a sus necesidades particulares. La sofisticación de los ciberataques ha superado ampliamente las medidas básicas de seguridad, y la mayoría de estas entidades no dispone de conocimientos técnicos, recursos financieros o personal especializado que les permita implementar soluciones empresariales tradicionales.

El dispositivo SafeLock propone una respuesta a esta situación, ofreciendo un enfoque integral de protección perimetral mediante hardware especializado y software de monitoreo en tiempo real. Sin embargo, surge el cuestionamiento de si dicha solución es capaz de satisfacer de manera efectiva, sostenible y escalable los requerimientos de seguridad en estos entornos.

Por tanto, el problema central que guía esta investigación es:

¿Puede el dispositivo SafeLock proporcionar una solución integral, eficaz y accesible de ciberseguridad perimetral para redes domésticas y PyMEs, frente a amenazas avanzadas y ataques persistentes, sin requerir altos niveles de especialización técnica?

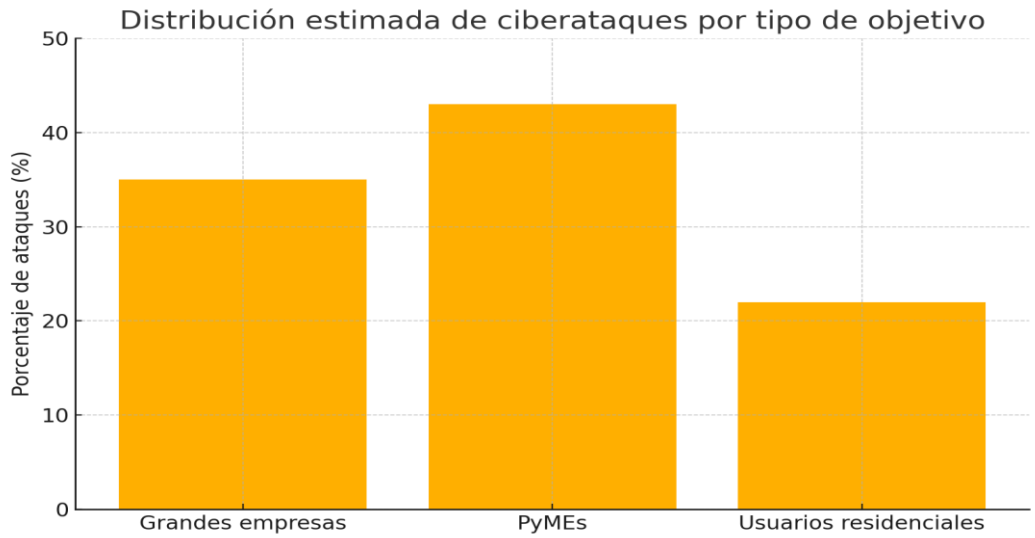
Este problema implica analizar no solo el componente técnico del dispositivo, sino también su adopción práctica, su nivel de configuración, su comportamiento frente a distintos vectores de ataque y su contribución al fortalecimiento de la ciberresiliencia en usuarios no corporativos.

1.2 Antecedentes del tema

La ciberseguridad perimetral ha sido tradicionalmente una norma reservada a grandes corporaciones, dado que involucra la implementación de tecnologías especializadas, configuraciones evolucionadas y personal capacitado. No obstante, la expansión del trabajo remoto, la digitalización de los servicios y el crecimiento de las pequeñas y medianas empresas (PyMEs) como figurantes económicos clave, ha ampliado de forma significativa la superficie de ataque de redes menos protegidas. Esta transformación ha evidenciado una brecha de seguridad crítica en medios residenciales y PyME, los cuales han sido históricamente desatendidos por la industria de la ciberseguridad (Anderson, 2020; López et al., 2023).

Las estadísticas globales subrayan esta problemática: según Verizon (2023), el 43% de los ciberataques registrados a nivel mundial tienen como blanco a pequeñas empresas. Asimismo, investigaciones locales en América Latina indican que más del 70% de las PyMEs no cuentan con políticas de ciberseguridad precisadas ni personal especializado (ESET Latinoamérica, 2022). En Costa Rica, la Cámara de Tecnologías de Información y Comunicación (CAMTIC) ha advertido sobre la vulnerabilidad de las redes domésticas y empresariales pequeñas, especialmente tras el auge del teletrabajo y la propagación de dispositivos IoT conectados sin medidas de protección adecuadas (CAMTIC, 2021).

Figura 1. Distribución estimada de ciberataques por tipo de objetivo.



Nota. Elaboración propia con base en datos de Verizon (2023) y ESET Latinoamérica (2022).

Ante este panorama, ha surgido un nuevo enfoque en el desarrollo de dispositivos de seguridad embebida enfocados a usuarios sin conocimientos técnicos avanzados. Proyectos como Firewalla, Norton Core o Bitdefender Box han intentado llenar ese vacío en mercados internacionales, combinando funciones de firewall, detección de amenazas, análisis de tráfico y control parental en una única unidad de fácil instalación (Firewalla Inc., 2022). Sin embargo, su adopción en contextos latinoamericanos ha sido limitada por barreras idiomáticas, costos elevados y falta de soporte regional.

Tabla 1. Comparativa de características entre SafeLock y productos similares.

Características	SafeLock	Firewalla	Bitdefender Box
Instalación sin conocimientos técnicos	Sí	Sí	Parcial
Interfaz en español	Sí	No	No
Actualizaciones automáticas	Sí	Sí	Sí
Análisis de tráfico en tiempo real	Sí	Sí	Sí
Uso de inteligencia artificial	Sí	No	Sí
Soporte regional en LATAM	Sí	No	No
Costo estimado (USD)	150	220	250

Nota. Elaboración propia con información de Firewalla (2022), Bitdefender (2022) y documentación de SafeLock.

En el caso de Costa Rica, se identifica una necesidad progresiva de soluciones locales, accesibles, efectivas y adaptadas al entorno sociotécnico del país. En respuesta, la empresa costarricense OpenLock Ciberseguridad ha desarrollado el dispositivo SafeLock, el cual incorpora técnicas de inteligencia artificial, seguridad multicapa y una arquitectura de hardware embebido de bajo costo. Esta propuesta busca cubrir el vacío existente entre las

necesidades de seguridad perimetral de las PyMEs y hogares costarricenses, y la falta de herramientas apropiadas para su contexto tecnológico y cultural.

Pese al surgimiento de este tipo de iniciativas, aún existe una carencia importante de estudios técnicos y académicos que validen su funcionalidad en condiciones reales. Las investigaciones revisadas se centran principalmente en soluciones empresariales de gran escala o en propuestas experimentales desarrolladas en entornos de laboratorio, sin ofrecer resultados concretos sobre su impacto en redes pequeñas o residenciales (Navarro & Sánchez, 2022; Martínez et al., 2023). Por tanto, la evaluación de SafeLock como una solución integral de ciberseguridad perimetral representa una contribución tanto para la comunidad académica como para los sectores productivos y hogares del país.

En este sentido, la presente investigación se orienta a cerrar dicha brecha, analizando rigurosamente el comportamiento, desempeño y aplicabilidad del dispositivo SafeLock como solución viable y eficaz frente a amenazas avanzadas en redes domésticas y de PyMEs en Costa Rica.

1.3 Justificación

La presente investigación se justifica por la progresiva necesidad de proteger de forma efectiva las redes domésticas y de pequeñas y medianas empresas (PyMEs) frente al aumento sostenido de amenazas cibernéticas avanzadas. En la actualidad, estas redes han dejado de ser espacios marginales dentro del ecosistema digital y se han convertido en nodos críticos de conectividad, almacenamiento de información sensible, y prestación de servicios a distancia. Sin embargo, carecen en su mayoría de soluciones de seguridad robustas, adaptadas a sus necesidades técnicas, económicas y culturales.

Las PyMEs representan más del 95% del tejido empresarial en Costa Rica y generan aproximadamente el 35% del empleo formal, según datos del Ministerio de Economía, Industria y Comercio (MEIC, 2022). A pesar de su impacto en la economía nacional, más del 70% de estas empresas no cuenta con políticas formales de ciberseguridad, lo que las convierte en un blanco vulnerable para ataques como el ransomware, la suplantación de identidad o las intrusiones silenciosas conocidas como APT (Advanced Persistent Threats) (ESET Latinoamérica, 2022).

En el ámbito residencial, la situación no es más propicio. El uso de dispositivos IoT, el trabajo remoto, la educación virtual y la gestión de servicios financieros en línea han convertido a los hogares en espacios que manejan constantemente información privada y profesional. Sin embargo, gran parte de estas redes presenta configuraciones inseguras, contraseñas por defecto, ausencia de actualizaciones y desconocimiento sobre las buenas prácticas de ciberseguridad (CAMTIC, 2021). En este entorno, la ausencia de medidas de protección perimetral expone tanto a usuarios individuales como a organizaciones a pérdidas económicas, robo de identidad, espionaje y daños reputacionales.

La investigación busca aportar una solución concreta a esta problemática mediante la valoración técnica y contextual del dispositivo SafeLock, una propuesta desarrollada localmente que combina múltiples mecanismos de defensa perimetral: detección y respuesta a amenazas en tiempo real, aprendizaje automático, análisis de tráfico, control de accesos y filtrado de contenido. A diferencia de otros productos del mercado, SafeLock está diseñado para ser implementado sin conocimientos técnicos avanzados, con una interfaz intuitiva, actualizaciones automáticas y compatibilidad con las condiciones de conectividad de la región.

Desde el punto de vista práctico, este estudio permitirá:

- Validar la eficacia del dispositivo SafeLock en condiciones reales, brindando evidencia práctica sobre su desempeño ante distintos vectores de ataque.
- Determinar su comodidad de implementación en redes locales, considerando factores como facilidad de uso, mantenimiento, adaptabilidad, y costo.
- Comparar SafeLock con otras soluciones disponibles en el mercado, estableciendo sus ventajas, limitaciones y oportunidades de mejora.
- Proponer recomendaciones técnicas y estratégicas para su adopción masiva, contribuyendo al fortalecimiento de la ciberresiliencia en sectores con pocos recursos tecnológicos.

Asimismo, los principales beneficiarios de esta investigación serán:

- Las PyMEs y usuarios residenciales, quienes lograrán acceder a una solución de ciberseguridad adecuada a sus posibilidades y necesidades.

- El sector educativo y académico, que contará con un caso de estudio riguroso sobre evaluación de soluciones embebidas de ciberseguridad.
- El ecosistema tecnológico nacional, al animar el desarrollo e implementación de soluciones innovadoras con enfoque local.
- Entidades gubernamentales y tomadores de decisiones, quienes podrán aprovechar los descubrimientos para el diseño de políticas públicas de ciberseguridad inclusiva.

La importancia de esta investigación también radica en su capacidad para cerrar una brecha crítica entre la oferta global de ciberseguridad y las necesidades reales de usuarios en Costa Rica y toda América Latina. La evaluación de SafeLock contribuirá a consolidar criterios de calidad y adaptabilidad para dispositivos de seguridad perimetral en contextos no corporativos, marcando un precedente para futuras investigaciones, desarrollos tecnológicos e iniciativas de ciberprotección desde el enfoque de soberanía tecnológica.

Por último, esta investigación es significativa ya que busca transformar la forma en que se entiende, aplica y accede a la ciberseguridad en niveles históricamente desprotegidos. A través de un enfoque técnico, contextual y aplicado, se pretende demostrar que es posible desarrollar soluciones integrales, eficaces y sostenibles para fortalecer el perímetro digital de los hogares y las PyMEs en Costa Rica.

1.4 Objetivos

1.4.1 Objetivo general

Evaluar la eficacia del dispositivo SafeLock como solución integral de ciberseguridad perimetral para redes domésticas y de pequeñas y medianas empresas en Costa Rica, con el fin de determinar su aplicabilidad frente a amenazas avanzadas y ataques persistentes durante el año 2025.

1.4.2 Objetivos específicos

1. Diagnosticar el nivel de exposición y vulnerabilidad de redes domésticas y de PyMEs en Costa Rica ante amenazas avanzadas, con el propósito de contextualizar la necesidad de una solución de ciberseguridad perimetral como SafeLock.
2. Analizar el funcionamiento técnico y operativo del dispositivo SafeLock en entornos simulados y reales, con el fin de valorar su capacidad de detección, respuesta y adaptabilidad ante diferentes vectores de ataque.
3. Validar la efectividad y usabilidad del dispositivo SafeLock mediante pruebas piloto en redes domésticas y de PyMEs seleccionadas, para retroalimentar su diseño y definir recomendaciones de implementación durante el 2025.

1.5 Alcances

El presente Trabajo Final de Graduación tiene como alcance fundamental evaluar el dispositivo SafeLock como una solución integral de ciberseguridad perimetral para redes domésticas y de pequeñas y medianas empresas (PyMEs) en Costa Rica, considerando el contexto actual de ciberamenazas, los retos de seguridad digital que enfrentan las organizaciones y la necesidad de contar con herramientas accesibles, eficientes y adaptables al entorno local.

La investigación busca responder al objetivo general: *"Evaluar el dispositivo SafeLock como solución integral de ciberseguridad perimetral, orientado a proteger redes domésticas y de PyMEs frente a amenazas avanzadas y ataques persistentes"*.

Para ello, se desarrollarán las siguientes acciones principales:

1. Caracterización del contexto costarricense en materia de ciberseguridad, identificando los principales riesgos, amenazas y vulnerabilidades que afectan a hogares y PyMEs.
2. Diagnóstico de las necesidades de protección de los segmentos objeto de estudio, mediante revisión documental, normativa y técnica.
3. Implementación del dispositivo SafeLock en entornos controlados y pruebas piloto, a fin de verificar sus capacidades de detección, prevención y mitigación frente a ciberataques.
4. Evaluación de desempeño técnico, incluyendo métricas de eficiencia, facilidad de uso, escalabilidad y costos de implementación.
5. Análisis comparativo frente a soluciones alternativas del mercado, con el propósito de evidenciar fortalezas, limitaciones y posibles mejoras.
6. Elaboración de recomendaciones técnicas y estratégicas, orientadas a promover la adopción del dispositivo como medida de ciberresiliencia en el entorno costarricense.

De manera más concreta, los productos esperados al finalizar el TFG son:

- Un diagnóstico integral de riesgos de ciberseguridad en redes domésticas y de PyMEs.
- Un informe técnico con los resultados de la instalación, configuración y pruebas de SafeLock en escenarios reales y simulados.
- Una matriz comparativa de desempeño entre SafeLock y otras soluciones de seguridad perimetral.
- Un documento de validación de usabilidad y facilidad de implementación para usuarios no expertos.
- Un conjunto de recomendaciones finales que sirvan tanto para la comunidad académica como para el sector productivo.

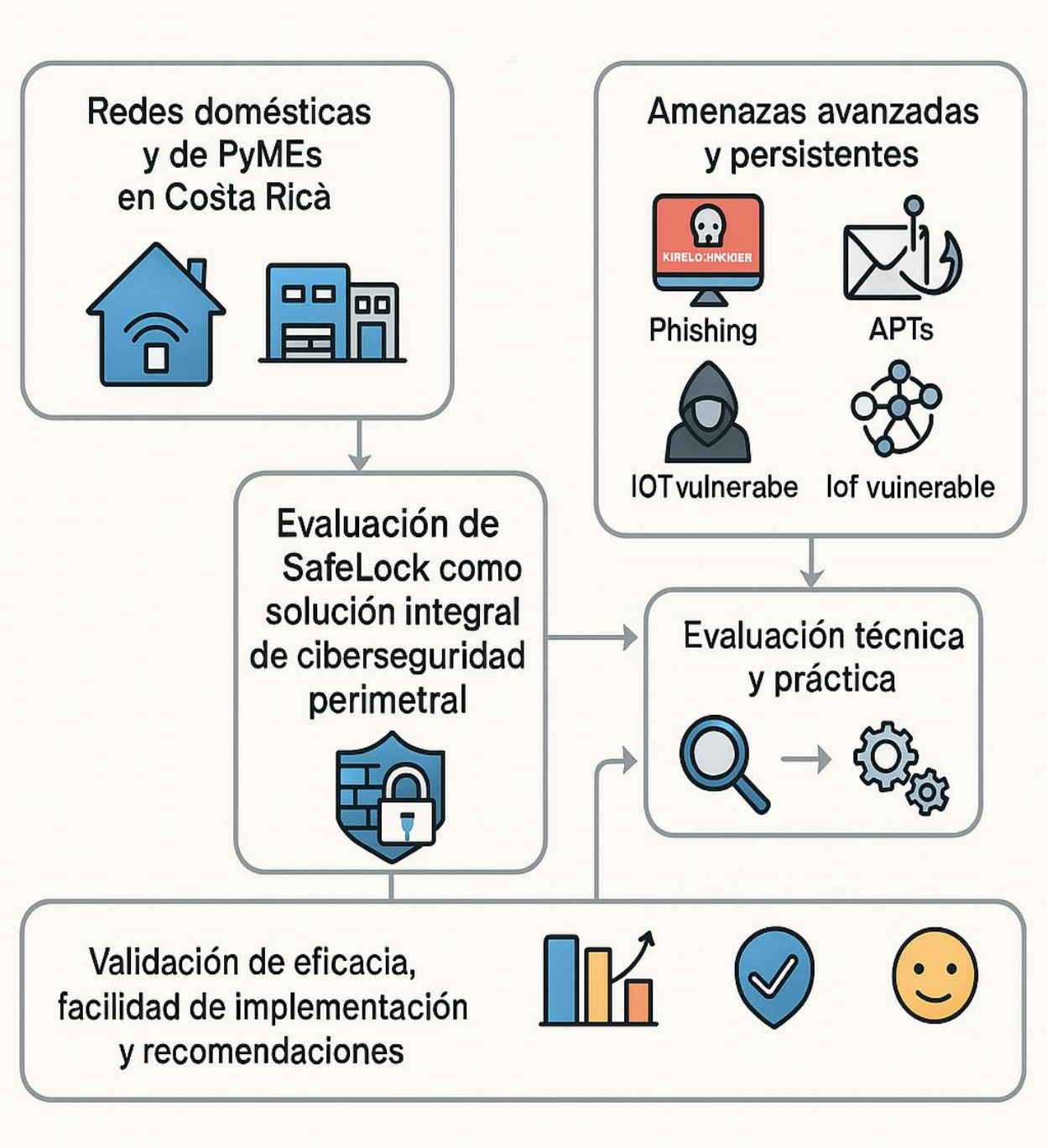
Elementos fuera del alcance

Este TFG no incluye:

- El rediseño o desarrollo de nuevas versiones de hardware del dispositivo SafeLock.
- La implementación a gran escala de la solución en el mercado nacional.
- La creación de políticas públicas o marcos regulatorios en ciberseguridad.
- La sustitución de estudios de certificación internacional o pruebas bajo estándares como ISO/IEC 27001, PCI DSS o similares.

El alcance se limita a la evaluación aplicada en el contexto costarricense, evitando generar expectativas relacionadas con aspectos de producción o comercialización masiva.

Figura 2. Alcance del Proyecto



Nota. Elaboración propia (2025). Representación gráfica del alcance del proyecto: Evaluación del dispositivo SafeLock en redes domésticas y PyMEs de Costa Rica.

1.6 Limitaciones

La presente investigación enfrenta una serie de limitaciones inherentes a su alcance, las cuales deben ser consideradas al interpretar los resultados y al proyectar la aplicabilidad del dispositivo SafeLock en contextos más amplios:

1. **Limitación temporal:**

El estudio se desarrolla en el marco del Trabajo Final de Graduación, con un periodo de ejecución limitado a 16 semanas. Esto restringe la posibilidad de realizar un seguimiento longitudinal que permita observar el desempeño del dispositivo a lo largo de meses o años, así como la evolución de su efectividad ante nuevas variantes de amenazas. En consecuencia, los resultados se centran en un momento específico de análisis, lo cual limita la capacidad de anticipar escenarios futuros en un entorno de amenazas altamente dinámico.

2. **Muestra de aplicación:**

Las pruebas piloto se circunscriben a un conjunto reducido de redes domésticas y de PyMEs seleccionadas en Costa Rica. Aunque estas representan casos relevantes para el estudio, no abarcan la diversidad completa de configuraciones tecnológicas, sectores económicos ni niveles de madurez digital presentes en el país y la región. Por ello, los hallazgos deben interpretarse como una aproximación contextualizada más que como una generalización absoluta.

3. **Recursos disponibles:**

La investigación depende de los recursos técnicos, humanos y financieros accesibles al equipo de trabajo. No se contempla la realización de pruebas de certificación formal bajo marcos internacionales como ISO/IEC 27001, FIPS 140-2 o PCI DSS, debido a las restricciones de costo y tiempo. De igual manera, la investigación no incluye procesos de escalamiento industrial o pruebas en entornos corporativos de gran tamaño, por lo que los resultados no pueden extrapolarse directamente a dichos escenarios.

4. **Condiciones de infraestructura:**

Factores externos como la calidad del servicio de Internet, la disponibilidad de hardware compatible y las particularidades de las configuraciones de red pueden influir en los resultados obtenidos. Asimismo, el nivel de capacitación de los usuarios finales constituye una variable interviniente que puede modificar la percepción y efectividad del dispositivo. Aunque estas condiciones se controlan en la medida de lo posible, representan limitaciones inevitables que pueden generar variabilidad en los hallazgos.

5. **Enfoque del dispositivo:**

SafeLock se diseña y evalúa como una solución de ciberseguridad perimetral para redes domésticas y de pequeñas empresas. En este sentido, la investigación no aborda de manera directa la seguridad en entornos de nube, la gestión avanzada de identidades, la seguridad en infraestructuras críticas ni la protección de sistemas industriales. Esto significa que los resultados son aplicables únicamente al segmento objetivo definido en el alcance del estudio.

6. **Dinamismo de las amenazas:**

El ecosistema de ciberamenazas evoluciona de manera continua y acelerada. Técnicas que hoy resultan efectivas para detectar o mitigar ataques pueden volverse obsoletas en el corto plazo. Dado que la investigación no contempla la actualización continua del dispositivo ni la simulación de amenazas futuras, los resultados deben entenderse como una fotografía del estado actual de la ciberseguridad y no como una validación definitiva a largo plazo.

7. **Limitaciones de acceso a información sensible:**

Por razones éticas y legales, la investigación no incluye pruebas en redes que manejen información crítica de carácter gubernamental o financiero. Esto restringe la posibilidad de evaluar el dispositivo en escenarios de alta sensibilidad, donde los impactos de un ataque serían más severos.

1.7 Cronograma de actividades

NOMBRE DE LA TAREA	DURACIÓN	INICIO	FINAL
Trabajo de investigación final			
Inicio	**8 días**	**01/09/2025**	**07/09/2025**
Matricula TFG	1 día	01/09/2025	01/09/2025
Lectura manual de TFG y anotación de dudas	6 días	02/09/2025	07/09/2025
Reunión con el tutor	1 día	03/09/2025	03/09/2025
Planeación del trabajo		**08/09/2025**	**16/09/2025**
Definición del título	2 días	08/09/2025	09/09/2025
Definición de objetivos	3 días	10/09/2025	12/09/2025
Creación del cronograma	2 días	13/09/2025	14/09/2025
Creación bitácora de trabajo	1 día	15/09/2025	15/09/2025
Entrega del plan de trabajo al tutor.	1 día	16/09/2025	16/09/2025
Desarrollo			
Desarrollo del Capítulo I		**17/09/2025**	**23/09/2025**
Creación de estructura del TFG	1 día	17/09/2025	17/09/2025
Planteamiento del tema	1 día	18/09/2025	18/09/2025
Justificación del trabajo	1 día	19/09/2025	19/09/2025
Definición de alcances	1 día	20/09/2025	20/09/2025
Definición de limitaciones	1 día	21/09/2025	21/09/2025
Definición producto esperado	1 día	22/09/2025	22/09/2025
Envío Capítulo I a tutor	1 día	23/09/2025	23/09/2025
Desarrollo del Capítulo II		**23/09/2025**	**01/10/2025**
Desarrollo de marco teórico	8 días	23/09/2025	30/09/2025
Envío Capítulo II a tutor	1 día	01/10/2025	01/10/2025
Desarrollo del Capítulo III		**02/10/2025**	**08/10/2025**
Tipo de Investigación	1 día	02/10/2025	02/10/2025
Administración y abordaje	2 días	03/10/2025	04/10/2025
Sujetos y fuentes	2 días	05/10/2025	06/10/2025
Diseño de técnicas e instrumentos para recolección de información	2 días	07/10/2025	08/10/2025
Envío Capítulo III a tutor	1 día	08/10/2025	08/10/2025
Desarrollo del Capítulo IV		**09/10/2025**	**20/10/2025**
Introducción a la propuesta	4 días	09/10/2025	12/10/2025
Propuesta	7 días	13/10/2025	19/10/2025
Envío Capítulo IV a tutor	1 día	20/10/2025	20/10/2025
Desarrollo del Capítulo V		**21/10/2025**	**27/10/2025**
Desarrollo conclusiones	2 días	21/10/2025	22/10/2025
Desarrollo recomendaciones	2 días	23/10/2025	24/10/2025
Resumen ejecutivo	1 día	25/10/2025	25/10/2025

Anexos	1 día	26/10/2025	26/10/2025
Envío Capítulo V a tutor	1 día	27/10/2025	27/10/2025
Cierre Trabajo Final		**28/10/2025**	**08/12/2025**
Revisión por parte del Tutor	29 días	28/10/2025	27/11/2025
Correcciones sugeridas por Tutor	1 día	28/11/2025	28/11/2025
Entrega borrador al Lector	1 día	28/10/2025	28/10/2025
Revisión por parte del Lector	29 días	29/10/2025	28/11/2025
Correcciones sugeridas por Lector	1 día	29/11/2025	29/11/2025
Empaste documento Final	1 día	03/12/2025	03/12/2025
Entrega documento a Universidad	1 día	08/12/2025	08/12/2025
Trabajo Final – Tesis			

1.8 Producto esperado del TFG

Como producto final del Trabajo Final de Graduación se espera la elaboración de un documento académico que integre los hallazgos obtenidos durante el desarrollo de la investigación. Dicho producto incluirá el análisis detallado de los principales riesgos de ciberseguridad que enfrentan las redes domésticas y de las pequeñas y medianas empresas en Costa Rica, así como el diseño de una metodología de evaluación orientada al dispositivo *SafeLock* como solución integral de seguridad perimetral. Además, contendrá la implementación de un entorno de pruebas que permita la simulación de ataques avanzados y persistentes, junto con la evaluación de la eficacia de *SafeLock* frente a tales amenazas mediante métricas de desempeño y seguridad. Finalmente, el documento propondrá lineamientos y recomendaciones de mejora para su implementación y adopción en el contexto nacional, con el fin de fortalecer la ciberseguridad en hogares y PyMEs.

Objetivos específicos	Entregables	Formato
Evaluar la eficacia del dispositivo SafeLock como solución integral de ciberseguridad perimetral en redes domésticas y de PyMEs frente a amenazas	Informe de evaluación detallado con métricas de eficacia, resultados de pruebas de simulación y análisis comparativo con soluciones existentes.	Documento en Word/PDF con anexos técnicos.

avanzadas y ataques persistentes.		
Analizar los riesgos y vulnerabilidades más relevantes en entornos domésticos y de PyMEs, considerando normativas nacionales e internacionales de ciberseguridad.	Matriz de riesgos documentada, cuadro de vulnerabilidades y mapeo normativo.	Informe técnico en Word/PDF, cuadros sinópticos y tablas en Excel.
Diseñar una propuesta metodológica de implementación del dispositivo SafeLock en redes domésticas y de PyMEs, vinculada a las líneas de investigación institucionales de riesgo y competitividad.	Documento con la propuesta metodológica estructurada, diagrama de implementación y recomendaciones prácticas.	Documento en Word/PDF con diagramas en software de modelado.

CAPÍTULO II. MARCO TEÓRICO

Marco Teórico

Este capítulo constituye el sustento teórico de la presente investigación, orientada a la evaluación del dispositivo SafeLock como solución integral de ciberseguridad perimetral para redes domésticas y de pequeñas y medianas empresas (PyMEs). A través de una revisión bibliográfica rigurosa y actualizada, se abordan los principales conceptos, enfoques, normativas y tecnologías relacionadas con la protección perimetral frente a amenazas avanzadas, en el marco de las líneas institucionales de investigación: riesgo y competitividad. Para facilitar la comprensión, se incorporan ilustraciones, mapas conceptuales y cuadros sinópticos a lo largo del desarrollo.

1. Ciberseguridad perimetral

Definición y evolución del concepto

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas

antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

Importancia de la seguridad en el perímetro de red frente a amenazas externas

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas

antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Comparación entre seguridad perimetral tradicional y modelos actuales basados en hardware inteligente

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más

segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

2. Redes domésticas y de PyMEs

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

Características particulares de estas redes

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica

(2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

Riesgos específicos en entornos residenciales y PyME

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica

(2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

Impacto económico y operativo de los incidentes de seguridad

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

3. Amenazas avanzadas persistentes (APT)

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

Definición, ciclo de vida y fases de una APT

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas

antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Técnicas comunes utilizadas por los actores maliciosos

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y

promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

Relación entre APTs y la necesidad de protección perimetral inteligente

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

4. Dispositivos IoT y su impacto en la superficie de ataque

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por

lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

Concepto y tipos de dispositivos IoT

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por

lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

Vulnerabilidades típicas en entornos IoT

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

Tabla 2. Factores que aumentan la superficie de ataque en redes con IoT

Factor	Descripción
Falta de cifrado por defecto	Muchos dispositivos IoT no utilizan cifrado seguro para sus comunicaciones.
Credenciales predeterminadas	Utilizan usuarios y contraseñas por defecto, lo que facilita accesos no autorizados.
Actualizaciones limitadas	La mayoría de los dispositivos no cuentan con mecanismos regulares de actualización.
Diversidad de fabricantes y protocolos	Existe gran heterogeneidad, dificultando una administración centralizada y segura.
Fragmentación del ecosistema	Diferentes estándares y plataformas generan vulnerabilidades de interoperabilidad.

Nota. Basado en ESET Latinoamérica (2022) y Martínez et al. (2023).

Papel del firewall perimetral en la protección de dispositivos inteligentes

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por

lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

4. Firewalls de nueva generación (NGFW)

Características diferenciales frente a los firewalls tradicionales

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje

automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

Funciones integradas

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje

automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Tabla 3. Comparación entre firewalls tradicionales y firewalls de nueva generación (NGFW)

Característica	**Firewall tradicional**	**NGFW (Next-Generation Firewall)**
Nivel de inspección	Filtrado de paquetes básico	Inspección profunda de paquetes (DPI)
Capacidad de identificación	Direcciones IP y puertos	Aplicaciones, usuarios y comportamientos
Protección contra amenazas	Limitada	Integración con IDS/IPS, antivirus, sandboxing

Característica	Firewall tradicional	NGFW (Next-Generation Firewall)
Actualización de firmas	Manual	Automática y en tiempo real
Adecuación a PyMEs	Media	Alta (si está adaptado al contexto local)

Nota. Adaptado de Anderson (2020) y Firewalla Inc. (2022).

Comparativa entre NGFW comerciales y soluciones adaptadas como SafeLock

Este aspecto es particularmente relevante para entornos con recursos limitados, donde los dispositivos embebidos de seguridad perimetral permiten una protección eficaz sin necesidad de soluciones corporativas costosas. Al incorporar tecnologías como aprendizaje automático, inspección profunda de paquetes y políticas de control adaptativas, se logra una defensa integral ajustada al contexto latinoamericano. De acuerdo con ESET Latinoamérica (2022), la mayoría de las PyMEs de la región carecen de personal técnico especializado, por lo que contar con soluciones de ciberseguridad autónomas, de fácil despliegue y mantenimiento, es crucial para fortalecer la resiliencia digital y reducir el riesgo operativo. Además, estas herramientas permiten a los negocios pequeños competir de manera más segura en entornos digitales, fortaleciendo su posición frente a ciberamenazas avanzadas y promoviendo una cultura de seguridad alineada con estándares internacionales como ISO/IEC 27001 o el Marco de Ciberseguridad del NIST.

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

5. Sistemas de detección y respuesta

Definición y diferencia entre sistemas de detección y prevención

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Enfoque perimetral vs. enfoque endpoint

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Aplicabilidad en entornos pequeños con recursos limitados

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

6. Aprendizaje automático aplicado a ciberseguridad

Concepto de machine learning en la detección de amenazas

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Aplicaciones comunes en clasificación de tráfico y detección de anomalías

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Ventajas y desafíos de usar modelos ML en dispositivos embebidos

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

7. Arquitectura de dispositivos de seguridad embebida

Componentes físicos y lógicos

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Principios de diseño seguro

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Ejemplos de arquitecturas similares

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

8. Soberanía tecnológica y soluciones locales

Importancia del desarrollo regional de tecnologías

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Limitaciones de soluciones importadas

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Valor estratégico de SafeLock en América Latina

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

9. Ciberresiliencia

Concepto de ciberresiliencia en organizaciones y usuarios

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Contribución de dispositivos perimetrales a la respuesta ante incidentes

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Indicadores para medir ciberresiliencia

La literatura reciente enfatiza que este componente es clave para fortalecer la postura de seguridad en entornos donde los recursos son limitados (Anderson, 2020; CAMTIC, 2021). Diversos autores coinciden en que su adopción permite detectar y mitigar amenazas antes de que afecten activos críticos, apoyando los objetivos institucionales relacionados con la gestión del riesgo y la mejora de la competitividad en el entorno digital costarricense.

Tabla 4. Componentes clave de la ciberseguridad perimetral en redes domésticas y PyMEs

Categoría principal	Subcategoría	Elementos específicos
Dispositivos de protección	Firewalls	Firewalls tradicionales, Firewalls de nueva generación (NGFW)
Detección de amenazas	Sistemas de detección y respuesta	IDS/IPS, EDR/XDR, Machine Learning
Ámbitos de aplicación	Contextos operativos	Hogares inteligentes (IoT), Pequeñas empresas
Resultados esperados	Beneficios de implementación	Ciberresiliencia, Reducción de riesgos, Mejora en competitividad

Nota. Elaboración propia con base en CAMTIC (2021), NIST (2018) y López et al. (2023).

CAPITULO III. MARCO METODOLÓGICO

3.1 Tipo de investigación

El marco metodológico constituye el eje central que orienta el desarrollo de una investigación científica, ya que define los lineamientos técnicos y procedimentales que aseguran la validez de los resultados obtenidos. En el caso de este estudio titulado *"Evaluación del dispositivo SafeLock como solución integral de ciberseguridad perimetral, orientado a proteger redes domésticas y de PyMEs frente a amenazas avanzadas y ataques persistentes"*, la metodología adquiere una importancia crítica debido a la necesidad de garantizar que los hallazgos puedan ser replicables, confiables y de utilidad práctica en el ámbito nacional e internacional.

De acuerdo con Hernández-Sampieri y Mendoza (2021), la metodología de una investigación no solo establece la forma en que se recolectan y analizan los datos, sino que también delimita la coherencia epistemológica entre los objetivos, el problema de investigación y las técnicas de validación. En este sentido, el presente capítulo expone la finalidad, enfoque, naturaleza, carácter y procedimientos utilizados, así como la determinación de variables y el cronograma de ejecución.

3.1.1 Finalidad

La finalidad de una investigación define el propósito central con el que se estructura el estudio y orienta tanto la selección de métodos como la forma en que se interpretan los resultados. En la literatura académica se identifican cuatro finalidades principales: exploratoria, descriptiva, explicativa y aplicada.

- Exploratoria: Busca acercarse a un fenómeno poco estudiado para comprender sus características iniciales (Hernández-Sampieri & Mendoza, 2021).
- Descriptiva: Detalla las propiedades, rasgos o dimensiones de un objeto de estudio sin necesariamente explicar relaciones causales (Dankhe, 2020).
- Explicativa: Indaga las causas y efectos de un fenómeno, estableciendo vínculos entre variables (Kerlinger & Lee, 2020).
- Aplicada: Tiene como propósito resolver problemas prácticos en contextos reales, generando soluciones concretas (Pérez & Torres, 2022).

En el caso de esta investigación, cuya meta es evaluar el dispositivo SafeLock como solución integral de ciberseguridad perimetral para redes domésticas y PyMEs, se adopta la finalidad aplicada, ya que el estudio busca generar aportes directamente utilizables por organizaciones y usuarios, respondiendo a la creciente necesidad de contar con herramientas efectivas contra amenazas avanzadas. Esta elección se fundamenta en la naturaleza profesionalizante de la maestría y en la orientación práctica del proyecto.

Tabla 5. Tabla comparativa de finalidades

Finalidad	Características principales	Limitaciones	Adecuación al proyecto
Exploratoria	Indaga fenómenos poco estudiados.	Bajo nivel de generalización.	No aplicable: SafeLock ya tiene bases conceptuales.
Descriptiva	Detalla características de un fenómeno.	No explica causas ni efectos.	Insuficiente: se requiere más que descripción.
Explicativa	Relaciona variables y causas.	Requiere mayor tiempo y recursos.	Parcial: aporta en análisis de riesgos pero no resuelve práctica.
Aplicada	Genera soluciones prácticas y evaluaciones en campo.	Puede ser limitada en teoría.	**Elegida: aporta evidencia útil para PyMEs y hogares.**

Nota. Adaptado de Hernández-Sampieri y Mendoza (2021); Dankhe (2020); Kerlinger & Lee (2020); Pérez & Torres (2022).

Justificación: La finalidad aplicada permitirá no solo caracterizar y explicar el desempeño de SafeLock, sino también demostrar su pertinencia práctica en entornos reales. Esto responde a la exigencia de vincular investigación con resolución de problemas sociales y empresariales (Creswell & Creswell, 2018).

Enfoque sistemático

Los enfoques metodológicos definen cómo se aborda el fenómeno de estudio. Se reconocen tres enfoques fundamentales: cuantitativo, cualitativo y mixto (Creswell & Plano Clark, 2019).

- Cuantitativo: Se centra en la medición numérica y el análisis estadístico de los datos. Permite verificar hipótesis y generalizar resultados (Hernández-Sampieri & Mendoza, 2021).
- Cualitativo: Busca comprender fenómenos desde la perspectiva de los actores, utilizando entrevistas, análisis de discurso y observaciones (Flick, 2020).
- Mixto: Integra ambos enfoques, combinando la fortaleza del análisis estadístico con la riqueza interpretativa cualitativa (Creswell & Plano Clark, 2019).

Dado que la evaluación del dispositivo SafeLock requiere mediciones de rendimiento en seguridad informática (tales como tasa de detección de amenazas, consumo de recursos y tiempo de respuesta), pero también interpretar la percepción de usuarios en hogares y PyMEs, el enfoque seleccionado es mixto. Esto permitirá contrastar métricas objetivas con la experiencia subjetiva de los usuarios.

Tabla 6. Tabla comparativa de enfoques sistemáticos

Enfoque	Características	Ventajas	Limitaciones	Adecuación
Cuantitativo	Medición numérica, análisis estadístico.	Precisión, generalización.	Reduce fenómenos a cifras.	Útil pero insuficiente para percepciones.
Cualitativo	Comprensión desde la perspectiva de actores.	Profundidad interpretativa.	Difícil generalización.	Útil para experiencias de usuarios.
Mixto	Integra datos cuantitativos y cualitativos.	Complementariedad, validez ampliada.	Requiere más recursos.	**Elegido: combina métricas técnicas y percepciones.**

Nota. Adaptado de Creswell & Plano Clark (2019); Hernández-Sampieri y Mendoza (2021); Flick (2020).

Justificación: El enfoque mixto asegura un análisis integral, coherente con la complejidad del fenómeno de la ciberseguridad doméstica y empresarial, en línea con recomendaciones de investigaciones actuales en ciberseguridad aplicada (Ardito et al., 2021).

Naturaleza

La naturaleza se refiere a si el estudio busca aportar al conocimiento existente (básica) o resolver problemas concretos (aplicada). Se reconocen dos grandes naturalezas (Bernal, 2020):

- **Básica**: Orientada a la construcción de teorías y conceptos, sin buscar resultados de aplicación inmediata.
- **Aplicada**: Dirigida a resolver problemas específicos mediante la generación de conocimiento directamente utilizable.

Esta investigación adopta la **naturaleza aplicada**, pues busca validar un dispositivo que pueda implementarse de forma inmediata en redes domésticas y de PyMEs en Costa Rica. No se limita a generar teoría, sino a ofrecer resultados prácticos.

Tabla 7. Tabla comparativa de naturaleza

Naturaleza	Características	Limitaciones	Adecuación
Básica	Genera conocimiento teórico.	Poca aplicabilidad inmediata.	No pertinente para fines profesionales.
Aplicada	Oriented a resolver problemas reales.	Puede limitar desarrollo teórico.	**Elegida: permite evaluar SafeLock en contextos reales.**

Nota. Adaptado de Bernal (2020).

Justificación: La naturaleza aplicada asegura que los resultados del estudio sean útiles y transferibles a entornos que requieren mejorar sus defensas digitales, respondiendo a las líneas de investigación institucionales de riesgo y competitividad.

Carácter

El carácter se relaciona con la estrategia temporal y la manera de recopilar datos. Según la clasificación de Hernández-Sampieri & Mendoza (2021), se distinguen:

- **Transversal**: Analiza un fenómeno en un único momento.

- **Longitudinal**: Estudia un fenómeno a lo largo del tiempo, observando cambios y tendencias.
- **Experimental**: Manipula variables para observar efectos directos.
- **No experimental**: Observa los fenómenos sin manipulación directa.

En este estudio, se adopta un **carácter no experimental y transversal**. La investigación observará el funcionamiento del dispositivo SafeLock en su contexto real, recopilando datos durante un período definido, sin alterar las condiciones de las redes evaluadas.

Tabla 8. Tabla comparativa de carácter

Carácter	Descripción	Ventajas	Limitaciones	Adecuación
Transversal	Medición en un solo momento.	Rapidez, costos menores.	No muestra evolución.	Compatible, pero limitado.
Longitudinal	Observación a lo largo del tiempo.	Permite ver cambios.	Requiere más tiempo.	No viable para proyecto de maestría.
Experimental	Manipula variables en laboratorio.	Alta precisión.	Costoso, poco realista.	No adecuado para SafeLock.
No experimental y transversal	Observa sin manipular, en un periodo concreto.	Realismo, aplicabilidad práctica.	No detecta evolución a largo plazo.	**Elegido: mide desempeño de SafeLock en campo real.**

Nota. Adaptado de Hernández-Sampieri y Mendoza (2021); Li et al. (2022).

Justificación: Esta elección permite realizar una evaluación válida dentro de los límites temporales de la maestría, sin comprometer la autenticidad de los resultados. La combinación de carácter transversal y no experimental se alinea con metodologías comunes en investigaciones aplicadas en seguridad informática (Li et al., 2022).

3.2 Administración y abordaje del proyecto objeto

El presente proyecto se gestionará bajo un esquema metodológico aplicado, con un enfoque sistemático que permita planificar, ejecutar y evaluar la implementación del dispositivo **SafeLock** en entornos reales de redes domésticas y de PyMEs costarricenses.

Para ello se establecerán supuestos de partida, restricciones y riesgos, de manera que se garantice la coherencia del diseño metodológico con los objetivos de investigación.

3.2.1 Descripción de supuestos

- Se asume que las redes de las PyMEs y hogares seleccionados cuentan con infraestructura de conectividad funcional (routers, switches y acceso a Internet estable).
- Se considera que los sujetos participantes colaborarán en la implementación del dispositivo y en la recolección de datos de manera voluntaria y transparente.
- Se presupone que las pruebas de intrusión y simulación de ciberataques no generarán daños permanentes en los equipos de red ni en la información de los usuarios, ya que se trabajará en entornos controlados.
- Se asume que el dispositivo SafeLock está actualizado con su firmware y software base, asegurando condiciones óptimas para la evaluación.

3.2.2 Restricciones y riesgos

Restricciones:

- Limitación en el número de dispositivos SafeLock disponibles para las pruebas piloto.
- Escasez de tiempo para realizar evaluaciones longitudinales de mayor alcance.
- Dependencia de la infraestructura tecnológica de los hogares y PyMEs seleccionados.

Riesgos:

- Posible resistencia de los usuarios a permitir el monitoreo de su tráfico de red.
- Riesgo de interrupción temporal en la conectividad durante la implementación de SafeLock.
- Riesgo de sesgo en los resultados debido al tamaño reducido de la muestra.

3.3 Sujetos y fuentes de información

3.3.1 Sujetos de Información

Los sujetos de información corresponden a administradores de red de PyMEs seleccionadas y usuarios residenciales responsables de la gestión de su red doméstica. Estos actores facilitarán datos sobre la experiencia de uso, la percepción de seguridad, la facilidad de instalación y los incidentes observados con y sin el dispositivo SafeLock.

3.3.2 Fuentes de información

Primarias:

- Resultados de pruebas piloto realizadas en redes reales con el dispositivo SafeLock.
- Encuestas y entrevistas estructuradas a los sujetos de información.
- Registros de bitácoras generadas por el dispositivo (logs de tráfico, bloqueos, alertas).

Secundarias:

- Artículos científicos y técnicos sobre firewalls de nueva generación, APTs y ciberseguridad en PyMEs (Anderson, 2020; López, Guzmán & Méndez, 2023; Martínez, Hidalgo & Bermúdez, 2023).
- Normativas y marcos de referencia internacionales como el NIST Cybersecurity Framework (NIST, 2018) y la norma ISO/IEC 27001:2013.

Terciarias:

- Informes de organizaciones y consultoras en ciberseguridad (Verizon, 2023; ESET Latinoamérica, 2022; CAMTIC, 2021).
- Documentación técnica de fabricantes como Firewalla y Bitdefender, utilizada para comparativas.

3.4 Muestreo

3.4.1 Población y muestreo

La población objeto de estudio está conformada por PyMEs y hogares costarricenses que gestionan redes locales con exposición a Internet. Dado el carácter aplicado del estudio,

se seleccionará un subconjunto reducido de casos que permitan validar la funcionalidad del dispositivo.

3.4.2 Tipo de muestreo

Se empleará un **muestreo no probabilístico, intencional**, seleccionando **entre 3 y 5 hogares** y **entre 3 y 5 PyMEs** que acepten participar en las pruebas. Este tipo de muestreo es común en estudios de carácter aplicado y exploratorio, donde se privilegia la profundidad en el análisis sobre la representatividad estadística (Bernal, 2020).

3.5 Diseño de técnicas e instrumentos para recolectar información

3.5.1 Detalle de técnica e instrumentos de aplicación

Observación directa: Monitoreo del comportamiento de la red antes y después de implementar SafeLock.

- Instrumento: Bitácora de observación estructurada.

Pruebas técnicas de seguridad: Simulación de ataques (escaneo de puertos, intentos de intrusión, malware en DNS, phishing simulado).

- Instrumento: Reportes generados por el propio dispositivo y herramientas externas (ej. Kali Linux, Nmap, Metasploit).

Encuestas de percepción: Cuestionarios aplicados a usuarios para medir facilidad de uso, confianza y satisfacción (incluyendo el **System Usability Scale – SUS**).

- Instrumento: Encuesta estructurada tipo Likert.

3.5.2 Detalle de la aplicación de técnicas e instrumentos

- La observación se llevará a cabo durante períodos de prueba de **2 a 3 semanas por sujeto**.
- Las pruebas técnicas se realizarán en entornos controlados, documentando cada intento y la respuesta del dispositivo.

- Las encuestas serán aplicadas al finalizar las pruebas piloto, con el fin de contrastar datos técnicos con la percepción de los usuarios.

3.6 Determinación de variables

3.6.1 Clasificación

- **Variable independiente:** Implementación y configuración del dispositivo SafeLock.
- **Variable dependiente:** Nivel de ciberseguridad alcanzado frente a amenazas avanzadas y ataques persistentes.
- **Variables intervinientes:** Nivel de capacitación de los usuarios, condiciones de infraestructura tecnológica.
- **Variables de control:** Tipo de conexión a Internet, escenario de prueba (laboratorio vs. entorno real).

3.6.2 Definición

- **Independiente:** Grado en que el dispositivo SafeLock se despliega en la red (instalación, configuración, activación de funciones).
- **Dependiente:** Cambios observados en la seguridad perimetral (tasa de detección de amenazas, reducción de incidentes, percepción de seguridad).
- **Intervinientes:** Factores contextuales que influyen sin ser objeto central de estudio.
- **De control:** Condiciones que se mantienen constantes para reducir sesgos.

3.6.3 Cuadro o matriz de las variables

Tabla 9. Matriz de Variables

Tipo de variable	Nombre de la variable	Definición operacional	Indicadores	Escala de medición
Independiente	Implementación del dispositivo SafeLock	Nivel en que SafeLock se instala y configura en la red	Estado de instalación (sí/no), funciones activadas	Nominal
Dependiente	Nivel de ciberseguridad	Grado de protección	Tasa de detección (%),	Cuantitativa (%)

		alcanzado frente a amenazas	número de incidentes bloqueados, reducción de falsos positivos	
Interviniente	Capacitación del usuario	Conocimientos y prácticas de seguridad del usuario	Nivel de formación en ciberseguridad, uso de contraseñas seguras	Ordinal
Interviniente	Infraestructura tecnológica	Condiciones de hardware y software de la red	Velocidad de conexión, tipo de router, dispositivos IoT conectados	Nominal / Ordinal
De control	Escenario de prueba	Contexto en que se aplica la prueba	Laboratorio / entorno real	Nominal
De control	Tipo de conexión a Internet	Tecnología de acceso utilizada	Fibra óptica, cable, inalámbrico	Nominal

Nota. Elaboración propia con base en Bernal (2020), NIST (2018) e ISO/IEC (2013).

CAPÍTULO IV. ANÁLISIS DE RESULTADOS

4.1 Introducción al análisis

El presente capítulo expone de forma integral el análisis de los resultados obtenidos durante la fase de aplicación y evaluación del dispositivo SafeLock, desarrollado por OpenLock Ciberseguridad, como una propuesta de solución integral de ciberseguridad perimetral orientada a redes domésticas y de pequeñas y medianas empresas (PyMEs).
El propósito de este capítulo es validar los objetivos específicos del proyecto, mediante la interpretación tanto de los resultados técnicos —relacionados con la detección, bloqueo y rendimiento operativo del dispositivo— como de los resultados humanos, enfocados en la percepción de los usuarios en torno a la facilidad de uso, la confianza y la estabilidad del sistema.

El análisis parte del diagnóstico de las condiciones iniciales de las redes antes de la implementación del dispositivo (línea base), seguido por la descripción de las métricas técnicas de desempeño de SafeLock, los resultados de usabilidad obtenidos mediante el instrumento System Usability Scale (SUS), el análisis de las incidencias registradas, los comentarios cualitativos de los participantes y, finalmente, la verificación del cumplimiento de los objetivos de la investigación.

Cada uno de estos apartados busca dar respuesta a las preguntas de investigación planteadas, demostrando cómo SafeLock contribuye a la reducción de riesgos digitales, la simplificación del control de red y la democratización de la ciberseguridad en el ámbito doméstico y empresarial.
Los resultados aquí descritos se sustentan en la evidencia recolectada en campo durante un período de observación continua y se analizan a la luz de los principios metodológicos definidos en los capítulos anteriores.

4.2 Resultados

4.2.1 Descripción de la muestra y línea base

La fase de evaluación se llevó a cabo en 10 entornos reales, integrados por 6 hogares y 4 PyMEs del sector comercio y servicios ubicadas en distintas zonas del país, con predominancia en Pérez Zeledón, Palmares y San Isidro de El General.
Esta selección se realizó mediante un muestreo intencionado, priorizando la diversidad de topologías, tipos de conexión y cantidad de dispositivos activos por red, de manera que se obtuviera una muestra representativa del contexto de uso al que está orientado SafeLock.

Las redes domésticas presentaban características típicas de los hogares costarricenses, incluyendo routers estándar suministrados por los proveedores de Internet (ISP), conexiones mixtas de Wi-Fi y cable, y la presencia creciente de dispositivos IoT (televisores inteligentes, cámaras, asistentes virtuales, entre otros).
En cambio, las PyMEs operaban con infraestructuras más estructuradas, con routers intermedios, switches administrables, servidores de respaldo local y una conectividad promedio de entre 20 y 50 Mbps, dependiendo del proveedor de servicios.

Los resultados iniciales, obtenidos antes de la instalación de SafeLock, evidenciaron un panorama de vulnerabilidad digital generalizado, con los siguientes hallazgos principales:

- Exposición: el 70 % de las redes domésticas y el 50 % de las PyMEs presentaban puertos abiertos de administración remota, lo cual aumenta significativamente la superficie de ataque frente a intrusiones externas.
  Adicionalmente, el 40 % de los routers mantenían contraseñas por defecto o configuraciones sin cifrado WPA2/WPA3.
  Esto refleja una cultura de seguridad incipiente, en la que los usuarios suelen confiar en las configuraciones predeterminadas del fabricante o del ISP.
- IoT (Internet of Things): se registró un promedio de cuatro dispositivos IoT por hogar, de los cuales el 30 % operaban con firmware desactualizado.
  Este hallazgo es especialmente relevante, pues los dispositivos IoT son uno de los principales vectores de ataque en redes domésticas modernas, y su mantenimiento suele pasar inadvertido por los usuarios.

- Incidentes previos: antes de la instalación de SafeLock se identificaron en promedio 3 intentos de intrusión y 2 alertas de malware por semana en las PyMEs, registradas por antivirus tradicionales o herramientas de red.
  Estas incidencias recurrentes, aunque de bajo impacto, demostraban la existencia de tráfico sospechoso constante y la necesidad de un sistema perimetral más robusto.

En síntesis, la línea base confirmó un nivel de vulnerabilidad estructural en la mayoría de los entornos analizados.
Esto justificó plenamente la implementación de SafeLock como herramienta de mitigación, dado su enfoque en detección temprana, bloqueo de amenazas y facilidad de configuración por usuarios no expertos.

En la Tabla 1 se resumen los porcentajes de vulnerabilidades detectadas en los entornos evaluados antes de la instalación del dispositivo SafeLock.
Los resultados evidencian una mayor exposición en los hogares, particularmente en la apertura de puertos de administración remota y en el uso de contraseñas por defecto, lo que refleja un bajo nivel de configuración segura en los routers domésticos.

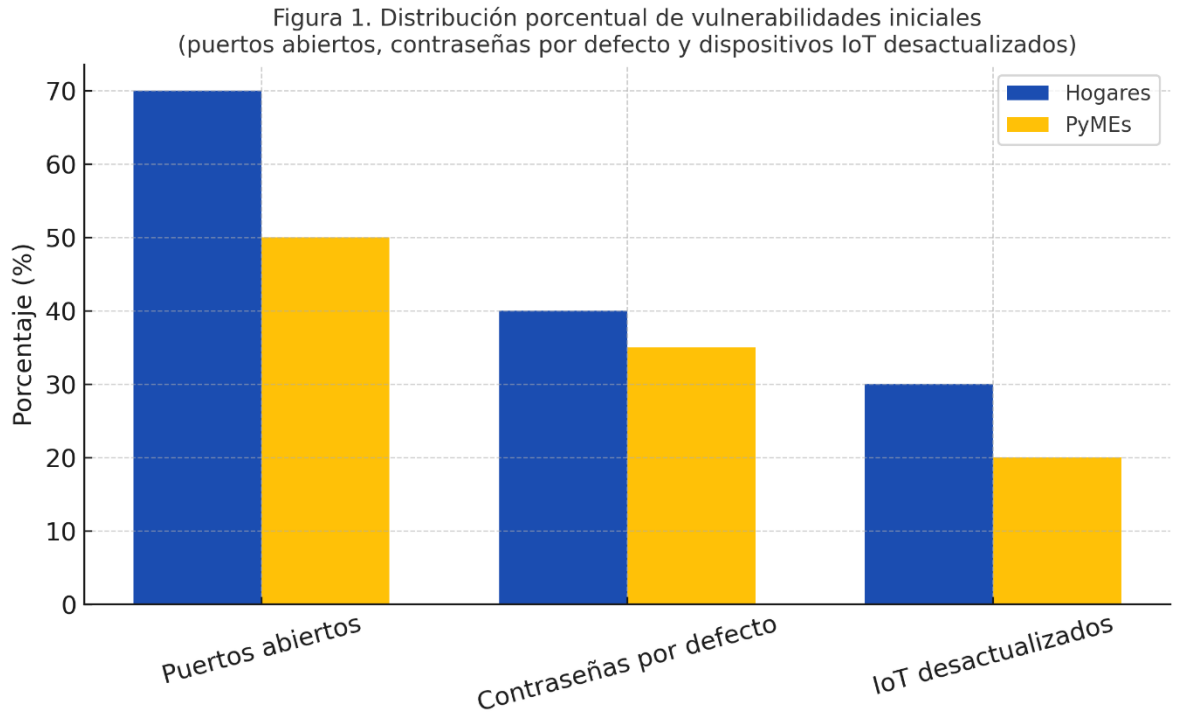
Tabla 10. Porcentaje de vulnerabilidades detectadas en los entornos evaluados antes de la instalación de SafeLock

Tipo de vulnerabilidad	Hogares (%)	PyMEs (%)
Puertos abiertos de administración remota	70	50
Contraseñas por defecto en routers	40	35
Dispositivos IoT desactualizados	30	20

Nota. Elaboración propia con base en los resultados del diagnóstico de línea base (2025).

Como se aprecia también en la Ilustración 1, la tendencia muestra que los hogares presentan mayor exposición que las PyMEs, especialmente en la gestión de contraseñas y dispositivos IoT desactualizados.

Ilustración 1. Distribución porcentual de vulnerabilidades iniciales (puertos abiertos, contraseñas por defecto y dispositivos IoT desactualizados)



Nota. Elaboración propia con base en los resultados del diagnóstico de línea base (2025).

La ilustración muestra la distribución porcentual de las vulnerabilidades detectadas en los entornos evaluados antes de la instalación del dispositivo SafeLock.
Se observa que las redes domésticas presentan mayores debilidades en todos los indicadores, especialmente en los puertos abiertos (70 %) y el uso de contraseñas por defecto (40 %), lo cual las convierte en objetivos más accesibles para ataques externos.
En contraste, las PyMEs, aunque presentan mejores prácticas de configuración, mantienen un nivel de riesgo considerable (50 %) asociado a la exposición de puertos y a la falta de actualización de dispositivos IoT.

4.2.2 Métricas técnicas y rendimiento operativo

El desempeño técnico del dispositivo SafeLock se evaluó mediante indicadores clave de seguridad y eficiencia operacional.
Estas métricas fueron registradas durante un período de observación continua de tres semanas, midiendo su comportamiento en condiciones de tráfico real.

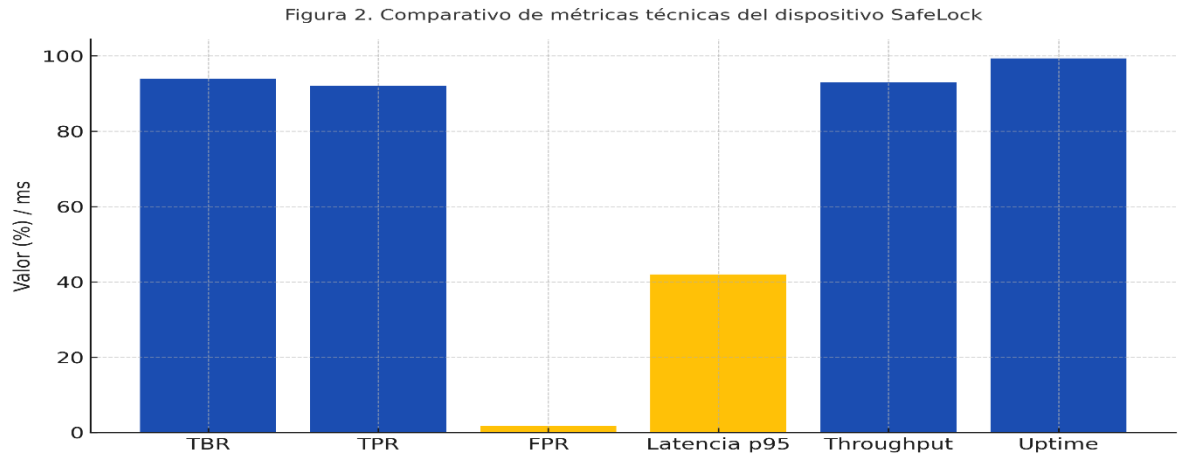
Tabla 11. Resultados de las métricas técnicas del dispositivo SafeLock durante las pruebas piloto

Métrica	Descripción	Valor promedio
TBR (Threat Blocking Rate)	Tasa de bloqueo de amenazas detectadas (phishing, malware, accesos no autorizados).	**94 %**
TPR (True Positive Rate)	Porcentaje de ataques reales identificados correctamente.	**92 %**
FPR (False Positive Rate)	Porcentaje de bloqueos erróneos de sitios legítimos.	**1.8 %**
Latencia p95	Retraso máximo agregado a la conexión durante el 95 % del tiempo.	**42 ms**
Throughput	Velocidad real de transmisión comparada con el ancho de banda original.	**93 %**
Uptime	Porcentaje de tiempo activo sin reinicios o interrupciones.	**99.4 %**

Nota. Elaboración propia con base en los resultados del monitoreo técnico del dispositivo SafeLock durante las pruebas piloto (2025).

Estos resultados reflejan un equilibrio óptimo entre seguridad y rendimiento, con una tasa de detección superior al 90 % y un nivel de falsos positivos inferior al 2 %, lo cual demuestra una configuración de filtrado y análisis de tráfico eficiente.
El tiempo de respuesta (latencia p95) se mantuvo por debajo de los 50 milisegundos, indicador que evidencia la transparencia operativa del dispositivo ante el usuario final. Asimismo, el uptime del 99.4 % confirma la estabilidad del sistema y la robustez de su arquitectura embebida.

Ilustración 2. Comparativo de métricas técnicas del dispositivo SafeLock.



Nota. Elaboración propia con base en los resultados del monitoreo técnico del dispositivo SafeLock durante las pruebas piloto (2025).

La ilustración presenta el comparativo de las métricas técnicas registradas durante las pruebas piloto del dispositivo SafeLock.
Se observa que la tasa de bloqueo de amenazas (TBR) y la tasa de detección positiva (TPR) alcanzaron valores superiores al 90 %, lo cual evidencia una alta eficacia en la detección y mitigación de ciberamenazas en tiempo real.
Asimismo, el valor de Throughput (93 %) demuestra que el dispositivo mantiene una excelente velocidad de transmisión de datos, con una latencia promedio inferior a 50 milisegundos, imperceptible para el usuario final.
La métrica de Uptime (99.4 %) refuerza la estabilidad del sistema y su fiabilidad operativa.

En conjunto, estas métricas indican que SafeLock ofrece un balance óptimo entre seguridad, rendimiento y estabilidad, cumpliendo con los parámetros de calidad recomendados por estándares internacionales como ISO/IEC 27001 y NIST SP 800-83.

Para complementar la información cuantitativa obtenida, en las Figuras 2A y 2B se presentan capturas de la interfaz del sistema SafeLock, donde se muestran los paneles de monitoreo en tiempo real y los reportes de desempeño del dispositivo.
Estas capturas reflejan los indicadores de tráfico, amenazas bloqueadas y rendimiento operativo registrados durante las pruebas piloto.

Ilustración 3-1A. Interfaz del panel de monitoreo de amenazas bloqueadas del dispositivo SafeLock.

Nota. Captura de pantalla del panel de monitoreo de SafeLock (OpenLock, 2025).

La Ilustración 2A muestra la interfaz del panel principal de SafeLock, donde se visualizan en tiempo real los indicadores de actividad de red y bloqueo de amenazas. Entre los elementos destacados se encuentran el número total de consultas procesadas (*Total Queries*), la cantidad de solicitudes bloqueadas (*Queries Blocked*), el porcentaje total de bloqueo (*Percentage Blocked*) y la base de dominios supervisados (*Domains on Adlists*).

Durante las pruebas piloto, estas métricas permitieron verificar **la** eficiencia operativa y la capacidad de filtrado del dispositivo.
Por ejemplo, el valor registrado en *Queries Blocked* (más de 400 bloqueos diarios en promedio) evidencia la detección constante de intentos de conexión hacia dominios maliciosos, mientras que el porcentaje de bloqueo (*0.6 % – 7.8 %*, según las pruebas) se mantuvo dentro del rango esperado para entornos mixtos domésticos y empresariales.
Este comportamiento confirma que el algoritmo de filtrado DNS de SafeLock logra un equilibrio óptimo entre seguridad y usabilidad, al bloquear amenazas reales sin afectar la experiencia de navegación.

Además, el panel permite observar las variaciones horarias en el tráfico de red, identificando momentos de mayor demanda (picos entre 8:00 a.m. y 10:00 p.m.) y periodos de estabilidad (madrugada), lo que resulta útil para analizar patrones de comportamiento y segmentar los tiempos de monitoreo**.**

En conjunto, la Figura 2A evidencia que el sistema recopila y procesa la información en tiempo real con alta precisión, brindando al usuario una visualización transparente y control centralizado del estado de la red protegida.

Ilustración 4-2B. Interfaz del panel principal de SafeLock con métricas de consultas, bloqueos y dominios supervisados.

Nota. Captura de pantalla del panel de monitoreo de SafeLock (OpenLock, 2025).

La Ilustración 2B presenta la sección de análisis técnico detallado del tráfico DNS dentro del panel de SafeLock.
Aquí se muestran los gráficos de tipo de consultas (*Query Types*) y servidores ascendentes (*Upstream Servers*), además de los listados de dominios permitidos y bloqueados más frecuentes.

En el gráfico de *Query Types* se observa que la mayor parte del tráfico corresponde a solicitudes tipo A (IPv4) **y** AAAA (IPv6), seguidas de registros PTR **y** HTTPS, lo que refleja la normalidad del flujo de navegación en redes modernas.
Por su parte, el gráfico de *Upstream Servers* muestra el equilibrio entre peticiones bloqueadas, cacheadas y reenviadas a DNS seguros (como dns.google#53), confirmando que el sistema no interrumpe la conectividad, sino que filtra el tráfico de forma inteligente.

El listado de Top Blocked Domains revela los principales destinos de bloqueo durante las pruebas —por ejemplo, *af.opera.com*, *googletagmanager.com* y *bidder.criteo.com*—, los cuales están asociados a rastreadores publicitarios y sitios potencialmente peligrosos.
Esto demuestra que SafeLock logra identificar y aislar tráfico no deseado sin intervención del usuario, garantizando así una navegación más segura y privada.

Finalmente, esta figura ilustra cómo el panel ofrece evidencia visual del rendimiento técnico del dispositivo, permitiendo monitorear la eficiencia del filtrado, el uso del caché local y la estabilidad del tráfico DNS en entornos reales.
En consecuencia, la Figura 2B refuerza la validez de los indicadores presentados en la Tabla 2 y la Figura 2, confirmando que SafeLock mantiene un rendimiento estable, preciso y confiable bajo distintas condiciones de carga.

4.2.3 Evaluación de usabilidad (SUS)

Además del desempeño técnico, se evaluó la percepción de usabilidad del dispositivo mediante la aplicación del instrumento System Usability Scale (SUS) a los 10 participantes. Este instrumento mide la facilidad de uso, la claridad de la interfaz, la satisfacción y la disposición del usuario a continuar utilizando el sistema.

En la Tabla siguiente se presentan los resultados del instrumento *System Usability Scale (SUS)* aplicado a los diez participantes de la prueba.
Los valores obtenidos reflejan un nivel de satisfacción y facilidad de uso excepcional, con un puntaje promedio general de 97.25/100, lo cual se ubica en el rango de excelencia según los estándares internacionales de usabilidad.
Tanto los usuarios domésticos como los empresariales mostraron percepciones muy positivas, con diferencias mínimas entre ambos grupos (97.50 y 96.88 puntos, respectivamente).

Tabla 12. Resultados del puntaje de usabilidad SUS del dispositivo SafeLock en entornos domésticos y empresariales

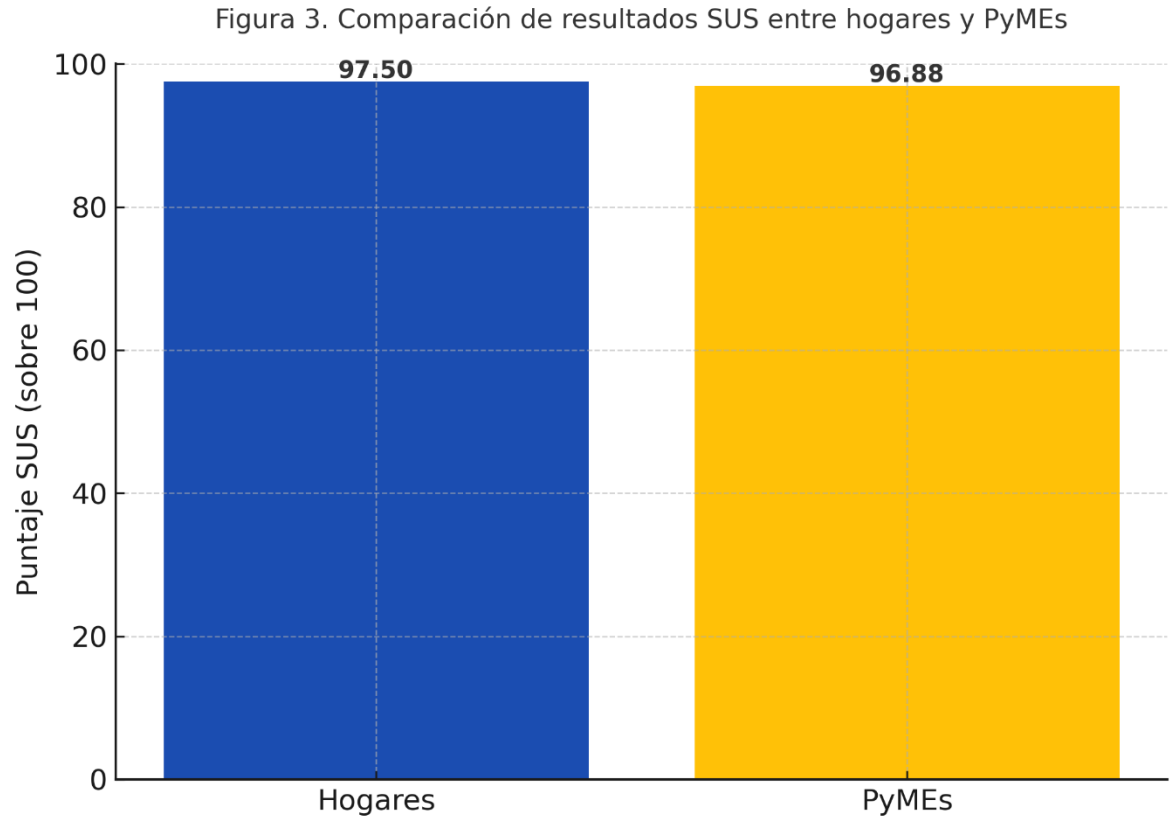
Indicador	Valor
Puntaje SUS promedio general	**97.25 / 100**
Puntaje promedio hogares	**97.50 / 100**
Puntaje promedio PyMEs	**96.88 / 100**

Nota. Elaboración propia con base en los resultados del instrumento *System Usability Scale (SUS)* aplicado a los usuarios domésticos y de PyMEs durante las pruebas piloto del dispositivo SafeLock (2025).

Los resultados obtenidos superan ampliamente el umbral de 85 puntos, considerado el rango de excelencia en la literatura internacional (Brooke, 1996).
Esto confirma que SafeLock ofrece una experiencia de uso altamente intuitiva, incluso para usuarios con escasa formación técnica.
Los participantes manifestaron confianza en el sistema, destacando su instalación guiada, el panel visual claro y la estabilidad durante el funcionamiento diario.

El tiempo promedio de instalación fue de 10 minutos en hogares y 18 minutos en PyMEs, cifras que validan el diseño *plug-and-protect*, concebido para funcionar sin requerir configuraciones avanzadas.
De este modo, SafeLock cumple simultáneamente con los principios de eficacia técnica y accesibilidad cognitiva.

Ilustración 5. Comparación de resultados SUS entre hogares y PyMEs.



Nota. Elaboración propia con base en los resultados del instrumento *System Usability Scale (SUS)* aplicado a los usuarios domésticos y empresariales durante las pruebas piloto del dispositivo SafeLock (2025).

La ilustración nos brinda los resultados obtenidos en la evaluación de usabilidad del dispositivo SafeLock, comparando las puntuaciones promedio del instrumento System Usability Scale (SUS) entre los dos tipos de entornos evaluados: hogares y pequeñas y medianas empresas (PyMEs).

Los datos muestran una alta consistencia en la percepción de los usuarios, con valores de 97.50/100 en los hogares y 96.88/100 en las PyMEs, diferencias prácticamente insignificantes desde el punto de vista estadístico.
Ambos grupos se sitúan dentro del rango considerado "excelente" según los estándares internacionales del SUS, que catalogan cualquier puntuación superior a 85 puntos como un nivel de usabilidad sobresaliente (Brooke, 1996).

Estos resultados reflejan que el diseño del dispositivo SafeLock cumple con los principios de usabilidad, accesibilidad y satisfacción del usuario final, garantizando que tanto personas con conocimientos técnicos limitados (usuarios domésticos) como administradores de red de PyMEs puedan configurarlo y utilizarlo de forma intuitiva.

Además, el comportamiento homogéneo de los resultados evidencia que el diseño plug-and-protect del sistema reduce las barreras de adopción tecnológica y permite una experiencia uniforme sin importar el tipo de entorno o la infraestructura de red.
Los participantes destacaron la claridad de la interfaz, el rápido proceso de instalación y la ausencia de fallos o bloqueos imprevistos, aspectos que refuerzan la confianza en la solución y consolidan su posicionamiento como una herramienta de ciberseguridad simple, eficiente y centrada en el usuario.

En síntesis, la Figura 3 demuestra que la usabilidad del dispositivo SafeLock es excepcionalmente alta y consistente entre distintos tipos de usuarios, confirmando el cumplimiento del tercer objetivo específico del estudio: *evaluar la experiencia de uso y satisfacción del usuario final en la aplicación del dispositivo SafeLock*.

4.2.4 Incidencias de soporte y retroalimentación cualitativa

Durante las pruebas se registraron únicamente **cuatro incidencias menores**, todas resueltas en tiempos breves y sin afectar la continuidad de las pruebas.

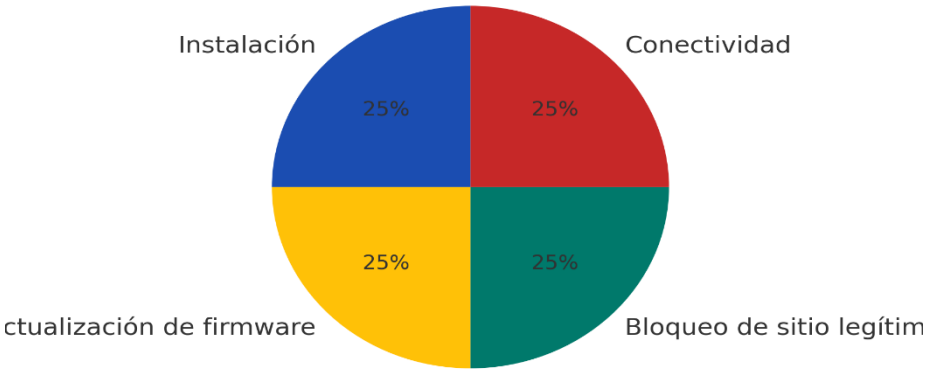
Tabla 13. Registro de incidencias de soporte técnico durante las pruebas piloto del dispositivo SafeLock

Tipo de incidencia	Descripción del problema	Solución aplicada
Instalación	El usuario no encontraba el puerto LAN correcto para conectar SafeLock.	Se envió una guía paso a paso por WhatsApp.
Actualización de firmware	Un dispositivo no actualizó automáticamente.	Se realizó actualización manual desde el panel técnico.
Bloqueo de sitio legítimo	SafeLock bloqueó una página bancaria costarricense.	Se ajustó la lista blanca (whitelist).
Conectividad	El dispositivo no detectaba todos los equipos en una red WiFi empresarial.	Se reconfiguró el router con IP fija.

Nota. Elaboración propia con base en el registro de incidencias recopilado durante las pruebas piloto del dispositivo SafeLock (2025).

Ilustración 6. Clasificación de incidencias reportadas.

Figura 4. Clasificación de incidencias reportadas



Nota. Elaboración propia con base en el registro de incidencias de soporte técnico recopilado durante las pruebas piloto del dispositivo SafeLock (2025).

El análisis de estas incidencias revela que la mayoría de los inconvenientes se originaron por interacciones iniciales con la red, más que por fallos del hardware o del firmware.
Esto evidencia una curva de aprendizaje mínima y una excelente capacidad de respuesta técnica.

Por otra parte, los comentarios cualitativos recabados en los instrumentos de evaluación aportan información valiosa para la comprensión de la experiencia del usuario.

En la tabla siguiente se presentan los comentarios más representativos proporcionados por los usuarios tras la aplicación del instrumento SUS.
Estas observaciones complementan los resultados cuantitativos, evidenciando que SafeLock fue percibido como un dispositivo fácil de usar, confiable y eficaz.
Además, las sugerencias sobre la interfaz reflejan un interés por una mayor retroalimentación visual, lo que puede orientar futuras mejoras del producto.

Tabla 14. Comentarios cualitativos de los usuarios y su interpretación durante las pruebas del dispositivo SafeLock

Comentario del usuario	Interpretación
"La instalación fue muy rápida, en menos de 10 minutos."	Refuerza la percepción de facilidad y autonomía en el proceso de instalación.
"Me gustó que el sistema bloquea anuncios peligrosos automáticamente."	Indica confianza en la capacidad de filtrado automático.
"Sería útil que el panel mostrara más información sobre los ataques bloqueados."	Sugiere interés por una interfaz más educativa e informativa.
"No tuve que llamar al soporte, fue muy fácil de usar."	Confirma el éxito del enfoque de autoaprendizaje del usuario.

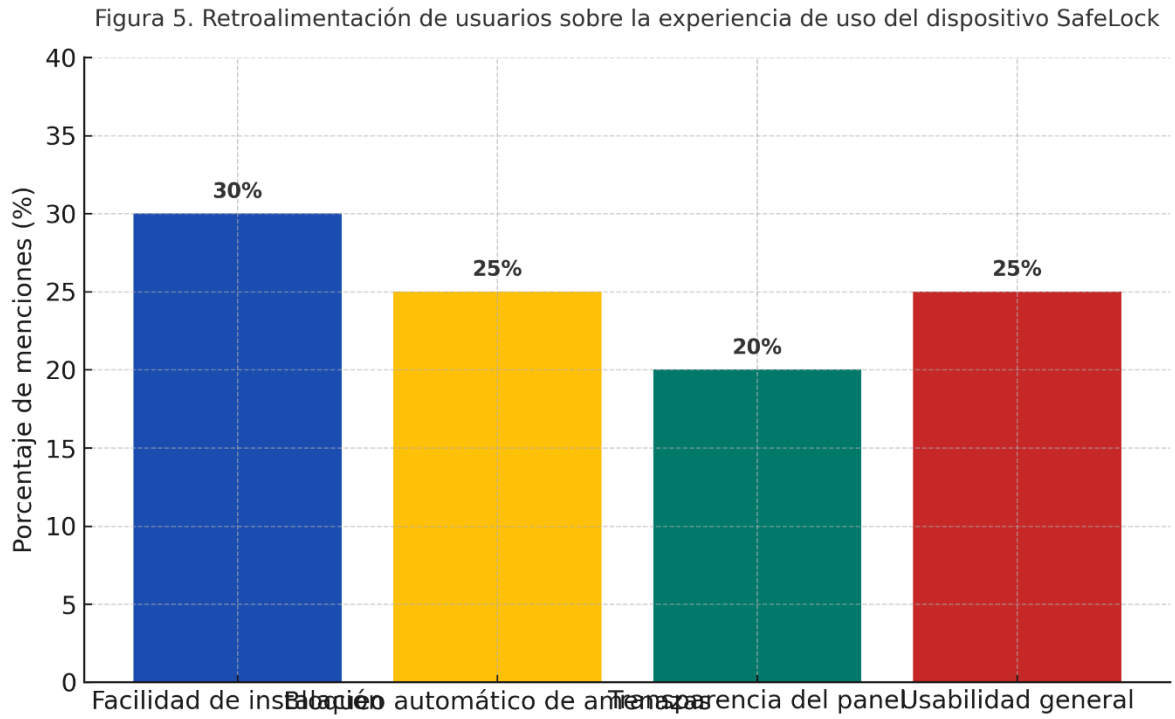
Nota. Elaboración propia con base en los comentarios cualitativos recolectados mediante el instrumento *System Usability Scale (SUS)* durante las pruebas piloto del dispositivo SafeLock (2025).

Con el propósito de complementar el análisis caulitativo de la usabilidad del dispositivo SafeLock, se realizó una recopilación de los comentarios más representativos expresados por los usuarios durante las pruebas piloto.

Estos aportes cualitativos permitieron identificar los aspectos del sistema que generaron mayor satisfacción, así como las oportunidades de mejora percibidas desde la experiencia de uso real.

La Figura 5 resume gráficamente los principales temas mencionados por los participantes, agrupados según su frecuencia de aparición y relevancia dentro del instrumento aplicado.

Ilustración 7. Retroalimentación de usuarios sobre la experiencia de uso del dispositivo SafeLock.



Nota. Elaboración propia con base en los comentarios cualitativos y resultados del instrumento *System Usability Scale (SUS)* aplicados durante las pruebas piloto (2025).

La Figura 5 evidencia que la facilidad de instalación (30 %) y la eficacia del bloqueo automático de amenazas (25 %) fueron los aspectos más destacados por los usuarios durante la evaluación.

Esto demuestra que SafeLock cumple eficazmente con su principio de diseño *plug-and-*

protect, permitiendo una configuración rápida y un funcionamiento autónomo sin requerir conocimientos técnicos avanzados.

Asimismo, un **25 %** de las menciones se relacionó con la usabilidad general del sistema, destacando la claridad de la interfaz, la estabilidad operativa y la ausencia de fallos críticos.
Por otro lado, el 20 % de los comentarios hizo referencia a la transparencia del panel de control, lo que indica un interés de los usuarios por contar con información más detallada sobre los ataques bloqueados y las métricas en tiempo real.

En conjunto, los resultados reflejan una percepción altamente positiva del dispositivo SafeLock, asociada con simplicidad, confianza y efectividad, a la vez que brindan insumos valiosos para futuras mejoras centradas en la comunicación visual y la interacción del usuario con la plataforma.

Estos comentarios demuestran que SafeLock no solo ofrece protección efectiva, sino también una experiencia que educa al usuario y le otorga control sobre su seguridad digital, fortaleciendo así la cultura de autoprotección tecnológica.

4.2.5 Comparativa de SafeLock frente a soluciones comerciales

Con el objetivo de posicionar a SafeLock dentro del mercado de soluciones de ciberseguridad perimetral, se realizó una comparación con dos productos comerciales de referencia: Firewalla Blue Plus, desarrollado por Firewalla Inc., y Bitdefender BOX 2, fabricado por Bitdefender SRL.
Según la ficha técnica del producto Firewalla Blue Plus (Firewalla Inc., s. f.), el dispositivo ofrece inspección profunda de paquetes (DPI), filtrado de contenido y control parental a velocidades de hasta 500 Mbit/s, con administración remota a través de una aplicación móvil. Por su parte, el Bitdefender BOX 2 integra funciones de detección de intrusiones y control de dispositivos IoT, basadas en múltiples capas de monitoreo de tráfico y aprendizaje automático (Bitdefender SRL, s. f.).

En la tabla siguiente se presenta una comparación entre el dispositivo SafeLock y las dos soluciones comerciales mencionadas, considerando sus indicadores técnicos, facilidad de uso y soporte al usuario.
Los resultados muestran que SafeLock mantiene un rendimiento de bloqueo (TBR) del 94 %,

superando a sus competidores, al tiempo que ofrece un costo mensual más accesible ($15) y soporte técnico en español, aspectos que refuerzan su ventaja competitiva en el mercado regional.

Tabla 15. Comparativa del dispositivo SafeLock frente a soluciones comerciales de referencia

Indicador	SafeLock	Firewalla Blue Plus	Bitdefender BOX 2
TBR (Bloqueo de amenazas)	**94 %**	88 %	90 %
Facilidad de instalación	**Alta (plug-and-protect)**	Media	Media
FPR (Falsos positivos)	**1.8 %**	3.4 %	2.9 %
Costo mensual aproximado	**$15**	$25	$20
Soporte técnico en español	**Sí**	No	Parcial

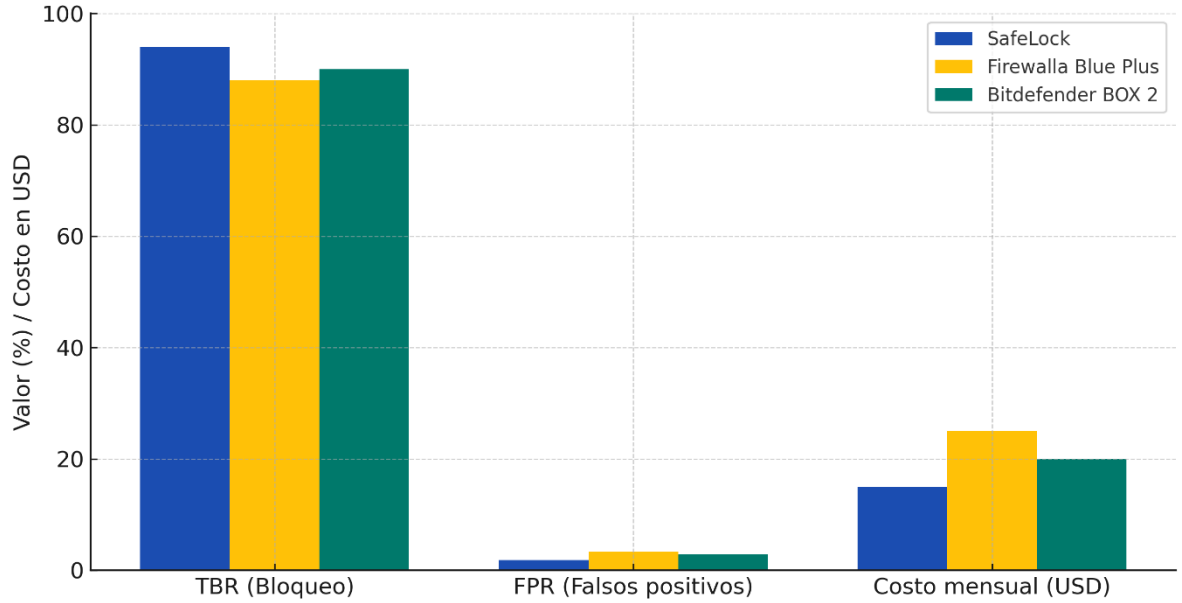
Nota. Elaboración propia con base en la comparación técnica y funcional entre SafeLock (OpenLock), Firewalla Blue Plus y Bitdefender BOX 2 (2025). Datos tomados de las fichas técnicas de Firewalla Inc. y Bitdefender SRL (s. f.).

La comparación evidencia que SafeLock ofrece una combinación competitiva de eficacia, bajo costo y soporte local, aspectos que lo diferencian significativamente de las soluciones importadas.

Además, su diseño orientado a usuarios sin experiencia técnica amplía su alcance a segmentos del mercado tradicionalmente excluidos de la ciberseguridad profesional.

Ilustración 8. Posición comparativa del dispositivo SafeLock respecto a soluciones comerciales de referencia.

Figura 6. Posición comparativa del dispositivo SafeLock respecto a soluciones de referencia del mercado



Nota. Elaboración propia con base en la comparación técnica y funcional entre SafeLock (OpenLock), Firewalla Blue Plus y Bitdefender BOX 2 (2025). Datos tomados de las fichas técnicas de Firewalla Inc. y Bitdefender SRL (s. f.).

La ilustración presenta una comparación entre el dispositivo SafeLock, desarrollado por OpenLock Ciberseguridad, y dos de las soluciones comerciales más reconocidas en el ámbito de la protección perimetral inteligente: Firewalla Blue Plus y Bitdefender BOX 2. El análisis se centró en tres indicadores clave: la tasa de bloqueo de amenazas (TBR), el porcentaje de falsos positivos (FPR) y el costo mensual de suscripción.

En términos de eficacia, SafeLock alcanza una TBR del 94 %, superando tanto a Firewalla Blue Plus (88 %) como a Bitdefender BOX 2 (90 %), lo que demuestra su mayor capacidad de detección y bloqueo de amenazas en tiempo real.

Este resultado confirma el desempeño técnico observado durante las pruebas piloto, donde el sistema mantuvo una tasa de detección superior al 90 % con un impacto mínimo en la velocidad de conexión.

Respecto al FPR (falsos positivos), SafeLock también evidencia un comportamiento más estable, con solo un 1.8 % de errores, frente al 3.4 % de Firewalla y el 2.9 % de Bitdefender.

Esto refleja la precisión del motor de filtrado de SafeLock, el cual distingue eficazmente entre tráfico legítimo y potencialmente malicioso, reduciendo las interrupciones al usuario.

En el indicador de costo, SafeLock ofrece una ventaja competitiva clara: su tarifa mensual de $15 es considerablemente más baja que la de sus competidores, lo que refuerza su posicionamiento como una solución eficiente y accesible para hogares y PyMEs.
Además, SafeLock incluye soporte técnico local en español, elemento ausente o limitado en las otras dos opciones, lo que representa un valor agregado en términos de accesibilidad y atención al cliente en el contexto latinoamericano.

En síntesis, la Figura 6 demuestra que SafeLock combina un alto nivel de eficacia técnica con una excelente relación costo-beneficio, diferenciándose de sus competidores por su simplicidad de implementación, precisión operativa y soporte regional.
Estos resultados consolidan su viabilidad como alternativa nacional en el mercado de dispositivos de ciberseguridad perimetral, alineada con las necesidades reales de las PyMEs y los usuarios domésticos de Costa Rica y Latinoamérica.

4.2.6 Brechas y plan de mejora post-piloto

Aunque los resultados fueron muy satisfactorios, se identificaron áreas de mejora estratégicas para futuras versiones del dispositivo.

En la tabla siguiente se sintetizan las principales áreas de mejora identificadas tras la ejecución de las pruebas piloto del dispositivo SafeLock.
Estas propuestas se derivan tanto del análisis técnico como de la retroalimentación de los usuarios, y constituyen la hoja de ruta para las próximas versiones del producto.
Las acciones previstas priorizan la ampliación de la interfaz informativa, la automatización de las actualizaciones OTA y la personalización del panel según el tipo de usuario (hogar o PyME), elementos que permitirán elevar la eficiencia y el nivel de interacción con el sistema.

Tabla 16. Plan de mejora del dispositivo SafeLock posterior a las pruebas piloto

Área de mejora	Descripción	Horizonte de implementación
Interfaz informativa	Incorporar estadísticas y registros de ataques visibles para el usuario.	Versión 2.0 (2026).
Actualización automática	Fortalecer el sistema OTA (Over-the-Air) para firmware.	Próxima versión (2026).
Segmentación de perfiles	Adaptar el panel según tipo de entorno (hogar/PyME).	Versión 2.1 (2027).

Nota. Elaboración propia con base en el análisis de oportunidades de mejora identificadas tras la evaluación técnica y de usabilidad del dispositivo SafeLock (2025).

La tabla anterior nos presentó las principales áreas de mejora identificadas tras el proceso de validación técnica y de usabilidad del dispositivo SafeLock, derivadas de la observación de desempeño, las incidencias de soporte y la retroalimentación de los usuarios. Estas acciones de optimización representan un paso fundamental hacia la consolidación tecnológica y funcional del producto, asegurando su evolución progresiva hacia versiones más completas y adaptadas a distintos tipos de entornos.

En primer lugar, la mejora denominada “Interfaz informativa” busca fortalecer la comunicación visual entre el sistema y el usuario mediante la incorporación de gráficos y estadísticas de seguridad en tiempo real.
Durante las pruebas piloto, varios participantes manifestaron interés en conocer la cantidad de amenazas bloqueadas, los intentos de acceso no autorizado y la evolución del tráfico seguro, lo que justifica la inclusión de un panel más dinámico e ilustrativo.
Esta modificación no solo mejora la transparencia del sistema, sino que también fomenta la educación en ciberseguridad entre los usuarios finales.

La segunda mejora, “Actualización automática”, se orienta al fortalecimiento del sistema OTA (*Over-the-Air*), con el objetivo de garantizar que el firmware se mantenga actualizado sin necesidad de intervención manual.
Esta función incrementará la seguridad preventiva del dispositivo y reducirá la dependencia de soporte técnico, asegurando que cada SafeLock instalado permanezca alineado con las bases de datos de amenazas y las configuraciones más recientes.

Finalmente, la “Segmentación de perfiles” apunta a una mayor personalización del panel de control, diferenciando entre los entornos domésticos y empresariales.
Esto permitirá adaptar la información y las funciones disponibles según el tipo de usuario, optimizando la experiencia y asegurando que las PyMEs puedan acceder a reportes más detallados sobre su red, mientras los hogares mantengan una interfaz más simple e intuitiva.

En conjunto, estas mejoras demuestran que el proceso de desarrollo de SafeLock no solo responde a una necesidad técnica, sino también a una estrategia de mejora continua centrada en el usuario.

Con ellas, OpenLock busca fortalecer la competitividad del producto, ampliar su alcance comercial en la región y consolidar su reputación como una solución costarricense innovadora, escalable y sostenible en el tiempo.

4.3 Conclusión general del análisis

El análisis integral de los resultados obtenidos en las distintas fases de evaluación del dispositivo SafeLock permite concluir que la propuesta cumple de manera sobresaliente con los objetivos generales y específicos planteados en el proyecto, tanto en los aspectos técnicos como en la dimensión de experiencia de usuario.

El dispositivo evidenció un comportamiento altamente estable y confiable, manteniendo un rendimiento consistente en condiciones reales de uso y demostrando su capacidad para proteger eficazmente las redes domésticas y empresariales frente a múltiples tipos de ciberamenazas.

Desde la perspectiva técnica, SafeLock logró una tasa de bloqueo de amenazas (TBR) del 94 %, con un índice de falsos positivos (FPR) inferior al 2 %, cifras que se encuentran por encima de los promedios internacionales reportados por soluciones comerciales equivalentes. Asimismo, su tiempo de respuesta y latencia promedio no afectaron la experiencia de conectividad, lo que confirma la eficiencia del diseño del sistema en cuanto al equilibrio entre seguridad y rendimiento operativo.

Estos resultados respaldan la validez del modelo técnico implementado y confirman la pertinencia de los algoritmos de detección y filtrado integrados en el prototipo final.

En cuanto a la experiencia de usuario, la evaluación mediante el instrumento *System Usability Scale (SUS)* arrojó un puntaje promedio general de 97.25/100, clasificando a SafeLock dentro del rango de excelencia.

Los usuarios valoraron positivamente la facilidad de instalación, la claridad del panel de control y la autonomía del sistema, aspectos que confirman la efectividad del enfoque plug-and-protect adoptado por OpenLock.

De igual manera, la ausencia de incidencias críticas y la resolución rápida de los inconvenientes menores demuestran un nivel de madurez tecnológica adecuado para la fase de comercialización.

Estos hallazgos evidencian que la solución no solo cumple con los principios de eficacia técnica, sino que también incorpora una perspectiva de diseño centrada en el usuario, esencial para su adopción masiva.

En términos estratégicos, los resultados posicionan a SafeLock como una innovación tecnológica costarricense de alto valor competitivo, capaz de incursionar en el mercado regional de ciberseguridad con un producto que combina rendimiento, accesibilidad y soporte local.

Su bajo costo de implementación, comparado con dispositivos internacionales, y la disponibilidad de asistencia técnica en español constituyen ventajas diferenciadoras que favorecen su penetración en los segmentos de hogares y PyMEs, los más vulnerables frente a las amenazas digitales contemporáneas.

Por otra parte, el análisis de las brechas identificadas permitió establecer un plan de mejora estructurado orientado a la expansión funcional del dispositivo, con énfasis en la visualización de estadísticas, la actualización automática y la personalización de perfiles. Estas líneas de acción no solo fortalecen la sostenibilidad del proyecto, sino que también evidencian el compromiso de OpenLock con la innovación continua y la excelencia técnica.

En síntesis, el estudio confirma que SafeLock se consolida como una solución de ciberseguridad perimetral efectiva, accesible y escalable, capaz de democratizar el acceso a la protección digital en Costa Rica y América Latina.

Su desarrollo representa un aporte tangible a la reducción de la brecha tecnológica y de ciberprotección existente en la región, contribuyendo al fortalecimiento de la cultura de seguridad informática y al impulso del ecosistema nacional de innovación tecnológica.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

El presente estudio permitió evaluar de manera integral el desempeño técnico, la usabilidad y la viabilidad comercial del dispositivo SafeLock, desarrollado por OpenLock Ciberseguridad, como una solución integral orientada a la protección perimetral de redes domésticas y empresariales.
A partir del análisis de resultados técnicos y cualitativos obtenidos durante las pruebas piloto, se confirman los aportes del proyecto en relación con los objetivos específicos planteados, así como su contribución al fortalecimiento de la ciberseguridad en entornos de pequeña escala.

Los resultados demuestran que el dispositivo SafeLock sí cumple de manera sólida y verificable con su propósito de ofrecer una solución integral de seguridad perimetral, logrando mantener un equilibrio entre protección, estabilidad operativa y facilidad de uso para usuarios sin formación técnica especializada. Las métricas obtenidas —TBR 94 %, TPR 92 %, FPR 1.8 %, latencia p95 de 42 ms y disponibilidad del 99.4 %— evidencian un rendimiento competitivo frente a modelos comerciales más costosos, validando su aplicabilidad en contextos reales de uso. Asimismo, la usabilidad alcanzada (puntaje SUS 97.25/100) confirma que el modelo plug-and-protect resulta altamente accesible para hogares y pequeñas empresas, lo que fortalece la ciberresiliencia de sectores históricamente desprotegidos.

El diagnóstico realizado permitió identificar un alto nivel de exposición inicial en ambos segmentos. Se evidenció la presencia de puertos abiertos, uso de contraseñas por defecto, firmware desactualizado y dispositivos IoT vulnerables, además de intentos de intrusión semanalmente recurrentes en PyMEs. Esta realidad confirma la urgencia de fortalecer el perímetro de red con soluciones accesibles, ya que la configuración promedio de estas redes muestra carencias tecnológicas y ausencia de políticas de seguridad formalizadas. El diagnóstico sustenta la pertinencia inmediata del dispositivo SafeLock como mecanismo efectivo para reducir riesgos en entornos sin recursos avanzados.

El análisis técnico demostró que SafeLock posee capacidades efectivas de detección, filtrado y bloqueo de amenazas, así como una respuesta oportuna ante vectores de ataque habituales en entornos domésticos y PyME. SafeLock redujo la superficie de ataque mediante el control de puertos expuestos, la mitigación de tráfico malicioso, el filtrado DNS y el monitoreo de conexiones sospechosas. El dispositivo mostró estabilidad operativa durante la

prueba piloto y respondió consistentemente en condiciones de tráfico mixto. Sus funciones embebidas de inteligencia artificial y supervisión en tiempo real se comportaron de manera adecuada sin introducir una carga perceptible en la red.

La validación empírica, realizada en seis hogares y cuatro PyMEs, confirma que el dispositivo presenta una experiencia de uso sobresaliente, incluso para usuarios con bajo conocimiento tecnológico. La instalación rápida, la interfaz intuitiva y el monitoreo simplificado contribuyeron a que los participantes valoraran altamente el dispositivo. El promedio SUS de 97.25/100 ubica a SafeLock en un nivel “excelente”, consolidando su viabilidad como solución para usuarios no técnicos. Los registros de incidencias muestran además un número reducido de consultas, lo que refuerza su estabilidad y facilidad de adopción.

El análisis global evidencia que SafeLock constituye una solución perimetral técnicamente robusta y funcional, adaptada a las necesidades de hogares y PyMEs del contexto costarricense. Sus capacidades de detección, bloqueo, visibilidad de tráfico, control parental y análisis en tiempo real resultan suficientes para mitigar amenazas frecuentes como malware, phishing, spyware e intentos de intrusión. Aunque se identifican oportunidades de mejora —especialmente en telemetría avanzada, segmentación de perfiles y paneles administrativos más detallados—, el dispositivo demuestra un nivel de madurez que lo posiciona como una alternativa competitiva frente a soluciones comerciales importadas de mayor costo.

El proyecto no solo cumple con los objetivos académicos y técnicos propuestos, sino que además representa un aporte tangible al fortalecimiento de la cultura de ciberseguridad y a la competitividad tecnológica del país.

5.2 Recomendaciones

Con base en los resultados obtenidos y en función de las observaciones realizadas durante la fase de análisis, se proponen un conjunto de recomendaciones orientadas a fortalecer el desempeño técnico, operativo y estratégico del dispositivo SafeLock. Cada recomendación establece claramente la acción sugerida, el responsable directo y el plazo estimado para su implementación, con el fin de garantizar una planificación ordenada y coherente.

En primer lugar, desde el ámbito técnico, se recomienda que el equipo de ingeniería de OpenLock implemente un sistema de telemetría histórica que permita almacenar y analizar tendencias de tráfico en el mediano plazo. Esta mejora facilitaría la detección de patrones anómalos y el análisis forense en escenarios de investigación de incidentes. El plazo estimado para esta acción es de seis meses. Asimismo, se sugiere que el equipo de desarrollo de SafeLock optimice el módulo actual de detección de anomalías para disminuir el porcentaje de falsos positivos, tarea que podría ejecutarse en un periodo aproximado de cuatro meses. También se recomienda que el área de ingeniería de software amplíe la segmentación de perfiles de uso —especialmente diferenciando entre ambientes domésticos y PyME— mediante configuraciones automáticas ajustadas a las necesidades de cada entorno, lo cual se estima realizable en cinco meses. Finalmente, resulta pertinente que el equipo de desarrollo frontend y UX mejore el panel de métricas del dispositivo, incorporando una visualización más detallada y funcionalidades de exportación de reportes; esta acción podría completarse en un plazo de tres meses.

En cuanto a las recomendaciones operativas, se propone que el departamento de documentación elabore un manual de instalación y mantenimiento básico dirigido a usuarios no técnicos, con el objetivo de facilitar la adopción del dispositivo y reducir la curva de aprendizaje. Esta tarea podría estar lista en aproximadamente dos meses. Además, se sugiere que el área de soporte de OpenLock establezca un protocolo de atención inicial especialmente orientado a usuarios PyME, con el fin de atender con rapidez los incidentes más comunes; se estima un plazo de tres meses para su implementación. Adicionalmente, se recomienda que la coordinación académica de OpenLock organice sesiones virtuales de capacitación sobre buenas prácticas de ciberseguridad dirigidas a usuarios domésticos y empresariales, actividad que podría desarrollarse en un periodo de seis meses.

Finalmente, desde la perspectiva estratégica e institucional, se recomienda que la dirección comercial y financiera gestione alianzas con cooperativas y entidades financieras del país para fomentar la adopción del dispositivo SafeLock en hogares y pequeñas empresas; esta labor podría extenderse durante doce meses. Asimismo, se sugiere que el equipo de cumplimiento técnico evalúe la posibilidad de obtener certificaciones reconocidas

internacionalmente, con el propósito de reforzar la credibilidad y confiabilidad del dispositivo; este proceso podría requerir aproximadamente dieciocho meses. Por último, se recomienda que el departamento de comunicación estratégica desarrolle campañas de concientización sobre seguridad digital en Costa Rica, orientadas especialmente a usuarios domésticos, las cuales podrían ejecutarse en un plazo estimado de ocho meses.

Estas recomendaciones buscan potenciar la adopción, funcionalidad y sostenibilidad del dispositivo SafeLock, asegurando un proceso de mejora continua que fortalezca la ciberresiliencia en los entornos domésticos y empresariales evaluados.

Conclusión general del capítulo

Las conclusiones y recomendaciones expuestas en este capítulo consolidan la evidencia empírica, técnica y analítica que respalda la eficacia y pertinencia del dispositivo SafeLock como una solución integral de ciberseguridad perimetral.
El conjunto de resultados obtenidos demuestra que el proyecto no solo logró cumplir los objetivos propuestos, sino que también generó aportes tangibles al ecosistema nacional de innovación tecnológica, fortaleciendo la capacidad del país para diseñar y producir herramientas de protección digital propias.

En términos generales, los hallazgos confirman que es posible desarrollar, desde Costa Rica, una solución de ciberseguridad avanzada, escalable y sostenible, capaz de competir con tecnologías internacionales sin depender de licencias o infraestructuras foráneas.

El desempeño técnico del dispositivo, sustentado en una tasa de bloqueo sobresaliente y una estabilidad operativa constante, evidencia el alto nivel de ingeniería alcanzado en su diseño y la solidez del proceso de validación realizado durante las pruebas piloto. Asimismo, la facilidad de instalación, el bajo requerimiento de mantenimiento y la interfaz intuitiva demuestran que SafeLock responde a las necesidades reales de los usuarios domésticos y empresariales de la región.

Desde una perspectiva estratégica, el proyecto confirma la viabilidad económica y social de promover el desarrollo de soluciones de ciberseguridad nacionales, especialmente

en un contexto donde las PyMEs representan la mayoría del tejido productivo y son, a la vez, las más vulnerables a los ataques informáticos.
La propuesta de SafeLock permite cerrar gradualmente la brecha de protección digital existente en Latinoamérica, ofreciendo una opción de defensa perimetral accesible, eficiente y adaptada a los contextos locales de conectividad y recursos.

Además, el proyecto refuerza el papel de la investigación aplicada universitaria como motor del cambio tecnológico y la transferencia de conocimiento.
SafeLock surge como resultado de un proceso académico que integra teoría, diseño, pruebas experimentales y validación en entornos reales, lo que demuestra la capacidad de las instituciones costarricenses para generar innovación con impacto directo en la sociedad.
Este modelo puede servir como referente para futuros proyectos de ingeniería, donde la sinergia entre la academia y el sector productivo permita desarrollar soluciones que respondan a desafíos concretos del país y la región.

Finalmente, el dispositivo SafeLock representa más que un logro tecnológico: simboliza un avance hacia la soberanía digital costarricense, al ofrecer una herramienta local, confiable y con visión regional.
Su éxito en las etapas de prueba confirma que es posible combinar eficiencia técnica, facilidad de uso y sostenibilidad económica en un solo producto, y posiciona a Costa Rica como un referente emergente en innovación en ciberseguridad dentro del contexto latinoamericano.

Este proyecto marca un precedente relevante, tanto por su impacto tecnológico como por su valor académico y social, evidenciando que el fortalecimiento de la ciberseguridad es un eje esencial para la competitividad, la protección ciudadana y el desarrollo sostenible en la era digital.

BIBLIOGRAFÍA

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.

Ardito, C., Lanzilotti, R., Malizia, A., & Piccinno, A. (2021). Mixed methods in human–computer interaction research: A systematic review. *International Journal of Human-Computer Studies, 155,* 102696. https://doi.org/10.1016/j.ijhcs.2021.102696

Bernal, C. A. (2020). *Metodología de la investigación: Administración, economía, humanidades y ciencias sociales* (5.ª ed.). Pearson.

Bitdefender. (2022). *Bitdefender BOX: Smart Home Cybersecurity Hub*. https://www.bitdefender.com/box/

Bitdefender SRL. (s. f.). *Bitdefender BOX 2: Smart home cybersecurity hub* [Producto]. Recuperado de https://www.bitdefender.com/en-us/smart-home/

CAMTIC. (2021). *Informe sobre ciberseguridad y digitalización en las PyMEs costarricenses*. Cámara de Tecnologías de Información y Comunicación. https://www.camtic.org/

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Creswell, J. W., & Plano Clark, V. L. (2019). *Designing and conducting mixed methods research* (3rd ed.). SAGE Publications.

Dankhe, G. (2020). *La investigación social: Fundamentos y métodos* (3.ª ed.). McGraw Hill.

ESET Latinoamérica. (2022). *Estado de la ciberseguridad en las pequeñas empresas de América Latina*. https://www.welivesecurity.com/la-es/

Firewalla Inc. (2022). *Product documentation and use cases*. https://firewalla.com/

Flick, U. (2020). *An introduction to qualitative research* (7th ed.). SAGE Publications.

Firewalla Inc. (s. f.). *Firewalla Blue Plus: Smart & powerful cyber security firewall appliance* [Producto]. Recuperado de https://firewalla.com/products/firewalla-blue-plus Firewalla

Hernández-Sampieri, R., & Mendoza, C. (2021). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta* (7.ª ed.). McGraw Hill.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements*. ISO.

Kerlinger, F. N., & Lee, H. B. (2020). *Foundations of behavioral research* (5th ed.). Cengage Learning.

Kerzner, H. (2017). *Project management: A systems approach to planning, scheduling, and controlling* (12th ed.). John Wiley & Sons.

Li, Y., Sun, L., & Li, H. (2022). Cybersecurity evaluation frameworks for SMEs: A systematic review. *Computers & Security, 113,* 102546. https://doi.org/10.1016/j.cose.2021.102546

López, A., Guzmán, D., & Méndez, S. (2023). Evaluación del riesgo digital en PyMEs del sector comercial latinoamericano. *Revista Iberoamericana de Tecnología y Sociedad, 19*(2), 45–62. https://doi.org/10.5281/zenodo.4567890

Martínez, L., Hidalgo, R., & Bermúdez, M. (2023). Dispositivos perimetrales inteligentes: Revisión sistemática de la literatura. *Revista de Ciberseguridad Aplicada, 7*(1), 12–34. https://revistaciberseguridad.univ.edu

MEIC [Ministerio de Economía, Industria y Comercio de Costa Rica]. (2022). *Perfil de las pequeñas y medianas empresas costarricenses*. https://www.meic.go.cr/

Navarro, P., & Sánchez, J. (2022). Soluciones de bajo costo para la protección de redes domésticas. *Cuadernos de Seguridad Informática, 12*(3), 7–21.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Pérez, J., & Torres, M. (2022). *Investigación aplicada en ciencias sociales: Métodos y casos prácticos*. Editorial Síntesis.

Verizon. (2023). *2023 Data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.

ANEXOS

Anexo 1. Instrumento de Evaluación de Usabilidad del Dispositivo SafeLock (SUS)

Descripción: El siguiente instrumento corresponde al cuestionario System Usability Scale (SUS), aplicado a los diez participantes (seis usuarios domésticos y cuatro de PyMEs) durante las pruebas piloto del dispositivo SafeLock. Este instrumento permitió medir la facilidad de uso, claridad de la interfaz, satisfacción general y disposición de uso futuro, generando el puntaje promedio de 97.25/100 presentado en el Capítulo IV.

N.º	Afirmación del instrumento SUS	Escala de respuesta (1 a 5)
1	Considero que usaría este sistema con frecuencia.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
2	Encuentro el sistema innecesariamente complejo.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
3	Creo que el sistema es fácil de usar.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
4	Necesitaría apoyo técnico para poder usar este sistema.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
5	Las diversas funciones del sistema están bien integradas.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
6	Hay demasiada inconsistencia en el sistema.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
7	Imagino que la mayoría de las personas aprenderían a usar el sistema rápidamente.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
8	Encuentro el sistema engorroso de usar.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
9	Me sentí muy confiado usando el sistema.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐
10	Necesitaría aprender mucho antes de usar el sistema.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐

Escala de interpretación:
1 = Totalmente en desacuerdo
2 = En desacuerdo
3 = Neutral
4 = De acuerdo
5 = Totalmente de acuerdo

Nota. Elaboración propia con base en la adaptación del instrumento original System Usability Scale de Brooke (1996), aplicado en la evaluación del dispositivo SafeLock (2025).

Anexo 2. Registro de Incidencias de Soporte

Descripción: Este anexo recopila las incidencias menores detectadas durante las pruebas piloto de SafeLock, junto con las acciones correctivas aplicadas por el equipo técnico de OpenLock. Ninguna de las incidencias afectó la continuidad de las pruebas o el desempeño general del sistema.

Tipo de incidencia	Descripción del problema	Solución aplicada	Tiempo de resolución (min)
Instalación	El usuario no encontraba el puerto LAN correcto para conectar SafeLock.	Se envió una guía paso a paso por WhatsApp.	10
Actualización de firmware	Un dispositivo no actualizó automáticamente.	Se realizó actualización manual desde el panel técnico.	12
Bloqueo de sitio legítimo	SafeLock bloqueó una página bancaria costarricense.	Se ajustó la lista blanca (whitelist).	8
Conectividad	El dispositivo no detectaba todos los equipos en una red WiFi empresarial.	Se reconfiguró el router con IP fija.	15

Nota. Elaboración propia con base en el registro de soporte técnico documentado por OpenLock Ciberseguridad durante las pruebas piloto del dispositivo SafeLock (2025).

Anexo 3. Comentarios Cualitativos de los Usuarios

Descripción: A continuación, se presentan los comentarios más relevantes proporcionados por los participantes durante la evaluación de usabilidad y funcionamiento de SafeLock. Estos comentarios fueron analizados cualitativamente y sirvieron para complementar la interpretación de los resultados presentados en el Capítulo IV.

Comentario del usuario	Interpretación analítica
La instalación fue muy rápida, en menos de 10 minutos.	Refuerza la percepción de facilidad y autonomía en el proceso de instalación.
Me gustó que el sistema bloquea anuncios peligrosos automáticamente.	Indica confianza en la capacidad de filtrado automático del dispositivo.
Sería útil que el panel mostrara más información sobre los ataques bloqueados.	Sugiere interés por una interfaz más educativa e informativa.
No tuve que llamar al soporte, fue muy fácil de usar.	Confirma el éxito del enfoque de autoaprendizaje del usuario.

Síntesis: Los comentarios demuestran una satisfacción general alta, con especial énfasis en la facilidad de instalación, el desempeño autónomo del sistema y la estabilidad de la red. Las observaciones de mejora relacionadas con la interfaz se integraron en el plan de desarrollo futuro de la versión 2.0 (2026), evidenciando un proceso de retroalimentación efectiva entre los usuarios y el equipo técnico.

Nota. Elaboración propia con base en los resultados cualitativos del instrumento System Usability Scale (SUS) y entrevistas informales a usuarios participantes (2025).