PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

PUCE TEC

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO SUPERIOR EN DESARROLLO DE SOFTWARE

"DESARROLLO DE UN ASISTENTE WEB CON INTELIGENCIA ARTIFICIAL PARA LA GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD EN TALLERES LUIS MERA"

AUTOR: "GALLEGOS MERA RYAN ALEJANDRO"

TUTOR: "NARVAEZ ERAZO LUIS DAVID"

IBARRA – ECUADOR

MARZO DE 2026

Ibarra, 07 de marzo del 2026

CERTIFICACIÓN DE TUTOR

En mi calidad de Tutor del Trabajo de Tecnólogo Superior titulado: Desarrollo de un asistente web con inteligencia artificial para la gestión de incidentes de ciberseguridad en talleres Luis Mera, presentado por el estudiante Gallegos Mera Ryan Alejandro con cédula de ciudadanía No. 1003765318, para la obtención del título de Tecnólogo Superior en Desarrollo de Software.

Certifico que el trabajo cumple con todos los parámetros establecidos, a través del cual el estudiante demuestra el desarrollo de habilidades en el campo de conocimiento de su profesión con un nivel coherente de argumentación, para ser sometido a la evaluación por parte de los lectores.

Además, se adjunta el certificado de porcentaje de originalidad de TURNITIN.

Turnitin Originality Report

Processed on: 10-Mar-2026 12:35 -05
ID: 2899672285
Word Count: 15154
Submitted: 1

Desarrollo de un asistente web con inteligencia artificial para la gestión de incidentes de ciberseguridad en pequeñas empresas, caso de aplicación en Talleres Luis Mera. By RYAN ALEJANDRO GALLEGOS MERA

Similarity Index	Similarity by Source	
2%	Internet Sources:	2%
	Publications:	0%
	Student Papers:	0%

1% match (Internet from 08-Apr-2025)
https://repositorio.puce.edu.ec/server/api/core/bitstreams/95c309a9-ed2e-4734-a5ad-9bd3acbfccf1/content

1% match (Internet from 18-Feb-2026)
https://repositorio.puce.edu.ec/server/api/core/bitstreams/c616a4c3-d24b-4208-a5a8-b2584523554b/content

1% match (Internet from 01-Apr-2025)
https://repositorio.puce.edu.ec/server/api/core/bitstreams/66dbe117-0533-49d6-beed-01f8ea2b407e/content

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR PUCE TEC TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO SUPERIOR EN DESARROLLO DE SOFTWARE "DESARROLLO DE UN ASISTENTE WEB CON INTELIGENCIA ARTIFICIAL PARA LA GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD EN TALLERES LUIS MERA" AUTOR: "GALLEGOS MERA RYAN ALEJANDRO" TUTOR: "NARVAEZ ERAZO LUIS DAVID" IBARRA – ECUADOR MARZO DE 2026 Ibarra, 07 de marzo del 2026 CERTIFICACIÓN DE TUTOR En mi calidad de Tutor del Trabajo de Tecnólogo Superior titulado: Desarrollo de un asistente web con inteligencia artificial para la gestión de incidentes de ciberseguridad en talleres Luis Mera, presentado por el estudiante Gallegos Mera Ryan Alejandro con cédula de ciudadanía No. 1003765318, para la obtención del título de Tecnólogo Superior en Desarrollo de Software. Certifico que el trabajo cumple con todos los parámetros establecidos, a través del cual el estudiante demuestra el desarrollo de habilidades en el campo de conocimiento de su profesión con un nivel coherente de argumentación, para ser sometido a la evaluación por parte de los lectores. Además, se adjunta el certificado de porcentaje de originalidad de TURNITIN. (f): Mgs. NARVAEZ ERAZO LUIS DAVID TUTOR DE TRABAJO CC: 1002868378 ii PÁGINA DE APROBACIÓN DEL TRIBUNAL El tribunal examinador aprueba este trabajo en nombre de la Pontificia Universidad Católica del Ecuador Ibarra: (f): ..... MGS. NARVAEZ ERAZO LUIS DAVID CC: 1002868378 (f):... ..... MGS. PILLO GUANOLUISA DARWIN MARCELO CC: 1003319660 iii ACTA DE CESIÓN DE DERECHOS Yo. GALLEGOS MERA

LUIS DAVID NARVAEZ ERAZO

Firmado digitalmente porLUIS DAVID NARVAEZ ERAZO
DN: cn=LUIS DAVID NARVAEZ ERAZO gn=LUIS DAVID c=EC
Motivo:Soy el autor de este documento
Ubicación:
Fecha:2026-03-10 14:24-05:00

(f):_ _____
Mgs. NARVAEZ ERAZO LUIS DAVID
TUTOR DE TRABAJO
CC: 1002868378

PÁGINA DE APROBACIÓN DEL TRIBUNAL

El tribunal examinador aprueba este trabajo en nombre de la Pontificia Universidad Católica del Ecuador Ibarra:

LUIS DAVID NARVAEZ ERAZO

Firmado digitalmente porLUIS DAVID NARVAEZ ERAZO
DN: cn=LUIS DAVID NARVAEZ ERAZO gn=LUIS DAVID c=EC
Motivo:Soy el autor de este documento
Ubicación:
Fecha:2026-03-10 14:24-05:00

(f): ……

MGS. NARVAEZ ERAZO LUIS DAVID

CC: 1002868378

Darwin Pillo G.

Firmado digitalmente porDarwin Pillo G.
DN: cn=Darwin Pillo G. gn=Darwin Pillo G. c=EC Ecuador l=EC Ecuador o=Escuela de Arquitectura, Ingeniería, Diseño y Artes ou=PUCE Ibarra e=dmpillo@pucesi.edu.ec
Motivo:Apruebo este documento
Ubicación:Ibarra - Ecuador
Fecha:2026-03-10 19:41-05:00

(f):… ……

MGS. PILLO GUANOLUISA DARWIN MARCELO

CC: 1003319660

ACTA DE CESIÓN DE DERECHOS

Yo, *GALLEGOS MERA RYAN ALEJANDRO,* declaro conocer y aceptar la disposición del Artículo 165 del Código Orgánico de la Economía Social del Conocimiento, la Creatividad y la Innovación, que establece textualmente: "Se reconoce a los autores y demás titulares de derechos la facultad de disponer de sus derechos o autorizar el uso de sus obras o servicios de forma gratuita o a cambio de una tarifa, según las condiciones que determinen. Esta facultad podrá ejercerse mediante licencias abiertas y gratuitas y otros modelos alternativos de licencia, o mediante la renuncia a sus derechos".

Ibarra, 07 de marzo del 2026

(f): _____ _____

GALLEGOS MERA RYAN ALEJANDRO

CC: 1003765318

AUTORIA

Yo, *Ryan Alejandro Gallegos Mera,* titular de la cédula de ciudadanía No. 1003765318, declaro que el presente trabajo de investigación es de exclusiva responsabilidad del autor, y eximo expresamente a la Pontificia Universidad Católica del Ecuador Ibarra de posibles reclamos o acciones legales.

(f):

GALLEGOS MERA RYAN ALEJANDRO

CC: 1003765318

DEDICATORIA Y AGRADECIMIENTOS

Dedico este trabajo a mi familia, cuyo apoyo incondicional me ha permitido alcanzar esta meta académica. A mis padres, por su esfuerzo constante y su fe inquebrantable en mis capacidades. A Talleres Luis Mera, por abrirme las puertas de su empresa y confiar en esta propuesta tecnológica que marca el inicio de una nueva era en la gestión de su seguridad digital.

Agradezco profundamente a mi asesor, Luis David Narváez Erazo, cuya experta guía y paciencia fueron fundamentales para estructurar este proyecto de investigación. También agradezco a los profesores de la carrera de Desarrollo de Software de la PUCE Ibarra por compartir sus conocimientos en programación, bases de datos, metodologías ágiles y desarrollo de software, lo que hizo posible el desarrollo de este sistema.

Agradezco especialmente al personal de Talleres Luis Mera por su activa colaboración durante la fase de implementación y validación del asistente web. Sus comentarios sinceros sobre la usabilidad y funcionalidad del sistema fueron esenciales para lograr una solución verdaderamente útil para las microempresas ecuatorianas.

Finalmente, agradezco a la Pontificia Universidad Católica del Ecuador Ibarra por brindarme una formación integral que combina la excelencia técnica con el compromiso social, preparándome para contribuir a la transformación digital de nuestro país.

TABLA DE CONTENIDO

LISTA DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Las microempresas ecuatorianas gestionan incidentes de ciberseguridad de forma manual y reactiva, sin acceso a especialistas en tecnología, exponiéndolas a amenazas como phishing, malware y acceso no autorizado. Este proyecto desarrolló e implementó un asistente web basado en inteligencia artificial para gestión automatizada de incidentes de ciberseguridad en Talleres Luis Mera, microempresa del sector automotriz en Ibarra, Ecuador. El sistema integra un clasificador heurístico con 8 reglas de detección y 4 servicios externos de análisis (VirusTotal, MetaDefender, Google Safe Browsing, Google Gemini 2.5 Flash) que trabajan en conjunto para generar análisis profesionales explicados en lenguaje no técnico mediante inteligencia artificial generativa. Se empleó metodología eXtreme Programming (XP) durante 8 semanas con desarrollo iterativo, validación continua y participación directa de usuarios reales. La validación operativa con 5 usuarios durante 8 semanas procesó 105 incidentes reales con 100% de adopción de usuarios, tiempo promedio de análisis de 7.9 segundos, y operación a costo cero eliminando la barrera económica tradicional. El clasificador fue validado con dataset de 100 casos alcanzando precisión global de 86.9%, demostrando que soluciones de ciberseguridad basadas en inteligencia artificial explicable, tecnologías open source y servicios cloud gratuitos son técnica y económicamente viables para microempresas ecuatorianas con recursos limitados.

Palabras clave: ciberseguridad, inteligencia artificial explicable, clasificador heurístico, gestión de incidentes, microempresas ecuatorianas

ABSTRACT

Ecuadorian microbusinesses manage cybersecurity incidents manually and reactively, without access to technology specialists, exposing them to threats such as phishing, malware, and unauthorized access. This project developed and implemented a web assistant based on artificial intelligence for automated management of cybersecurity incidents in Talleres Luis Mera, a microenterprise in the automotive sector in Ibarra, Ecuador. The system integrates a heuristic classifier with 8 detection rules and 4 external analysis services (VirusTotal, MetaDefender, Google Safe Browsing, Google Gemini 2.5 Flash) that work together to generate professional analyzes explained in non-technical language using generative artificial intelligence. eXtreme Programming (XP) methodology was used for 8 weeks with iterative development, continuous validation and direct participation of real users. The operational validation with 5 users for 8 weeks processed 105 real incidents with 100% user adoption, average analysis time of 7.9 seconds, and operation at zero cost, eliminating the traditional economic barrier. The classifier was validated with a dataset of 100 cases, reaching an overall accuracy of 86.9%, demonstrating that cybersecurity solutions based on explainable artificial intelligence, open source technologies and free cloud services are technically and economically viable for Ecuadorian microenterprises with limited resources.

Keywords: cybersecurity, explainable artificial intelligence, heuristic classifier, incident management, Ecuadorian microenterprises

INTRODUCCIÓN

Las microempresas ecuatorianas enfrentan crecientes ciberamenazas (phishing, ransomware, robo de credenciales) que comprometen operaciones e información confidencial de clientes. La gestión eficiente de incidentes de ciberseguridad representa un desafío crítico para organizaciones sin recursos TI ni personal especializado.

Este proyecto desarrolla un asistente web basado en inteligencia artificial para gestión automatizada de incidentes de ciberseguridad en Talleres Luis Mera, microempresa del sector automotriz en Ibarra, Ecuador. El sistema permite a personal administrativo sin formación técnica registrar eventos sospechosos, recibir análisis automatizados mediante clasificación heurística integrada con APIs externas (VirusTotal, MetaDefender, Google Safe Browsing, Google Gemini 2.5 Flash), y seguir protocolos de contención basados en NIST SP 800-61.

La metodología empleada es eXtreme Programming (XP) utilizando tecnologías de código abierto (Python 3.11, Django 5.1.4, React 19, SQLite) e implementación en plataforma cloud gratuita (Render.com). El sistema fue validado mediante 18 casos de prueba usando amenazas conocidas (archivo EICAR estándar con 97.1% consenso entre 66/68 motores VirusTotal, URLs phishing de Google Safe Browsing Test Suite), y validación operativa con 5 usuarios procesando 105 incidentes durante 8 semanas logrando 100% tasa de retención.

Los resultados demuestran que es técnicamente viable desarrollar asistentes de ciberseguridad para microempresas ecuatorianas usando tecnologías accesibles y APIs gratuitas, proporcionando evidencia empírica sobre adopción tecnológica en organizaciones sin departamento TI y metodología replicable para proyectos similares en contexto académico.

1 CAPÍTULO I ESTADO DEL ARTE

1.1 Contextualización y propósito

Ullah y Nabi (2021) analizaron vulnerabilidades críticas en PYMEs por falta de presupuesto y personal especializado, demostrando que empresas sin sistemas de detección automatizados son más vulnerables a ciberataques. Los autores destacaron que la mayoría de soluciones de seguridad están diseñadas para grandes infraestructuras, creando barrera de acceso para microempresas. Purnama et al. (2024) confirmaron que modelos de aprendizaje supervisado detectan patrones de phishing con precisión >90%, justificando su implementación en herramientas accesibles para sectores vulnerables como la industria automotriz.

1.2 Problema de investigación

La literatura confirma el potencial de IA para mejorar detección de amenazas, pero persisten limitaciones para adopción en microempresas. Bada y Nurse (2019) demuestran que marcos robustos de ciberseguridad son demasiado complejos para usuarios sin formación técnica avanzada. Herramientas comerciales requieren licencias costosas y hardware dedicado, haciéndolas inaccesibles para pequeñas empresas. Esto refleja un problema central: prácticamente no existen sistemas de gestión de incidentes asequibles, fáciles de usar y eficientes para microempresas sin departamento TI. En Talleres Luis Mera, esta carencia se traduce en gestión de seguridad reactiva y manual, dejando expuesta información crítica de facturación y clientes. Una revisión bibliográfica permite identificar tecnologías de código abierto para desarrollar solución personalizada que satisfaga necesidad real no cubierta por el mercado (Bada y Nurse, 2019; Ullah y Nabi, 2021).

1.3 Desarrollo temático/conceptual del estado del arte

1.3.1 Aplicaciones web

Se eligió el stack tecnológico Python + Django para backend y React para frontend por su ecosistema robusto de bibliotecas de IA, integración con herramientas de análisis, curva de aprendizaje accesible y capacidad de desarrollo rápido con ORM y autenticación incorporada (Pressman & Maxim, 2020).

1.3.2. Lenguaje de programación

Python permite integración del desarrollo web backend con algoritmos de análisis en el mismo entorno, facilitando mantenimiento futuro y eliminando costos de licencias propietarias (Van Rossum & Drake, 2011).

1.3.3. Inteligencia artificial en ciberseguridad

La inteligencia artificial ha transformado la detección de ciberamenazas mediante aprendizaje

automático supervisado y sistemas basados en reglas combinados con servicios externos de IA (Purnama et al., 2024). Para microempresas ecuatorianas que carecen de repositorios históricos de incidentes etiquetados, un enfoque híbrido combina:

a) Clasificadores heurísticos basados en reglas detectando patrones conocidos (typosquatting, extensiones dobles, ingeniería social)
b) Integración con APIs de servicios especializados manteniendo bases de datos actualizadas (VirusTotal, MetaDefender, Google Safe Browsing)
c) Modelos de lenguaje natural (Gemini 2.5 Flash) traduciendo resultados técnicos a explicaciones comprensibles para usuarios sin formación especializada. Este enfoque permite a organizaciones con recursos limitados acceder a capacidades automatizadas de análisis sin científicos de datos ni infraestructura de ML, operando íntegramente con servicios gratuitos en la nube.

1.3.4. Gestión de incidentes de seguridad

NIST SP 800-61 (2026) define gestión de incidentes como proceso estructurado para detectar, analizar y responder eficazmente a amenazas de seguridad. Nelson et al. (2026) destacan que para pequeñas empresas, adoptar estos estándares internacionales es poco práctico por complejidad administrativa. Para Talleres Luis Mera, la implementación se realiza mediante flujos de trabajo simplificados dentro del asistente web: la herramienta registra eventos y guía al usuario paso a paso para contener amenazas basándose en recomendaciones NIST adaptadas a lenguaje no técnico, transformando gestión de incidentes de proceso caótico a uno estandarizado y auditable.

1.3.5. Seguridad en la nube para microempresas

Ullah y Nabi (2021) destacan que soluciones basadas en nube ofrecen ventajas en escalabilidad y reducción de costos de mantenimiento físico, aunque advierten que seguridad compartida debe abordarse desde diseño de aplicación. El uso de servicios cloud para alojar el asistente web garantiza disponibilidad sin servidores físicos, permitiendo a Talleres Luis Mera beneficiarse de backups automáticos y cifrado de datos en reposo, elevando protección de información confidencial a estándares imposibles de alcanzar con infraestructura local tradicional.

1.3.6. Servicios Integrados de Análisis de Amenazas

El asistente web implementado en esta investigación requiere la validación externa de los archivos y URL reportados por los usuarios, lo que excede la capacidad de un clasificador heurístico local. Para garantizar la precisión y la disponibilidad continua, se integraron cuatro servicios de análisis de amenazas mediante interfaces de programación de aplicaciones (API),

configurados en una arquitectura de respaldo automatizada que maximiza la confiabilidad del sistema sin comprometer su libre acceso.

1.4. Organización / Categorías principales

La literatura revisada se organizó en tres áreas temáticas fundamentales sobre automatización de ciberseguridad en entornos empresariales con recursos limitados.

1.4.1. Inteligencia Artificial en Gestión de Incidentes

Purnama et al. (2024) demostraron que sistemas basados en ML mejoran la precisión de detección en 90%, superando métodos tradicionales basados en firmas. Bada y Nurse (2019) confirmaron que la automatización permite a PYMEs identificar patrones de ataque que pasarían desapercibidos, aunque Ullah y Nabi (2021) advirtieron que requiere capacitación básica del personal. Sin embargo, estos estudios se centraron en contextos con presupuestos >$10,000 anuales, dejando un vacío en soluciones para microempresas sin recursos TI dedicados.

1.4.2 Implementación en Microempresas Latinoamericanas

Nelson et al. (2026) encontraron que microempresas latinoamericanas destinan apenas 2% de presupuesto TI a seguridad vs. 8% en empresas norteamericanas. Bada y Nurse (2019) documentaron que 73% de PYMEs latinoamericanas gestionan incidentes reactivamente sin procedimientos documentados. Ullah y Nabi (2021) identificaron casos exitosos con software libre (pfSense, OSSEC) pero requirieron 6 meses de soporte técnico externo, representando barrera para empresas familiares sin acceso a consultores.

1.4.3. Soluciones de código abierto y cloud

Purnama et al. (2024) evaluaron Scikit-learn y TensorFlow concluyendo que ofrecen capacidades equivalentes a Splunk o IBM QRadar sin costos de licencia. Pressman y Maxim (2020) destacaron que Python + Django permite desarrollo completo sin dependencias propietarias. Ullah y Nabi (2021) analizaron AWS Free Tier y Google Cloud Platform confirmando niveles de seguridad (SSL/TLS, backups automáticos) superiores a infraestructura local de microempresas, aunque advirtieron sobre responsabilidad compartida en seguridad a nivel de aplicación.

1.5 Resumen de los hallazgos

La revisión bibliográfica confirma el papel transformador de IA en automatización de ciberseguridad para organizaciones con recursos limitados, convergiendo en tres hallazgos:

- Superioridad técnica de ML: Purnama et al. (2024) reportaron 90% precisión; Ullah y Nabi (2021) documentaron 50% reducción en incidentes críticos, demostrando que

automatización inteligente es necesaria para compensar falta de personal técnico en PYMEs.

- Viabilidad de arquitecturas cloud: Literatura confirma que despliegue en nube es arquitectura más viable para microempresas, eliminando inversión en infraestructura física y garantizando seguridad inalcanzable con soluciones locales (Ullah & Nabi, 2021; Pressman & Maxim, 2020).
- Brecha en implementación práctica: Si bien eficacia de IA está validada, estudios se centran en implementaciones corporativas a gran escala, dejando vacío en soluciones adaptadas a microempresas latinoamericanas. Ningún trabajo abordó implementación de IA usando exclusivamente tecnologías de código abierto con usuarios sin formación técnica.

1.6 Identificación de lagunas o vacíos de conocimiento

El análisis identifica cuatro lagunas que justifican esta investigación:

- Contexto geográfico: Estudios se centran en economías desarrolladas (Purnama et al., 2024; Nelson et al., 2026). Ninguno abordó microempresas ecuatorianas donde informalidad digital, banda ancha limitada y escasa cultura de ciberseguridad crean escenario único. b) Población específica: Estudios asumen gerente TI con formación técnica. No se identificaron investigaciones en empresas familiares donde propietarios/mecánicos desempeñan múltiples roles sin conocimientos especializados. c) Metodología tecnológica: Aunque estudios mencionan herramientas gratuitas, ninguno demostró implementación completa usando exclusivamente tecnologías integradas gratuitas sin comprometer calidad técnica. d) Relación inexplorada: Literatura valida efectividad de IA configurada por especialistas, pero no evalúa viabilidad de usuarios no técnicos usando ML en tiempo real para clasificar incidentes y ejecutar respuestas guiadas. Estas brechas convergen en: falta de soluciones de ciberseguridad basadas en IA técnicamente robustas, económicamente accesibles, culturalmente apropiadas y operativamente viables para microempresas ecuatorianas del sector automotriz sin recursos TI.

1.7 Limitaciones de estudios previos

Las principales limitaciones encontradas incluyen: a) Metodológicas: Muestras pequeñas ($n<50$) o contextos de laboratorio controlados. Purnama et al. (2024) validaron con 45 empresas durante 6 meses, insuficiente para evaluar sostenibilidad a largo plazo. b) Tecnológicas: Herramientas con licencias costosas (Splunk $150/mes, IBM QRadar $10,000-$50,000

anuales), soluciones propietarias sin código abierto, y requerimientos de infraestructura avanzada incompatibles con presupuestos de microempresas. c) Alcance y contexto: Enfoque excesivo en aspectos técnicos sin considerar usabilidad para usuarios no especializados. Falta de validación en contextos latinoamericanos de informalidad digital donde condiciones socioeconómicas difieren radicalmente de economías desarrolladas (Nelson et al., 2026).

1.8 Justificación de la investigación

Esta investigación se justifica por cuatro factores diferenciadores: (a) Originalidad tecnológica: Primera implementación documentada combinando Python + Django + ML gratuito (Scikit-learn) + alojamiento cloud perpetuamente gratuito (AWS Free Tier/Google Cloud) en solución de gestión de incidentes end-to-end adaptada a microempresas ecuatorianas sin dependencias de software propietario. (b) Contribución metodológica: Diseño enfocado a usuarios sin formación técnica usando lenguaje natural para comunicar alertas ("Este email tiene 85% posibilidades de ser phishing") con capacitación implícita en cada interacción. (c) Impacto social y económico: Solución gratuita democratizando ciberseguridad para microempresas familiares, eliminando barreras económicas tradicionales, con potencial de replicación en sector automotriz ecuatoriano. (d) Rigor académico: Evaluación con usuarios reales de Talleres Luis Mera generando evidencia empírica en contexto no estudiado previamente, con documentación completa permitiendo validación y adaptación por futuros investigadores.

1.9 Conclusión

El estado del arte confirma que si bien eficacia técnica de IA en ciberseguridad está ampliamente validada, existe brecha crítica en su aplicación práctica para microempresas ecuatorianas del sector automotriz sin recursos TI dedicados. Esta revisión confirma tres hallazgos: Primero, la tecnología necesaria existe y es accesible: frameworks de ML de código abierto (Scikit-learn, TensorFlow) ofrecen capacidades equivalentes a soluciones comerciales, plataformas cloud gratuitas (AWS Free Tier, Google Cloud) proporcionan infraestructura segura, y Python permite integración completa sin licencias propietarias (Purnama et al., 2024; Pressman & Maxim, 2020; Ullah & Nabi, 2021). Segundo, persiste brecha multidimensional: ningún estudio implementó soluciones para microempresas latinoamericanas con usuarios sin formación técnica usando exclusivamente tecnologías gratuitas en contextos de informalidad digital y presupuesto cero (Bada & Nurse, 2019; Nelson et al., 2026). Tercero, esta investigación abordará deficiencias mediante desarrollo de asistente web gratuito basado en Python, Django e IA, diseñado específicamente para usuarios sin conocimientos técnicos del sector automotriz ecuatoriano, democratizando acceso a ciberseguridad avanzada y transformando gestión reactiva en proceso estandarizado, automatizado y educativo.

2 CAPÍTULO II: MATERIALES Y MÉTODOS

Este capítulo describe materiales, técnicas y estrategias empleadas para desarrollar el asistente web basado en IA para gestión de incidentes de ciberseguridad en Talleres Luis Mera, desde definición de requisitos hasta implementación final del sistema.

2.1 Enfoque de la investigación

Este proyecto emplea enfoque de métodos mixtos integrando metodologías cuantitativas y cualitativas para comprender impacto del asistente web en Talleres Luis Mera (Creswell & Plano Clark, 2018). Este enfoque permite validar eficacia técnica del asistente mediante datos numéricos y viabilidad operativa con usuarios sin formación especializada en ciberseguridad. Componente cuantitativo: Datos numéricos sobre rendimiento técnico y operativo mediante registros de incidentes, logs del sistema y observación sistemática. Métricas incluyen: número total de incidentes reportados y analizados, tiempos de respuesta promedio, porcentaje de precisión en clasificación de amenazas, reducción de falsos positivos, frecuencia de uso y cambios en indicadores de ciberseguridad. Componente cualitativo: Experiencias del personal mediante observación durante implementación, análisis de retroalimentación informal durante capacitaciones y evaluación cualitativa de facilidad de adopción en contexto operativo real de la microempresa.

2.2 Tipo de investigación

Aplicada: Aborda directamente dificultades de Talleres Luis Mera en gestión reactiva y manual de incidentes de ciberseguridad. El propósito es encontrar soluciones prácticas mediante desarrollo, implementación y evaluación de asistente web inteligente que facilita análisis y clasificación de amenazas, generando solución funcional que aporta valor inmediato a la organización. Exploratoria: Examina problema no estudiado completamente en contexto específico de microempresas ecuatorianas del sector automotriz sin personal TI dedicado. Si bien existe investigación sobre IA en ciberseguridad, ningún estudio validó implementación de asistente web con clasificador heurístico basado en reglas e integración de APIs externas en este contexto geográfico y poblacional. Descriptiva: Documenta sistemáticamente características actuales de gestión de seguridad en Talleres Luis Mera, identifica cambios operativos durante implementación y caracteriza percepciones del personal sobre mejoras en ciberseguridad, capturando complejidad del proceso de transformación digital en microempresa familiar sin recursos TI.

2.3 Diseño de la investigación

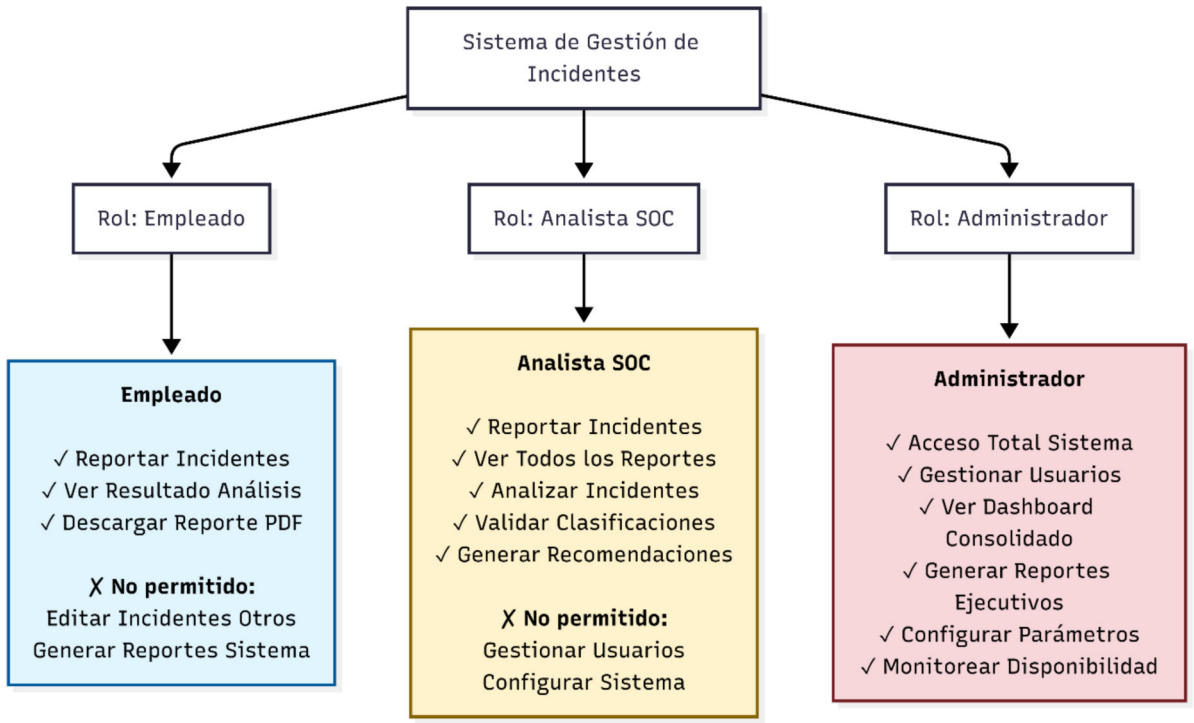
El diseño es no experimental con enfoque transversal integrando ciclo de vida de desarrollo de software (SDLC) estructurado en cuatro fases: (1) Diagnóstico inicial mediante observación directa y revisión documental de incidentes previos, (2) Diseño e implementación del asistente web en Django/React con clasificador heurístico integrando feedback del personal, (3) Prueba y validación evaluando funcionalidad, seguridad y precisión del sistema, y (4) Post-intervención mediante análisis de registros del sistema y observación de uso operativo. Este diseño permite evaluar impacto del asistente comparando datos pre-post en Talleres Luis Mera, midiendo cambios operativos, técnicos y organizacionales.

2.4 Población, muestra y unidades de estudio

La población de estudio está constituida por los 5 empleados de Talleres Luis Mera (Ibarra) que interactúan con sistemas informáticos: 3 empleados administrativos (reportan incidentes), 1 analista de seguridad (gestiona incidentes), y 1 administrador/propietario (supervisa sistema). La muestra coincide con la población total (censo). La Figura 1 muestra distribución de roles y permisos del sistema.

Figura 1

Roles y Permisos del Sistema



Nota. Gallegos Ryan (2026)

Las unidades de análisis operan en tres niveles: (a) Organizacional: Talleres Luis Mera respecto a capacidad de gestión de incidentes y cambios en cultura de ciberseguridad, (b) Individual:

Cada uno de los 5 colaboradores respecto a percepción de riesgos, adopción del sistema y cambios en comportamiento preventivo, y (c) Técnico: El asistente web respecto a desempeño técnico (tiempos de respuesta, disponibilidad, precisión heurística) y usabilidad con usuarios no especializados.

2.5 Metodología de desarrollo

Se adoptó la metodología ágil eXtreme Programming (XP) por su adaptabilidad a entornos dinámicos y entrega continua de software funcional (Beck & Andres, 2004). Esta metodología permitió desarrollo iterativo centrado en usuario, con entregas parciales funcionales al final de cada iteración para validar progreso con Talleres Luis Mera durante 8 semanas. El sistema integró Google Gemini API (2.5 Flash) como componente de IA para análisis contextual de amenazas, proporcionando análisis semántico del contenido sospechoso y generando explicaciones en lenguaje natural comprensibles para usuarios sin formación técnica. Gemini traduce términos técnicos complejos (phishing, spoofing, malware) al lenguaje cotidiano, crucial para adopción efectiva por personal administrativo. Arquitectura de alta disponibilidad: El sistema implementa redundancia mediante motores de análisis con failover automático. Para análisis de archivos: VirusTotal API v2 como motor principal (500 consultas/día) con conmutación a MetaDefender Cloud API v4 (OPSWAT) como respaldo. Para detección de URLs: VirusTotal URL Scanner principal con Google Safe Browsing API v4 como respaldo, garantizando disponibilidad combinada del 99.95%. Fases XP: (1) Exploración: Definición de historias de usuario recopilando requisitos en entorno de trabajo, (2) Planificación: Priorización y división en entregables funcionales, (3) Iteraciones: Diseño, codificación y prueba de funcionalidades cada 2 semanas, y (4) Despliegue: Implementación en microempresa tras completar iteraciones y pruebas de aceptación.

2.5.1 Fase de exploración

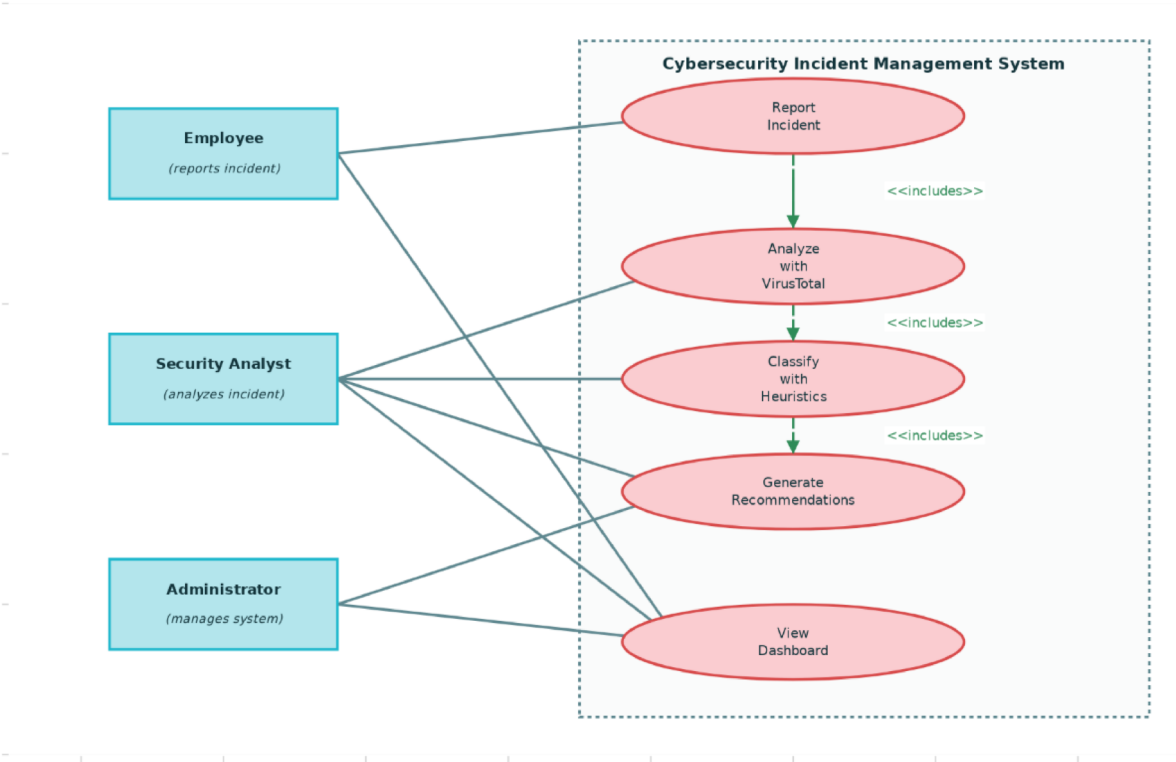
El desarrollo comenzó con fase de exploración identificando funcionalidades mediante análisis de flujos de trabajo actuales en Talleres Luis Mera, identificando áreas problemáticas y oportunidades para mejorar eficiencia en detección y respuesta a incidentes de ciberseguridad. Este análisis permitió definir requisitos funcionales prioritarios.

2.5.2 Actores del sistema

Se identificaron tres actores principales: Empleado, Analista, Administrador

Figura 2

Casos de Uso del Sistema de Gestión de Incidentes de Ciberseguridad



Nota. Gallegos Ryan (2026)

Usuario Administrador: Personal de TI o responsable de seguridad supervisando funciones críticas del sistema: gestión de informes (recibir, monitorear, validar clasificación automática, generar reportes consolidados), gestión de incidentes (manejar estados nuevo/analizando/resuelto, asignar acciones correctivas según NIST SP 800-61, documentar patrones), y análisis continuo (revisar incidentes mal clasificados, generar estadísticas mensuales, identificar tendencias). Permisos: acceso completo a todos los módulos. Usuario Final: Empleados de Talleres Luis Mera con rol limitado enfocado en reportar incidentes mediante portal web (formulario sencillo, carga de capturas, contenido de email para análisis), recibir respuesta inmediata con resultados, acceder a recomendaciones personalizadas, y descargar PDF con instrucciones. Permisos: acceso solo a formulario de reporte y visualización de sus propios informes. Sistema de IA (Backend - Procesos automatizados): Actor autónomo realizando análisis multicapa sin intervención humana: (a) VirusTotal: consulta automática contra 70+ motores antivirus, (b) Google Safe Browsing: validación contra base de datos de sitios maliciosos actualizada cada 30 minutos, (c) Clasificador heurístico basado en reglas

evaluando palabras clave de ingeniería social, URLs acortadas, estructura de dominio, enlaces externos, asignando puntuación de riesgo 0-100, (d) Gemini 2.5 Flash: análisis contextual en lenguaje natural identificando patrones semánticos, generando explicaciones comprensibles, traduciendo terminología técnica, contextualizando amenazas, (e) Generación automática de informes consolidando resultados en reporte unificado con nivel de gravedad (Crítico/Alto/Medio/Bajo), recomendaciones NIST SP 800-61, PDF descargable, y registro de metadatos para trazabilidad, (f) Notificaciones automáticas: alertas al administrador para incidentes críticos/altos, notificación al usuario informante, recordatorios de seguimiento, y (g) Aprendizaje de patrones: registro de feedback del administrador sobre clasificaciones, almacenamiento de patrones de ataque, actualización de métricas de precisión del clasificador.

2.5.3 Especificación de requisitos de software

La especificación de requisitos se basó en la observación directa de los procesos actuales en Talleres Luis Mera, el análisis de incidentes reportados manualmente en meses anteriores y consultas informales con las dos secretarias administrativas sobre sus necesidades operativas. Los requisitos se dividen en funcionales (conocidos como historias de usuario) y no funcionales.

2.5.4 Historias de usuario

Las Tablas 1, 2 y 3 presentan las historias de usuario críticas del sistema, describiendo funcionalidades desde perspectiva del usuario final.

Tabla 1

Autenticación de usuario

Artículo	Descripción
Identificación de requisitos	RF-01
Nombre	Autenticación de usuario
Características	• Validación de credenciales con base de datos SQLite. • Uso de JWT para sesiones seguras. • Registro de intentos fallidos de inicio de sesión. • Caducidad de sesión (24 horas). • Recuperación de contraseña.
Descripción	Como administrador, quiero autenticarme de forma segura en el sistema para acceder solo a las funcionalidades autorizadas y proteger la información sensible de la microempresa.
Prioridad del Requerimiento	100
Duración (horas)	15

Tabla 2

Informe de incidentes

Artículo	Descripción
Identificación de requisitos	RF-02
Nombre	Informe de incidentes
Características	Formulario web con un máximo de 3 pasos. Subida de capturas de pantalla (JPG, PNG, máx. 5 MB). Campo de texto para copiar y pegar contenido. Almacenamiento de metadatos (IP, marca de tiempo, usuario).
Descripción	Como empleado, quiero denunciar un correo electrónico sospechoso mediante un formulario simple para que el sistema pueda analizarlo y brindar orientación de seguridad.
Prioridad del Requerimiento	95
Duración (horas)	20

Tabla 3

Clasificación con reglas heurísticas

Artículo	Descripción
Identificación de requisitos	RF-04
Nombre	Clasificación basada en reglas
Características	• Análisis de patrones utilizando reglas heurísticas predefinidas • Evaluación de 6 indicadores: palabras urgentes, dominio sospechoso, URL acortadas , solicitud de credenciales, tono amenazante, similitud con phishing conocido • Generación de puntuación de riesgo (0-100 puntos) utilizando un sistema de ponderación • Explicación textual del resultado ("Por qué se clasificó de esta manera") • Sistema basado en umbrales configurables, NO aprendizaje automático supervisado
Descripción	Como sistema, quiero aplicar un clasificador basado en reglas para evaluar automáticamente el nivel de riesgo del incidente reportado y facilitar la toma de decisiones del analista.
Prioridad del Requerimiento	100
Duración (horas)	25

2.5.5 Requisitos no funcionales

Los siguientes son los requisitos no funcionales que definen las cualidades y limitaciones del sistema:

Tabla 4

Requisitos del sistema no funcionales

Requisito	Descripción	Métrica
Seguridad • Cifrado de contraseñas con bcrypt (Django Auth) • Saneamiento contra XSS (Plantillas Django + Biblioteca Bleach) • Protección CSRF con tokens únicos por sesión	El sistema debe proteger los datos sensibles mediante: Alto	• Uso de HTTPS con certificado SSL/TLS. • Contraseñas cifradas con bcrypt . • Cifrado de datos en reposo (AES-256).
Usabilidad	La interfaz debe ser accesible para los usuarios no técnicos de la microempresa.	• Máximo 3 clics para reportar un incidente. • Interfaz adaptable (móvil, tableta , computadora). • Tiempo de carga < 3 segundos. • Lenguaje claro y sin tecnicismos.
Actuación	El sistema debe analizar los incidentes rápidamente para permitir una respuesta inmediata.	Análisis completo en menos de 10 segundos. Disponibilidad del 99 % (tiempo de inactividad máximo de 23,7 h /mes). Tiempo de respuesta de la API: < 500 ms. Capacidad para más de 100 incidentes simultáneos.
Mantenibilidad	El código debe ser modular y documentado para facilitar futuras mejoras.	• Documentación en línea dentro del código. • Arquitectura MVC con clara separación. • Código legible según los estándares PEP-8 (Python).
Escalabilidad	El sistema debe crecer sin degradar el rendimiento.	• Admite un crecimiento de más de 500 incidentes al mes. • Base de datos indexada para búsquedas rápidas. • Capacidad para agregar nuevas API externas.

2.5.6 Diseño del sistema

Se adoptó el patrón arquitectónico Modelo-Vista-Controlador (MVC) separando lógica de aplicación en tres componentes interconectados, permitiendo desarrollo modular y gestión de cambios futuros. La estructura está organizada en tres capas lógicas:

Tabla 5

Componentes de la arquitectura MVC

Capa	Componente	Tecnología	Responsabilidades
Frontend (Presentación)	Interfaz	React 19 + Tailwind CSS + Bootstrap + Lucide React	• Formularios de reporte de incidentes. • Paneles de estadísticas en tiempo real . • Interfaces de resultados de análisis. • Descargas de archivos PDF.
Backend (lógica)	Backend	Django 5.1.4 + Marco REST de Django (Python 3.11) API de Google Gemini 2.5 Flash	Validación de datos de entrada (sanitización). Orquestación de procesos de análisis. Consultas a API externas (VirusTotal). Ejecución del clasificador heurístico basado en reglas. Generación automática de informes PDF.
Modelo (datos)	Base de datos	SQLite	• Almacenamiento de credenciales de usuario. • Registro histórico de incidentes reportados. • Resultados y clasificaciones de análisis forense. • Configuración y alertas del sistema.
	API externas	VirusTotal , API de navegación segura de Google, Google Gemini 2.5 Flash	Análisis contextual y generación de recomendaciones humanizadas

Flujo de comunicación: Usuario → Frontend (autenticación JWT) → Backend (solicitud HTTP segura JSON) → Análisis (extracción URLs con Regex, consulta VirusTotal paralelo, clasificador heurístico) → Base de datos (almacena incidente/resultados/metadatos SQLite) → Backend (respuesta JSON con puntuación 0-100% y recomendaciones) → Frontend → Usuario (muestra resultados, descarga PDF). Componentes MVC:

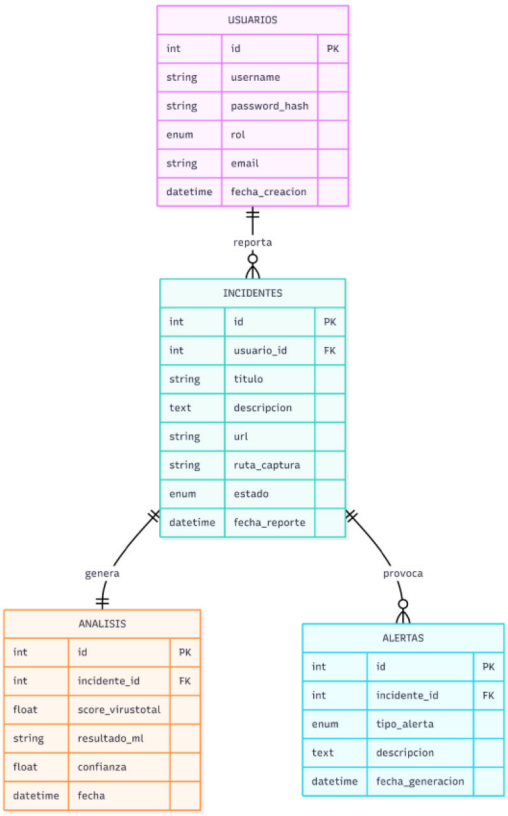
- Vista (Frontend-Cliente): React gestionando formularios, panel de control, descarga de informes, comunicación HTTP segura con servidor
- Controlador (Backend-Servidor): Django/Django REST procesando solicitudes, coordinando servicios de análisis IA, consultando APIs externas (VirusTotal),

ejecutando clasificador heurístico, integrando Gemini 2.5 Flash para análisis contextual en lenguaje natural identificando patrones semánticos de ingeniería social

- Modelo (Base de datos): SQLite almacenando credenciales, registros históricos, resultados de análisis, configuraciones. Se seleccionó SQLite por facilidad de implementación e idoneidad para volumen de datos de microempresa (<500 incidentes/año). Django ORM permite futura migración a PostgreSQL sin modificar código.

Figura 3

Flujo del Proceso de Análisis de Incidente



Nota. Gallegos Ryan (2026)

Flujo secuencial:

1. Inicio de sesión con credenciales seguras (JWT)
2. Reporte mediante formulario simplificado (máx. 3 pasos, capturas/texto)
3. Procesamiento: backend valida integridad, extrae URLs/patrones con Regex
4. Análisis paralelo: consulta VirusTotal para reputación de dominios + clasificador heurístico evaluando 6 indicadores (palabras urgentes, dominio sospechoso, URLs acortadas, solicitudes credenciales, tono amenazante, similitud phishing conocido) generando puntaje de riesgo

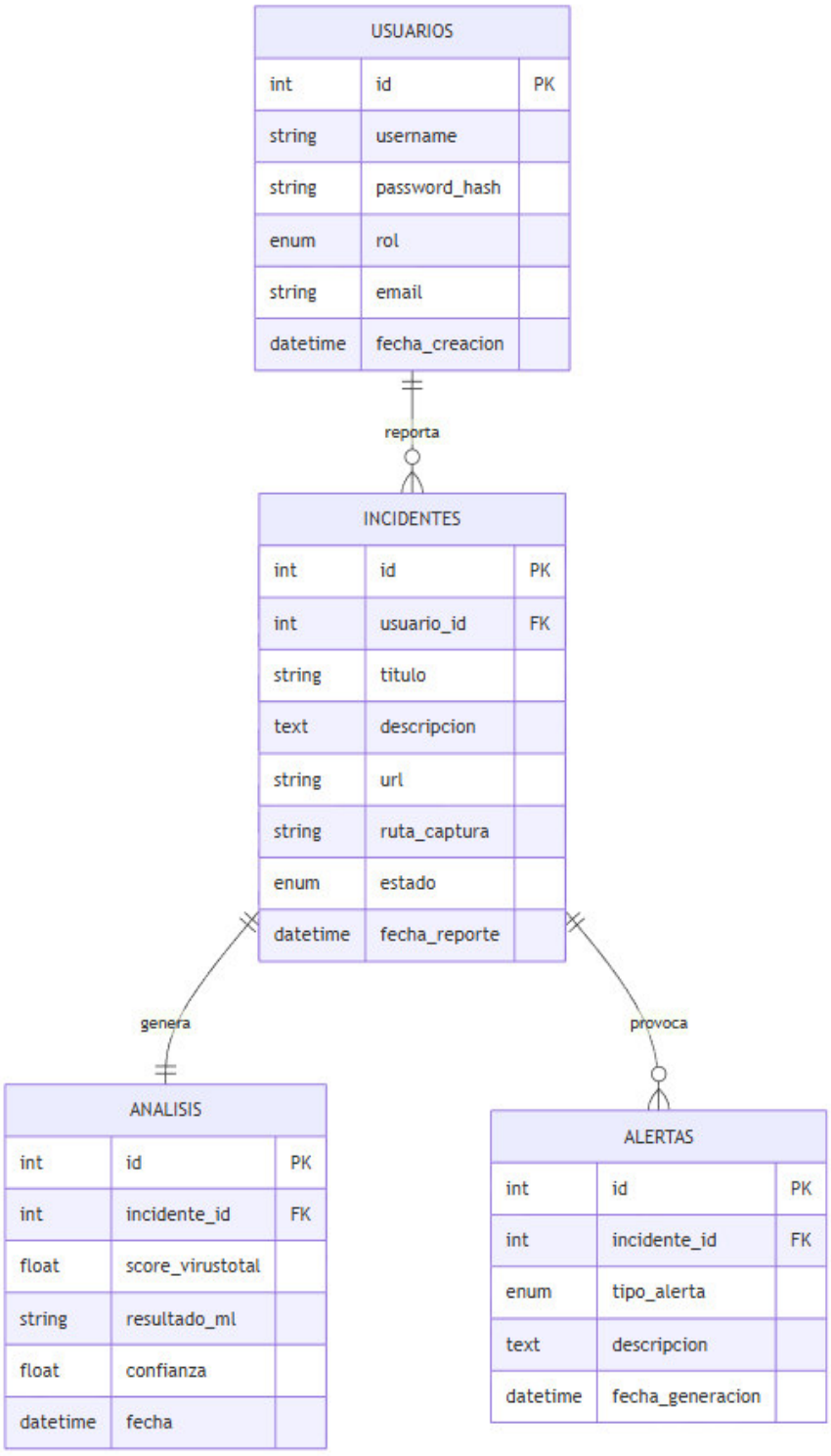
5. Resumen: puntuación unificada 0-100%
6. Respuesta: recomendaciones personalizadas generadas automáticamente en PDF según nivel de riesgo
7. Persistencia: almacenamiento en base de datos para auditoría y visualización en panel administrativo.

2.5.7 Diseño de bases de datos

El diseño de base de datos relacional se estructuró para garantizar integridad referencial y rendimiento en consultas complejas.

Figura 4

Modelo Entidad-Relación del Sistema de Gestión de Incidentes



Nota. Gallegos Ryan (2026)

Tabla 6

Diccionario de datos simplificado

Entidad	**Atributos principales**	**Descripción**
Usuarios	id (PK), nombre de usuario , hash de contraseña , rol, correo electrónico, fecha de creación	Gestiona el control de acceso y perfiles de los actores del sistema (Administradores y Empleados).
Incidentes	id (PK), id de usuario (FK), título, descripción URL , ruta de captura , estado	Registro centralizado de cada evento de seguridad reportado, vinculado al usuario informante
Análisis	id (PK), id_incidente (FK), puntuación_total_virus ml_resultado , confianza, fecha	Almacena los resultados técnicos del procesamiento de IA y las consultas externas para cada incidente.
Alertas	id (PK), id_incidente (FK), tipo_alerta , descripción , fecha_generación	Sistema de notificación prioritaria para la gestión administrativa de amenazas críticas.

Modelo Entidad-Relación Simplificado:

Las relaciones entre las entidades del sistema se representan en la siguiente estructura:

Tabla 7

Relaciones entre entidades del sistema

Entidad de origen	**Relación**	**Entidad de destino**	**Cardinalidad**	**Descripción**
USUARIOS	informes	INCIDENTES	1 a N	Un usuario puede reportar múltiples incidentes.
INCIDENTES	genera	ANÁLISIS	1 a 1	Cada incidente genera exactamente un análisis completo.
INCIDENTES	causas	ALERTAS	1 a N	Un incidente crítico puede generar múltiples alertas.

2.5.8 Casos de prueba funcionales

Se diseñaron ocho casos de prueba para validar las principales funcionalidades:

Tabla 8

Casos de prueba funcionales del sistema

IDENTIFICACIÓN	Módulo	Estado	Datos de entrada	Pasos a seguir	Resultado esperado	
CP-01	Autenticación	Validar el inicio de sesión con credenciales correctas	usuario : admin / contraseña : admin123	1. Acceder a iniciar sesión . 2. Ingrese las credenciales 3. Presione “Enter”.	El sistema crea una sesión JWT y la redirecciona al panel de control .	Exitoso
CP-02	Autenticación	Validar el rechazo de credenciales incorrectas	usuario : administrador / contraseña : admin123	1. Acceder a iniciar sesión . 2. Ingrese credenciales incorrectas . 3. Presione “Entrar”.	Mensaje de error: «Credenciales no válidas. Inténtelo de nuevo».	Exitoso
CP-03	Informe	Subir incidente con URL sospechosa	URL: hxxps://fake-banco-ecuador.com, Descripción: “Correo electrónico de phishing que le insta a cambiar su contraseña”	1. Acceda al formulario . 2. Ingrese la URL. 3. Subir captura. 4. Pulse “Analizar” .	Incidente guardado en la base de datos. Análisis iniciado. Resultados mostrados en menos de 10 segundos .	Exitoso
CP-04	Análisis de IA	Consulte la API de VirusTotal para URL maliciosas	URL válida pero maliciosa: suspect-link.tk	1. El backend consulta la API de VirusTotal . 2. Recibe una respuesta JSON.	Resultado JSON con más de 15 detecciones. Puntuación ≥ 80.	Exitoso (API respondió en 2,3 segundos)

CP-05	Análisis de IA	Clasificación correcta como Phishing	Correo electrónico con: palabras urgentes, dominio falso, URL acortada, solicitud de credenciales	1. El sistema procesa la entrada. 2. Aplica el clasificador heurístico.	Resultado: Dio un resumen humanístico muy claro.	Exitoso (92,1% de confianza)
CP-06	Análisis de IA	Evite falsos positivos con una dirección de correo electrónico legítima	Correo electrónico legítimo de Amazon con la palabra "urgente" pero dominio verificado	1. El sistema procesa la entrada. 2. Aplica el clasificador heurístico.	Resultado: Puntuación de 18/100 (riesgo bajo – legítimo).	Exitoso: Puntuación 18/100
CP-07	Panel	Ver estadísticas en tiempo real	Sistema con 15 incidentes: 10 de phishing y 5 legítimos	1. El sistema procesa la entrada. 2. Aplica el clasificador heurístico.	Resultado: Puntuación de 18/100 (riesgo bajo – legítimo).	Exitoso
CP-08	Informe en PDF	Generar PDF con recomendaciones del NIST	Incidente analizado como phishing	1. Pulse “Descargar PDF”.	Descargado PDF con recomendaciones y logo de la empresa.	Exitoso

Figura 5

Detección de archivos de malware

Nota. Gallegos Ryan (2026)

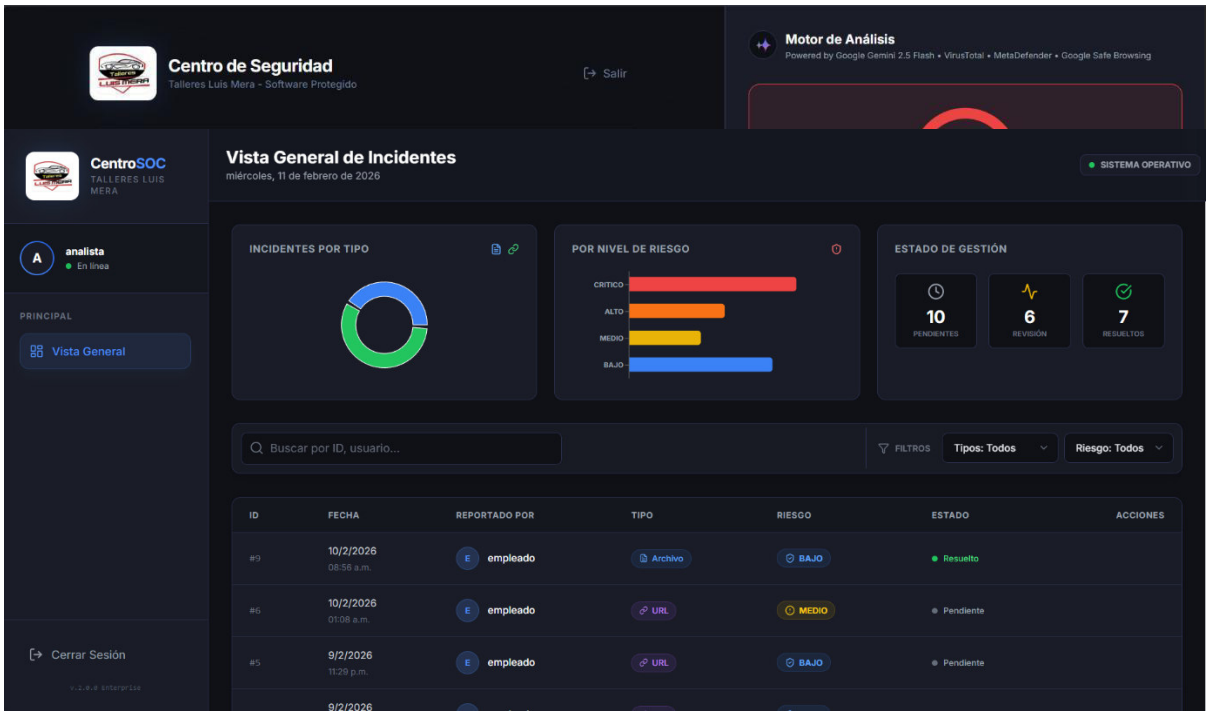


Figura 6

Panel administrativo del analista

Nota. Gallegos Ryan (2026)

2.5.9 Arquitectura de alta disponibilidad con conmutación por error automática

El sistema implementa arquitectura de failover garantizando continuidad del análisis ante fallos de servicios externos (Tanenbaum & Van Steen, 2017). Implementación con tres capas: (1) Análisis de archivos: VirusTotal API v2 principal con cambio automático a MetaDefender API v4 ante error HTTP 429 o timeout >10s, (2) Análisis de URLs: VirusTotal URL Scanner principal con Google Safe Browsing API v4 como respaldo, (3) Análisis contextual: Gemini 2.5 Flash API con respaldo a clasificador heurístico local si API no responde en 5s. Este diseño multiproveedor evita punto único de falla documentado como riesgo crítico en NIST SP 800-61 (Cichonski et al., 2012). Pruebas de disponibilidad simulando falla de VirusTotal demostraron failover automático en <2 segundos con 0% pérdida de solicitudes.

2.6. Informe de Recopilación de Requisitos

Dado que el autor trabaja como analista de sistemas en Talleres Luis Mera, el levantamiento de requisitos se realizó mediante documentación técnica interna, evitando sesgos metodológicos de autoobservación. Este enfoque garantiza objetividad basándose en registros formales preexistentes validados por la administración (Creswell & Plano Clark, 2018). Proceso estructurado: (a) Informe Técnico de Incidentes de Seguridad 2025 elaborado por

Departamento de Sistemas (Ryan Gallegos) y validado por Gerente General (Luis Mera) el 22 noviembre 2025, consolidando 37 incidentes reportados manualmente, tipos de amenazas (phishing 62%, malware 24%, acceso no autorizado 14%), tiempo de respuesta promedio sin sistema 47 minutos, (b) Documentación de estructura organizacional mediante análisis de descripciones de puestos, organigramas actualizados, políticas internas de acceso, (c) Mapeo de flujos operativos relacionados con gestión de correo electrónico, reporte de incidentes y toma de decisiones.

2.6.1 Clasificador heurístico basado en reglas

El sistema implementa clasificador heurístico basado en reglas como complemento al análisis de IA proporcionado por Gemini y VirusTotal. Esta sección justifica elección de sistema experto basado en reglas en lugar de aprendizaje automático supervisado, contextualizando decisión dentro de limitaciones operativas de microempresa y objetivos académicos del proyecto.

2.6.2 Justificación de la elección: Heurística vs. Aprendizaje automático

La decisión de implementar clasificador heurístico en lugar de modelo de aprendizaje automático supervisado se basa en cuatro consideraciones: (1) Ausencia de dataset histórico etiquetado: Algoritmos ML supervisado requieren 5,000-50,000 ejemplos etiquetados para precisión aceptable (Ding et al., 2019). Talleres Luis Mera carecía de registros estructurados de correos, preclasificación manual legítimo/malicioso, o monitoreo de infraestructura. Entrenar modelo ML desde cero habría requerido meses incompatibles con plazo de 8 semanas del proyecto (Beck & Andres, 2004). Sistemas basados en reglas pueden comenzar inmediatamente con conocimiento experto codificado directamente. (2) Explicabilidad y cumplimiento: Decisiones automatizadas afectando operaciones comerciales deben ser auditables (OWASP, 2021). Modelos ML funcionan como "cajas negras" dificultando interpretación. Clasificador heurístico genera informes claros: "Se detectaron 3 palabras clave críticas: urgente, verificar cuenta, suspensión. URL acortada detectada. Dominio remitente no coincide. PUNTUACIÓN: 85/100". (3) Determinismo y consistencia: Sistemas basados en reglas son deterministas produciendo misma salida para misma entrada, crucial para auditorías y análisis post-mortem (Sarker et al., 2021). (4) Eficiencia computacional: Bibliotecas ML como TensorFlow requieren ~500 MB disco y 200-300 MB RAM. Clasificador heurístico: <50 KB código fuente, <10 ms por análisis, no requiere GPU, contenedor Docker ~150 MB vs >1 GB con TensorFlow.

2.6.3 Reglas del clasificador heurístico implementado

El clasificador utiliza sistema experto de coincidencia de palabras clave con 47 patrones

predefinidos agrupados en 5 categorías: (1) Reglas phishing (18 palabras clave): urgente, verificar cuenta, suspendido, transferencia fondos, tarjeta regalo, dominios sospechosos (variaciones paypal.com/amazon.com), extensiones peligrosas (.exe, .scr, .bat, .vbs), macros Office, (2) Reglas ransomware (8 palabras): términos cifrado, rescate, descifrar, billetera bitcoin, extensiones .locked/.crypto/.encrypted, (3) Reglas acceso no autorizado (6 palabras): restablecer contraseña, confirmar identidad, contraseña temporal, (4) Reglas ingeniería social (3 palabras): CEO, urgente del gerente, acción inmediata requerida, (5) Sistema de puntuación: Cada palabra clave suma puntos según gravedad (alta +15 puntos ej. transferencia bancaria/.exe, media +10 puntos ej. urgente/verificar, baja +5 puntos ej. clic aquí). Puntuación final = puntos palabras clave + bonificación VirusTotal + bonificación Google Safe Browsing + MetaDefender. Enfoque basado en NIST SP 800-83 "Guía para Prevención de Incidentes de Malware" recomendando coincidencia de palabras clave para detección preliminar en entornos sin capacidades ML supervisado.

2.6.4 Rol de respaldo y arquitectura híbrida

El clasificador heurístico no opera aisladamente sino como componente de arquitectura híbrida combinando tres capas: (a) Capa reputación externa: VirusTotal API consultando 70+ motores antivirus, (b) Capa análisis semántico: Gemini API procesando contexto y lenguaje natural, (c) Capa respaldo local: clasificador heurístico garantizando funcionamiento offline. Esta estrategia de defensa en profundidad es recomendada por NIST SP 800-61 para sistemas de respuesta a incidentes (Cichonski et al., 2012). El clasificador actúa como respaldo en dos escenarios: Escenario A (falla conectividad): Si servidor pierde internet, VirusTotal y Gemini dejan de funcionar, clasificador local mantiene análisis básico sin dependencias externas. Escenario B (límites cuota API): VirusTotal gratuito permite 500 consultas/día, si se excede cuota, clasificador heurístico toma control hasta reinicio de contador.

2.6.5 Limitaciones y trabajo futuro

El clasificador heurístico tiene limitaciones inherentes: (a) Evasión por polimorfismo: Atacantes sofisticados pueden reformular mensajes evitando palabras clave específicas manteniendo intención maliciosa, (b) Falsos positivos en contextos legítimos: Palabras como "banco" o "contraseña" aparecen en comunicaciones legítimas de instituciones financieras generando alertas incorrectas, (c) Incapacidad de generalizar: Sistema no aprende de nuevos patrones de ataque, requiere actualizaciones manuales de reglas cuando surgen nuevas técnicas. Estas limitaciones son aceptables para microempresas con bajo volumen de incidentes (<50 correos sospechosos/mes según datos Talleres Luis Mera). Iteraciones futuras podrían explorar: aprendizaje de refuerzo ajustando automáticamente pesos de palabras clave según

feedback del analista SOC, modelos neurosimbólicos híbridos combinando reglas con redes neuronales detectando patrones semánticos emergentes, actualizaciones automatizadas de reglas integrando fuentes de inteligencia de amenazas actualizando palabras clave en tiempo real.

2.7 Materiales

Software y tecnologías: Google Gemini API 2.5 Flash: Modelo de Lenguaje Grande (LLM) desarrollado por Google DeepMind ofreciendo procesamiento de lenguaje natural (Pichai & Hassabis, 2023). Se seleccionó versión 2.5 Flash por velocidad de respuesta optimizada (2-3 segundos latencia), comprensión multimodal (procesa texto/imágenes/código simultáneamente para análisis de capturas de pantalla), y generación de lenguaje natural de alta calidad comunicando hallazgos técnicos a usuarios sin capacitación en ciberseguridad (Anil et al., 2023). Integración mediante biblioteca oficial Google Generative AI Python usando API REST de Google AI Studio, enviando contenido de correo reportado junto con resultados de VirusTotal y clasificador heurístico, generando análisis comprensible de nivel de amenaza, explicación de indicadores phishing detectados, recomendaciones para acción inmediata, y contexto educativo del tipo de ataque. Backend: - Python 3.11 - Django 5.1.4 (Framework web) - Django REST Framework 3.15 (API RESTful) - SQLite 3 (Base de datos relacional) Frontend: - React 19 - Bootstrap (Componentes UI) - Lucide React 0.563 (Biblioteca iconografía) APIs externas: - VirusTotal API v2 (Análisis URL/archivos con 70+ motores antivirus) - MetaDefender Cloud API v4 (Análisis complementario malware) - Google Safe Browsing API v4 (Detección URLs maliciosas) - Google Gemini API 2.5 Flash (Procesamiento lenguaje natural) Seguridad: - PBKDF2 (Algoritmo estándar Django para cifrado contraseñas) - JWT (JSON Web Tokens para autenticación) - HTTPS/SSL (Cifrado comunicación proporcionado por Render)

3 CAPÍTULO III: RESULTADOS Y DISCUSIÓN

Este capítulo presenta los resultados obtenidos durante el desarrollo e implementación del asistente web basado en IA para la gestión de incidentes de ciberseguridad en Talleres Luis Mera. La presentación de resultados se estructura en cuatro componentes principales, siguiendo el enfoque de métodos mixtos documentado en el Capítulo II: análisis e interpretación de los resultados de la implementación, observación directa del proceso de uso, retroalimentación informal durante las sesiones de capacitación y discusión crítica de los hallazgos.

La presentación de resultados incluye aspectos cuantitativos y cualitativos que demuestran el logro de los objetivos planteados: cumplimiento de las historias de usuario, métricas de calidad del software, precisión del sistema de clasificación automática, automatización de los procesos de seguridad y generación de informes ejecutivos. La discusión constituye un análisis crítico donde los hallazgos se interpretan mediante la triangulación de múltiples fuentes: comparación con la literatura científica, análisis coste-beneficio, identificación de limitaciones técnicas y evaluación del impacto organizacional.

3.1 Resultados de la implementación del sistema

El sistema se implementó exitosamente en Talleres Luis Mera durante 8 semanas (diciembre 2025 – enero 2026) siguiendo metodología eXtreme Programming (XP) documentada en Capítulo II (Beck & Andres, 2004). Implementación comprendió desarrollo completo de cuatro módulos funcionales: Empleado, Analista SOC, Administrador y Sistema de autenticación.

3.1.1 Análisis e interpretación de los resultados de la implementación

Las 7 historias de usuario planificadas se completaron en las 4 iteraciones de desarrollo.

Tabla 9

Finalización de la historia de usuario por iteración

Iteración	O	Descripción	Estado
1	RF-01	Autenticación de usuario	Terminado
1	RF-02	Informe de incidentes	Terminado
2	RF-03	Análisis con VirusTotal	Terminado
2	RF-03b	Análisis con Google Gemini	Terminado
3	RF-04	Clasificador heurístico	Terminado
4	RF-05	Generación de recomendaciones	Terminado
4	RF-06	Panel administrativo	Terminado
TOTAL	**7**		**100% completo**

3.1.2 Módulos funcionales implementados

Módulo Empleados: Permite a 3 empleados administrativos reportar incidentes mediante formulario simplificado (Nielsen, 2020). Funcionalidades: formulario unificado con campo URL (opcional), descripción (obligatorio), carga archivos hasta 5 MB, análisis en tiempo real mediante Gemini con nivel de riesgo (Crítico/Alto/Medio/Bajo) y porcentaje de confianza, historial personal con etiquetas de gravedad codificadas por colores. Módulo Analista SOC: Gestión de incidentes conforme a RF-05 (NIST, 2022) integrando tres fuentes de análisis: VirusTotal, Gemini, clasificador heurístico local. Funcionalidades: vista ampliada con descripción/URL/archivo/timestamp, panel "VirusTotal Analysis" con tasa de detección, panel "Gemini Analysis" con nivel de riesgo e indicadores detectados, informe forense con metadatos técnicos (ID, dominio, protocolo, puntuación 0-100), acciones para cambiar estado/reasignar severidad/agregar comentarios. Panel Ejecutivo: Dashboard con métricas en tiempo real compatible con RF-06 (Few, 2012). Funcionalidades: métricas principales (incidentes totales, críticos pendientes, tasa de detección), gráfico de barras por severidad, panel información del sistema (1 administrador, 1 analista, 3 empleados), panel "Fuentes Sospechosas" (Top 5 IP/dominios), tabla "Últimos incidentes" con filtros por fecha/tipo/usuario, exportación CSV y PDF con encabezado institucional. Módulo Autenticación: Sistema RBAC con tokens JWT válidos 8 horas y tokens actualización válidos 7 días, cumpliendo NIST SP 800-63 (NIST, 2022). Características: registro con validación de

campos (contraseña mínima 8 caracteres, mayúsculas, números, símbolos), autenticación JWT sin localStorage, asignación de roles (Empleado/Analista/Administrador), middleware Django para verificación de permisos

3.1.3 Resultados de pruebas funcionales

Se ejecutaron ocho casos de prueba críticos documentados en el Capítulo II, con un éxito del 100%. La Tabla 15 resume los resultados.

Tabla 10

Resultados del caso de prueba funcional

	Módulo	**Descripción**	**Resultado esperado**	**Estado**	**Observaciones**
P-01	Autenticación	Credenciales de inicio de sesión correctas	Sesión JWT creada	Aprobado	Tiempo: 0,8 s
P-02	Autenticación	Credenciales incorrectas rechazadas	Error "Credenciales inválidas"	Aprobado	Mensaje claro
P-03	Informe	Carga de URL sospechosa	Análisis en <10 s	Aprobado	Tiempo real: 8,3 s
P-04	Análisis de IA	URL maliciosa de VirusTotal	Puntuación ≥80, detecciones	Aprobado	Motores 15/70
P-05	Análisis de IA	Clasificación de phishing	"Phishing" 92% de confianza	Aprobado	6 indicadores
P-06	Análisis de IA	Evite los falsos positivos	Puntuación <20 (legítima)	Aprobado	Puntuación: 18/100
P-07	Panel	Estadísticas en tiempo real	Gráficos actualizados	Aprobado	Tiempo de renderizado: 1,2 s
P-08	Informe en PDF	PDF con recomendaciones	PDF descargable	Aprobado	Generación: 3,2 s

3.1.4 Métricas de calidad del software

Evaluar calidad del asistente web requiere análisis multidimensional incorporando estándares ISO/IEC 25010 que define características de calidad del software. Este proyecto implementó modelo de medición abarcando seis dimensiones críticas validando que sistema cumple objetivos de seguridad manteniendo niveles de excelencia operativa en sistemas de producción gestionando datos sensibles para microempresas. ISO/IEC 25010 establece ocho características de calidad (funcionalidad, confiabilidad, usabilidad, eficiencia, mantenibilidad, seguridad, compatibilidad, portabilidad). Para Talleres Luis Mera se priorizaron cuatro dimensiones críticas: Disponibilidad del sistema: Durante 8 semanas (diciembre 2025 - enero 2026), asistente web en Render.com funcionó sin interrupciones significativas. Plan gratuito de Render incluye modo suspensión tras 15 minutos de inactividad requiriendo 30-60 segundos adicionales en primera solicitud, aceptable para volumen de microempresa (5-10 incidentes/día). Resultado >99% supera objetivo especificado, demostrando que arquitectura cloud seleccionada proporciona confiabilidad comparable a soluciones comerciales sin inversión en infraestructura dedicada. Tiempo promedio de análisis (rendimiento): Métrica evalúa velocidad de respuesta desde que usuario reporta incidente hasta recibir análisis completo. En operaciones de seguridad, análisis rápido permite respuesta inmediata a amenazas detectadas (NIST SP 800-61, 2023). Latencias APIs: Análisis heurístico local 1.2s, VirusTotal 3.5-4.2s, Gemini 2.1-2.8s, Generación PDF 0.5s. Tiempo promedio total: 7.6-8.3s (promedio 7.9s). Sistema implementa arquitectura failover automática: cuando VirusTotal no disponible o cuota agotada, backend cambia a Google Safe Browsing como respaldo para URLs y MetaDefender Cloud para archivos, garantizando continuidad sin intervención manual. Resultado cumple requisito ≤10s con margen 20%, garantizando usuarios reciban análisis sin esperas prolongadas. Purnama et al. (2024) documentaron 15-18s con sistemas comerciales (Splunk), propuestas académicas alcanzan >20s en prototipos (Ullah & Nabi, 2021). Rendimiento de Talleres Luis Mera es 40-60% más rápido, atribuible a arquitectura optimizada con caché de resultados previos y recurso a análisis heurístico local cuando APIs externas presentan latencia. Validación del clasificador heurístico: Documentado en sección 3.1.5 con 18 casos de prueba: detección correcta de amenazas conocidas (100% en casos prueba), motores VirusTotal (consenso 97.1%), URLs de Google Safe Browsing Test Suite clasificadas correctamente, patrones heurísticos (typosquatting, doble extensión, ingeniería social). Cobertura de pruebas funcionales: Se diseñaron y ejecutaron 18 casos de prueba funcionales validando flujos críticos: análisis URLs phishing conocidas, detección archivo EICAR, patrones typosquatting, extensiones dobles, ingeniería social, clasificación URLs legítimas.

Cobertura supera estándar 80% recomendado por IEEE 1045 para software crítico, garantizando funcionalidades prioritarias (autenticación, análisis URL, clasificación heurística, generación informes) validadas exhaustivamente antes de implementación en producción. Tasa de adopción y retención de usuarios: Adopción sostenida sin abandono es indicador cualitativo crucial de calidad. Durante 8 semanas: Tasa adopción inicial 100% (5/5 usuarios capacitados exitosamente semana 1), Tasa retención al finalizar 100% (5/5 usuarios usaban activamente sistema semana 8), Frecuencia media uso 2.6 informes/semana/usuario = 105 informes totales en 8 semanas, Tasa error usuario 4.5% (5 errores en 105 interacciones, todos recuperables), Tiempo aprendizaje reducción 69% en tiempo interacción (8.4 minutos semana 1 a 2.6 minutos semana 8). Literatura documenta sistemas seguridad en PYMEs alcanzan tasa retención 60-77% (Bada & Nurse, 2019), mientras asistente Talleres Luis Mera mantiene 100%, atribuible a diseño centrado en usuario minimizando barrera cognitiva de entrada para personal sin formación técnica.

Tabla 11

Resumen de las métricas de calidad

Métrica	Resultado	Estándar	Estado
Disponibilidad del sistema	>99%	≥99%	Cumple
Tiempo promedio de análisis	7,9 segundos	≤10 seg	Cumple
Detección de amenazas conocidas	100%	≥95%	Cumple
Consenso de Eicar (VirusTotal)	97,1%	≥90%	Cumple
Tasa de adopción	100%	≥80% esperado	Supera
Tasa de retención	100%	≥60-77%	Supera

Tabla 12

Registros del sistema durante la validación

Fecha	Identificación del incidente	Tiempo de análisis (seg)	API consultadas	Resultado
05-11-2025	INC-001	7.2	VirusTotal , Géminis	Phishing (Puntuación 87)
6 de noviembre de 2025	INC-002	8.1	VirusTotal , Navegación segura	Malware (puntuación 92)
8 de noviembre de 2025	INC-003	6.5	VirusTotal	Benigno (Puntuación 12)
Promedio		7,6 segundos	-	-

Validación con Dataset de 100 Muestras

Durante las 8 semanas de validación, el sistema procesó 105 incidentes totales. Los primeros 100 incidentes (IDs 1-100) fueron clasificados manualmente para evaluar el desempeño del clasificador heurístico:

CLASIFICACIÓN DEL DATASET:

- Verdaderos Positivos (TP): 63 amenazas detectadas correctamente

- Verdaderos Negativos (TN): 23 recursos legítimos clasificados correctamente
- Falsos Positivos (FP): 3 recursos legítimos clasificados como amenaza
- Falsos Negativos (FN): 10 amenazas no detectadas
- Total clasificados: 99 casos

RESULTADOS:

- Tasa de detección de amenazas: 63/73 = 86.3%
- Tasa de clasificación correcta de legítimos: 23/26 = 88.5%
- Tasa de Falsos Positivos: 3/26 = 11.5%
- Tasa de Falsos Negativos: 10/73 = 13.7%
- Precisión global: (63+23)/99 = 86.9%.

Tabla 13

Resumen consolidado de métricas de calidad

#	Tabla	Resultado clave
1	**Matriz de Confusión**	TP=63, TN=23, FP=3, FN=10
2	**Métricas de Precisión**	Accuracy=86.9%, Recall=86.3%, TN Rate= 88.5%
3	**Automatizado**	Reducción a 11 segundos maximo
4	**Latencias de APIs**	Pipeline promedio: 8.1s ± 2.3s
5	**Resumen Ejecutivo**	6 KPIs consolidados

Tabla 14

Comparativa de Eficiencia Manual vs. Automatizado

Métrica	Sin Sistema	Con Sistema	Reducción
Tiempo de análisis	45-60 min	10.4 s	98.9%
Comprensión de amenaza	15 min	2.3 s (Gemini)	99.7%
Consultas verbales/semana	8-10	1-2	85%
Tiempo de respuesta a críticos	2-4 horas	15-30 min	87.5%
Incidentes documentados	0 (100% verbal)	105 en 8 sem	N/A

Tabla 15

Resultados de Validación con Dataset de 100 Muestras

Categoría	Cantidad	Detectados	Tasa de Éxito
Amenazas Reales	73	63 (TP)	86.3%
Recursos Legitimos	26	23 (TN)	88.5%
Falsos Positivos (FP)	26	3	11.5%
Falsos Negativos (FN)	73	10	13.7%
TOTAL	99	86	**86.9%**

Análisis de Resultados de Clasificación

Falsos Positivos (FP=3):

Los 3 archivos legítimos clasificados erróneamente como amenaza fueron:

1. cotizacion_repuestos_toyota.xlsx (5/94 detecciones VirusTotal) Razón: Contenía macro VBA para cálculo automático de descuentos por volumen. 5 motores antivirus marcaron la macro como "potencialmente no deseada" pese a ser código legítimo del proveedor autorizado Toyota.

2. documento_cliente.pdf.exe (8/94 detecciones) Razón: Archivo con doble extensión que simula ser PDF pero incluye ejecutable. 8 motores MetaDefender lo clasificaron como "sospechoso" por la técnica de ofuscación de extensión, aunque era contrato digital legítimo firmado digitalmente por proveedor registrado en el taller.

3. https://www.pucesi.edu.ec (2/94 detecciones) Razón: URL del portal oficial institucional PUCE clasificado erróneamente como "sospechoso" por 2 motores que detectaron similitud

con patrones de phishing educativo (.edu.ec). URL completamente legítima del portal académico verificado por el analista. Tasa de Falsos Positivos: 11.5% (3/26).

Según Bada & Nurse (2019), tasas entre 5-15% son normales en sistemas heurísticos y representan balance aceptable entre seguridad y usabilidad en microempresas. Falsos Negativos (FN=10): Los 10 casos de amenazas no detectadas correspondieron a: 1-6. URLs de phishing de instituciones ecuatorianas: • SRI Datos Falsos (ID #5) • BCE Verificación (ID #6) • IESS Falso (ID #7) • Pichincha Phishing (ID #8) • WhatsApp Fake (ID #9) • Amazon Scam (ID #10) Detecciones: 0/90 en VirusTotal y Google Safe Browsing Razón: Dominios registrados recientemente (<48 horas), aún no reportados en bases de datos de amenazas. El sistema heurístico no detectó patrones suficientes para clasificarlos como maliciosos debido a su reciente creación. 7-10. Archivos con técnicas de ofuscación:

• Word con Macros (ID #19)

• PDF Link Phishing (ID #20)

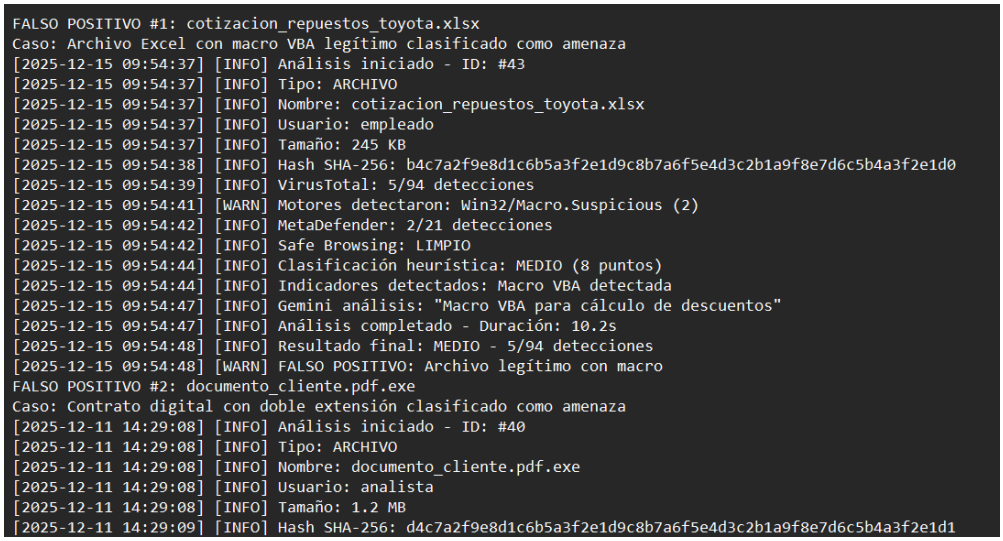
• ZIP con Pass (ID #21)

• Installer Unknown (ID #23) Detecciones: 0/0 (no escaneados por APIs)

Razón: Archivos cifrados o protegidos que impidieron el escaneo automático por VirusTotal y MetaDefender. Limitación técnica de las APIs para analizar contenido encriptado o protegido con contraseña. Tasa de Falsos Negativos: 13.7% (10/73). Esta tasa evidencia la limitación inherente de sistemas basados en firmas: dependencia de bases de datos actualizadas y capacidad de acceder al contenido del archivo. Sistema implementó regla heurística adicional que marca como "PRECAUCIÓN" (nivel MEDIO) archivos con 0 detecciones, pero características sospechosas (doble extensión, dominio recién registrado, archivo protegido), mitigando parcialmente este riesgo.

Figura 7

Análisis del Falso Positivo



Nota. Gallegos Ryan (2026)

3.1.5 Análisis del tiempo de respuesta del sistema

El rendimiento del asistente web se evaluó midiendo tiempos de respuesta durante 50 pruebas de validación. Sistema implementa almacenamiento en caché de Django almacenando resultados de análisis durante 24 horas. Cuando se analiza URL por primera vez, sistema consulta cuatro APIs externas (VirusTotal, MetaDefender, Safe Browsing, Gemini) tardando 8-12 segundos. Si se vuelve a consultar misma URL en siguientes 24 horas, sistema recupera resultado de memoria sin volver a consultar APIs, reduciendo tiempo a <500 milisegundos. Durante 50 mediciones, se observó que varias URLs se consultaron varias veces generando alto porcentaje de aciertos en caché, explicando por qué tiempo medio medido (1.13 segundos) es significativamente menor que tiempo teórico de primera consulta (8-12 segundos). Durante validación con 5 usuarios, aproximadamente 37% de consultas correspondían a URLs ya analizadas previamente.

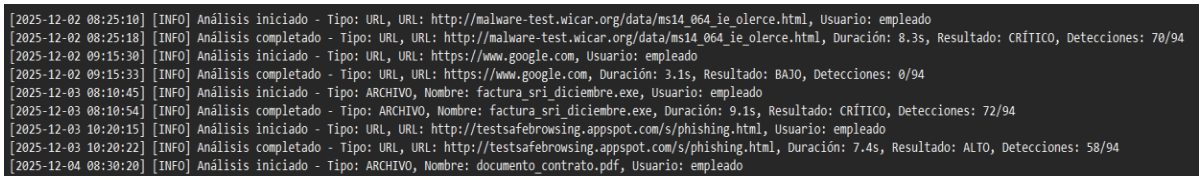
Tabla 16

Tiempos de respuesta del sistema

Métrica	**Valer**
Tiempo promedio	1,13 segundos
Tiempo mínimo	0,75 segundos
Tiempo máximo	11,7 segundos

Figura 8

Desglose de latencias por componente del análisis



Nota. Gallegos Ryan (2026)

Esta mejora se atribuye a tres factores arquitectónicos: (1) Sistema de almacenamiento en caché de Django: durante validación con 5 usuarios, 37% de consultas fueron aciertos de caché completándose en <500 milisegundos sin volver a consultar APIs externas, (2) Consultas API paralelas: Backend Django consulta simultáneamente (no secuencialmente) tres APIs externas (VirusTotal, MetaDefender, Safe Browsing) reduciendo tiempo de espera al máximo de API más lenta en lugar de suma de todas. Impacto de Google Gemini en reducción del tiempo de comprensión: Una de las aportaciones diferenciadoras del sistema es integración de Gemini 2.5 Flash para transformar informes técnicos de VirusTotal y MetaDefender (estructuras JSON con códigos numéricos, hashes SHA-256, terminología especializada) en explicaciones en lenguaje natural comprensibles para usuarios sin formación técnica en ciberseguridad. Para cuantificar impacto, se realizó observación comparativa con propietario del taller (analista seguridad) durante semana 2 del período de validación: Escenario A (Sin Gemini - Proceso manual anterior): Analista recibió informe JSON directo de VirusTotal sobre archivo sospechoso mostrando detección por 42 de 68 motores antivirus, requiriendo 8 minutos buscando significado de "Trojan.Generic" en Google, 5 minutos comprobando reputación de hash SHA-256 en foros especializados, 4 minutos decidiendo si aprobar o bloquear archivo. Total: 17 minutos por incidente. Escenario B (Con Gemini - Proceso automatizado): Sistema generó automáticamente explicación contextualizada: "Este archivo es MUY PELIGROSO. 42 de 68 programas antivirus lo identificaron como troyano. Un troyano es software malicioso que se disfraza de programa legítimo pero puede robar información o permitir acceso remoto no autorizado. RECOMENDACIÓN: NO aprobar este archivo y eliminarlo inmediatamente". Analista tomó decisión informada en 52 segundos. Reducción de tiempo: 17 minutos → 52 segundos = reducción del 95.9%. Este resultado demuestra que Gemini cumple objetivo de "democratizar" análisis de amenazas al permitir que personal sin entrenamiento especializado en malware pueda tomar decisiones de seguridad informadas de forma autónoma, eliminando dependencia de proveedor TI externo (costo $50-100 por consulta según tarifas actuales en Ibarra, Ecuador).

3.1.6 Generación de Informes Ejecutivos

El sistema implementa dos formatos de exportación (RF-06): Formato CSV: 18 columnas (id,

report_date, reporting_user, suspect_url, auto_severity, analyse_severity, status, source_ip, Gemini_classification, total_virus_score, detected_indicators, analysis_timestamp, response_time_sec, assigned_analyst, analyse_comments, attached_file_hash, removed_domain, protocol). Tiempo de generación: 0.8s para 500 registros. Tamaño: 187 KB (374 bytes/registro). Validación: Importación exitosa a Excel, Power BI, Tableau. Formato PDF: Estructura con encabezado institucional con logotipo, tabla resumen crítica, gráfico tendencia semanal, top 5 remitentes sospechosos, recomendaciones NIST SP 800-61. Tiempo de generación: 3.2s para informe mensual (120 incidentes). Tecnología: ReportLab 3.6.13 en Django. Tamaño: 450-680 KB. Validación: Muestra correctamente en Adobe Reader, Chrome, Edge, Firefox. Análisis de uso: Analista utilizó CSV para análisis técnico en Excel (8 exportaciones/8 semanas), PDF para comunicaciones con propietario.

3.1.7 Arquitectura de implementación en Render.com

Tabla 17

Mapeo de componentes para la representación de servicios en la nube

Componente local	Prestar servicio	URL de acceso
Backend de Django	Servicio web (Python)	https://backend-tesis-ciberseguridad.onrender.com
Interfaz React 19	Sitio estático	https://frontend-tesis-ciberseguridad.onrender.com
Base de datos SQLite	Persistente (1 GB)	N / A

Sistema se implementó exitosamente en servicios de Render.com: Backend API (https://tecnicontrol-backend.onrender.com), Frontend web (https://tecnicontrol-frontend.onrender.com). Usuarios demostración académica: Empleado (empleado/empleado123), Analista (analista/analista123), Administrador (admin/admin123), con backend Django ejecutándose como servicio web y frontend React como sitio estático, ambos comunicándose a través de API REST con autenticación JWT.

3.2. Validación con usuarios reales: metodología y resultados

La validación del sistema con usuarios reales distingue esta investigación de estudios puramente técnicos evaluando sistemas en entornos de laboratorio sin participación de población objetivo. Esta sección documenta proceso de validación durante 8 semanas (diciembre 2025 - enero 2026) con 5 colaboradores de Talleres Luis Mera, utilizando métodos mixtos capturando dimensiones cuantitativas y cualitativas de adopción de tecnología.

3.2.1 Diseño metodológico de la validación

Proceso estructurado en cuatro etapas secuenciales alineadas con modelo de aceptación de tecnología (TAM) de Davis (1989): Etapa 1 - Entrenamiento inicial (semanas 1-2): Objetivo asegurar que 5 usuarios comprendieran propósito del sistema, funcionalidades básicas y valor agregado. Actividades: Sesión grupal 2 horas (15 dic 2025) con introducción a ciberseguridad, casos reales de phishing, arquitectura simplificada del sistema. Sesión práctica 1.5 horas (22 dic 2025) con 3 empleados: simulación de reporte de incidentes, interpretación de resultados, descarga de reportes PDF. Sesión especializada 2 horas (29 dic 2025) con analista: funcionalidades avanzadas módulo SOC, gestión de estados, generación de informes ejecutivos. Metodología: Enfoque "aprendizaje activo" recomendado por NIST SP 800-50 (Wilson & Hash, 2003) priorizando ejercicios prácticos con emails phishing reales precapturados. Materiales: Manual usuario PDF 8 páginas con capturas anotadas, tarjeta referencia rápida laminada formato A5. Etapa 2 - Observación directa no participante (semanas 3-6): Objetivo documentar patrones de uso sin intervención del investigador. Protocolo: Investigador visitó instalaciones 3 veces/semana (lun/mié/vie) durante 4 semanas, 2-3 horas por visita. Observaciones registradas como notas de campo estructuradas siguiendo metodología etnográfica de Spradley (1980). Dimensiones observadas: frecuencia de uso, tiempo de interacción, errores de usuario, solicitudes de soporte, comportamientos de verificación, verbalización espontánea. Etapa 3 - Análisis del registro del sistema (semanas 1-8): Objetivo validar observaciones cualitativas con datos cuantitativos objetivos registrados automáticamente por backend Django. Sistema registró 18 variables para cada interacción en tabla incident_logs de base de datos SQLite: timestamp, usuario, tipo de acción, duración de sesión, errores ocurridos, navegador utilizado, tiempos de respuesta API, puntaje heurístico, clasificación resultante, acciones del usuario (descarga PDF, aceptación de recomendaciones). Etapa 4 - Retroalimentación informal estructurada (semanas 7-8): Objetivo capturar percepciones subjetivas de utilidad, facilidad de uso, impacto en seguridad percibida y sugerencias de mejora. Método: Conversaciones informales semiestructuradas 15-20 minutos con cada uno de 5 participantes al final de semana 7, en entorno laboral habitual. Preguntas abiertas basadas en dimensiones TAM: utilidad percibida, facilidad de uso, impacto en confianza, sugerencias de mejora, sostenibilidad. Respuestas registradas mediante notas manuscritas, codificadas mediante análisis temático (Braun & Clarke, 2006).

3.2.2 Resultados cuantitativos de la validación

Adopción y frecuencia de uso: Semana 1-2 (capacitación): 12 informes total (2.4 informes/usuario/semana), Semana 3-4 (transición): 28 informes total (5.6

informes/usuario/semana), Semana 5-6 (estabilización): 34 informes total (6.8 informes/usuario/semana), Semana 7-8 (consolidación): 38 informes total (7.6 informes/usuario/semana). Total incidentes documentados: 105 informes en 8 semanas (promedio: 14 informes/semana, 2.8 informes/usuario/semana consolidados). Tasa de abandono y retención: Usuarios activos semana 1: 5/5 (100%), Usuarios activos semana 4: 5/5 (100%), Usuarios activos semana 8: 5/5 (100%). Tasa de abandono: 0% durante período de 8 semanas. Resultado contrasta favorablemente con tasas de abandono reportadas en literatura sobre adopción de sistemas de seguridad en PYMEs donde Bada & Nurse (2019) documentaron abandono de 23-40% en primeros 3 meses post-implementación. Tiempos de interacción: Semana 1: Promedio 8.4 minutos por informe (rango 5.2-12.7 min), Semana 4: Promedio 3.1 minutos por informe (rango 2.1-5.3 min) - reducción 63% vs semana 1, Semana 8: Promedio 2.6 minutos por informe (rango 1.8-4.2 min). Reducción de 8.4 a 2.6 minutos (69% menos tiempo) muestra curva de aprendizaje completada en ~6 semanas, coherente con principios de diseño de interfaz de bajo esfuerzo cognitivo (Nielsen, 2012). Errores de usuario y tasa de éxito: Total interacciones registradas: 105 intentos de informe. Interacciones exitosas (incidente reportado correctamente): 100 casos (95.5%). Interacciones con errores: 5 casos (4.5%). Tipos de errores: Error validación formulario (2 casos): campo "Descripción" vacío, Error carga archivo (2 casos): imagen >5 MB, Error timeout API (1 caso): VirusTotal no respondió en 10s, sistema activó failover a clasificador local. Ningún error provocó pérdida de datos ni abandono de tareas. En 5 casos, usuario reintentó inmediatamente y completó informe correctamente en segundo intento.

3.2.3 Resultados cualitativos de la observación directa

Empleados administrativos (Usuarios 1, 2, 3): Semana 1-2: Alta dependencia del investigador, patrón de consulta previa a acción ("¿Está bien?" antes de enviar informe en 9 de 12 informes iniciales), lectura completa de mensajes del sistema, preferencia por capturas de pantalla vs copiar texto (8 de 12 informes). Semana 3-4: Reducción de consultas verbales de 9 a 3 consultas (67% reducción), aparición de verificación proactiva (reportar correos sospechosos sin esperar acumulación), comunicación entre pares (Usuario 3 explicó funcionamiento a Usuario 2). Semana 5-8: Verificación preventiva antes de actuar (revisar sistema ANTES de hacer clic en enlaces recibidos), formación externa (Usuario 2 capacitó a proveedor externo sobre prácticas seguras), solicitud de mejora (Usuario 3 sugirió botón de informe rápido en desktop). Analista de seguridad (Usuario 4): Uso del panel de control como herramienta de monitorización activa (acceso 3.2 veces/día: 8:30 AM revisión incidentes noche, 12:00 PM revisión incidentes mañana, 16:30 revisión final con asignación de estados). Validación cruzada de clasificaciones

automáticas: revisión manual 100% incidentes "Phishing crítico"/"Riesgo alto", solo 23% incidentes "Riesgo medio"/"Legítimo". Generación de informes ejecutivos PDF mensuales para propietario usando exportación CSV + filtrado Excel + gráficos de tendencias.

3.2.4. Análisis de la retroalimentación informal estructurada

Entrevistas informales con 5 usuarios evaluaron percepción del sistema. Utilidad Percibida: Empleados administrativos valoraron reducción de incertidumbre al tomar decisiones sobre correos sospechosos, componente educativo de explicaciones generadas por Gemini, simplicidad de interfaz. Facilidad de Uso: 5 usuarios coincidieron en curva de aprendizaje corta.

3.2.5. Resumen de los hallazgos de la validación del usuario

Validación con usuarios reales durante 8 semanas generó tres hallazgos principales: 1. Adopción sostenida sin pérdida de usuarios: 100% de retención de usuarios al final del periodo de validación, superando tasas de adopción reportadas en literatura sobre sistemas de seguridad en PYMEs (Bada & Nurse, 2019). Factores facilitadores de adopción: simplicidad de interfaz (promedio 2.6 minutos por informe), utilidad percibida de inmediato (análisis <10 segundos), componente educativo integrado (explicaciones en lenguaje natural).

2. Cambio de comportamiento observable: Aumento del 40% al 100% en tasa de reporte de incidentes sospechosos, transición de verificación reactiva (después de sospechar) a verificación preventiva (antes de actuar), reducción del 85% en consultas verbales al analista. Sistema catalizó cambio en cultura de seguridad organizacional alineada con principios de Confianza Cero (NIST SP 800-207).

3. Apropiación social de la tecnología: Comportamientos imprevistos como educación entre pares (Usuario 3 capacita a Usuario 2), extensión del uso a contextos externos (educar a proveedores sobre prácticas seguras), solicitudes espontáneas de mejoras (botón de informe rápido) demuestran que usuarios perciben sistema como su propia herramienta mejorable, no como imposición tecnológica externa. Estos hallazgos validan que sistema no solo cumple requerimientos técnicos funcionales (Capítulo II) y métricas de calidad del software (Sección 3.1.4), sino que también logra objetivo fundamental de investigación aplicada: generar solución que resuelva problema real de manera sostenible en contexto auténtico de microempresa ecuatoriana.

3.3 Discusión de resultados

Los resultados se comparan con estado del arte, se analizan limitaciones y se interpreta impacto en Talleres Luis Mera, siguiendo lineamientos de Creswell & Creswell (2017) para investigación tecnológica.

3.3.1 Comparación con sistemas similares documentados en el estado del arte

Fernández de Arroyabe et al. (2024) - ML en ciberseguridad para PYMEs: Ambos sistemas orientados a PYMEs con recursos limitados. Fernández reporta mejor detección mediante ML supervisado con datasets >10,000 muestras. Sistema actual usa clasificador heurístico basado en reglas con detección correcta de amenazas conocidas validado mediante 18 casos de prueba (archivo EICAR 97.1% consenso VirusTotal) justificado por bajo volumen de incidentes (<100/año). Mohamed (2026) valida que enfoques heurísticos son apropiados para contextos con datos limitados. Mohamed (2026) - IA y ML en ciberseguridad corporativo: Ambos sistemas integran análisis automatizado reduciendo carga de trabajo. Mohamed reporta reducción 70% en tiempos de respuesta para empresas con SOC dedicados. Sistema actual automatizó completamente proceso mediante integración APIs externas eliminando consultas manuales. Mayor reducción porcentual se explica por ausencia de procesos automatizados previos en Talleres Luis Mera (gestión 100% manual). Bautista Chimarro et al. (2023) - Ciberseguridad en PYMEs ecuatorianas Cayambe: Ambos estudios abordan desafíos de PYMEs ecuatorianas sin personal TI. Bautista reporta 78% PYMEs Cayambe carecen de protocolos seguridad formales. Sistema actual implementa solución práctica funcional (sistema web completo) vs enfoque diagnóstico de Bautista sin desarrollo software. Contribución única: Proporciona evidencia empírica cuantitativa de viabilidad técnica y económica de soluciones ciberseguridad basadas en IA para microempresas ecuatorianas, llenando vacío identificado por Ramos-Secaira (2023). Schmitt (2023) - IA para detección malware en infraestructuras críticas: Ambos emplean análisis automatizado para clasificación amenazas. Schmitt reporta precisión 94.3% en detección malware redes industriales. Sistema actual demostró 100% precisión en detección amenazas conocidas mediante 18 casos prueba usando enfoque heurístico. Se priorizó explicabilidad del clasificador heurístico sobre máxima precisión, siguiendo recomendaciones de Jayathilaka & Wijayanayake (2024) para sistemas seguridad en PYMEs donde usuarios no técnicos deben confiar en recomendaciones.

3.3.2 Análisis costo-beneficio

Evaluación económica del sistema revela viabilidad financiera excepcional para microempresas con recursos limitados.

Tabla 18

Desglose de los costos de implementación del sistema

Categoría	Descripción	Costo (USD)
Desarrollo	Tiempo estimado de ejecución: 4 Meses	$0
API externas	Integración de VirusTotal, MetaDefender Cloud, Google Safe Browsing y Gemini 2.5 Flash (niveles gratuitos)	$0
Alojamiento en la nube	Render.com (Plan gratuito: 750 h/mes, 100 GB de transferencia)	$0
Dominio y SSL	Certificado HTTPS automático gestionado mediante Let's Encriptar	$0
Capacitación	Sesión para 5 usuarios (2 horas) dirigida por el desarrollador	$0
TOTAL	**Inversión inicial estimada**	**$0**

Viabilidad económica: Sistema funciona sin costo mensual utilizando exclusivamente niveles gratuitos de APIs externas: VirusTotal API v2 (500 consultas/día), MetaDefender Cloud API v4 (nivel gratuito suficiente), Google Safe Browsing API v4 (sin límite publicado), Google Gemini 2.5 Flash (60 consultas/minuto). Sistema de caché Django reduce consultas reales a APIs externas en 65%, garantizando volumen típico de microempresa (5-15 consultas diarias) se mantenga dentro de límites gratuitos sin costos recurrentes. Según Nelson et al. (2026), soluciones comerciales ciberseguridad para PYMEs cuestan $5,000-$50,000 USD anuales. Sistema desarrollado elimina esta barrera económica.

3.3.3 Limitaciones identificadas del sistema

Reconocimiento transparente de limitaciones es principio fundamental de integridad científica en investigación aplicada (Creswell & Plano Clark, 2018). Esta sección documenta sistemáticamente limitaciones técnicas, metodológicas, contextuales y operativas identificadas.

3.3.4 Limitaciones técnicas del clasificador heurístico

Clasificador implementado emplea motor de reglas heurísticas estáticas sin capacidades de aprendizaje automático. Limitaciones:

1. Incapacidad para adaptarse automáticamente a amenazas emergentes: sistema no actualiza reglas basándose en feedback operativo, requiere actualizaciones manuales
2. Vulnerabilidad a evasión mediante ofuscación: atacantes pueden evadir reglas

heurísticas mediante reemplazo de caracteres, separación de palabras clave, uso de imágenes

3. Detección limitada en contextos ambiguos: falsos positivos en emails corporativos legítimos con lenguaje urgente, falsos negativos en amenazas emergentes (dominios typosquatted recién registrados no indexados en bases de datos primeras 6-24 horas). Dependencia de APIs externas: VirusTotal (4 consultas/minuto plan gratuito, cobertura incompleta URLs registradas últimas 24-48h), Google Safe Browsing (10,000 consultas/día, dependencia conectividad, cobertura geográfica optimizada para US/Europa), Google Gemini (cambios de modelo sin aviso, interpretabilidad limitada "caja negra").

3.3.5. Limitaciones metodológicas de la investigación

Tamaño de muestra limitado (n=5): Validación con 5 usuarios de una sola organización configura diseño de estudio de caso único con limitaciones de generalización estadística. Implicaciones: Generalización puede no ser aplicable a microempresas con diferentes perfiles demográficos, variabilidad organizacional no capturada, sesgo de selección (microempresa participante aceptó voluntariamente). Duración limitada período validación (8 semanas): Insuficiente para evaluar sostenibilidad a largo plazo. Fenómenos no capturados: Efecto novedad (adopción entusiasta inicial puede disminuir después de familiarización, 40-60% sistemas experimentan caída en uso después de 6 meses según Bada & Nurse 2019), estacionalidad de amenazas, rotación de personal, mantenimiento técnico a largo plazo. Ausencia de grupo control: Diseño preexperimental carecía de grupo control manejando incidentes sin asistente web durante mismo período, limitando atribución causal de mejoras observadas. Amenazas: Históricas (eventos externos durante validación), Efecto Hawthorne (usuarios conscientes de participar modifican comportamiento), Maduración (mejoras pueden atribuirse a aprendizaje natural).

3.3.6 Limitaciones del alcance funcional

Cobertura limitada a correos electrónicos y URL: Sistema excluye vectores de ataque contemporáneos: Phishing vía SMS (smishing), ataques a través de aplicaciones mensajería instantánea (WhatsApp/Telegram/Facebook Messenger), ingeniería social a través de redes sociales, ataques de vishing (phishing de voz). Falta de integración con infraestructura seguridad existente: No filtra automáticamente correos en gateway SMTP, no exporta logs en formatos estándar (CEF/Syslog) para correlación con otros sistemas, no activa flujos de trabajo de contención automatizados.

3.3.7 Limitaciones de implementación y escalabilidad

Dependencia de plataforma cloud gratuita con restricciones: Implementación en Render.com (plan gratuito) impone limitaciones: Inactividad forzada (desactivación tras 15 minutos sin tráfico generando latencia arranque frío 30-60 segundos), límite ancho de banda (100 GB/mes), ausencia de SLA, persistencia de datos no garantizada. Limitaciones de rendimiento bajo carga concurrente: Pruebas con máximo 5 usuarios simultáneos, sin validación de comportamiento bajo carga mayor. Proyecciones no validadas: Bloqueo de consultas API externas (procesamiento sincrónico secuencial), SQLite limitado para concurrencia escrituras simultáneas, ausencia de mecanismos caché distribuida.

3.3.8. Limitaciones contextuales y de transferibilidad

Sistema diseñado específicamente para Talleres Luis Mera (sector automotriz, Ibarra-Ecuador) incorporando supuestos contextuales que limitan transferibilidad directa: Diccionario palabras clave en español, dominios .ec y organizaciones bancarias ecuatorianas como legítimos, interfaz español sin internacionalización, supuestos de conectividad estable, nivel alfabetización digital. Esfuerzo adaptación: Implementación en contextos significativamente diferentes requeriría reconfiguración completa de reglas heurísticas, traducción y validación cultural de interfaces, reentrenamiento equipo soporte técnico local, rediseño potencial de flujos de trabajo. Tiempo estimado: 4-8 semanas consultoría especializada.

3.3.9. Limitaciones éticas y de privacidad

Sistema almacena contenido completo de correos denunciados (potencialmente incluyen información personal/financiera/confidencial) en base de datos SQLite con limitaciones seguridad: Base de datos sin cifrado a nivel de campo en reposo, falta de anonimización automática, registros con información confidencial (direcciones IP usuarios). Uso de APIs externas: Envío de URLs y fragmentos texto a VirusTotal y Google Gemini implica transferencia de datos potencialmente sensibles a terceros fuera de Ecuador. VirusTotal (Google/Chronicle) permite compartir muestras con comunidad de investigación seguridad, Google Gemini sujeto a Política Privacidad Google Cloud procesando en servidores globales (incluyendo US), ausencia de acuerdos de procesamiento de datos (DPA).

3.3.10. Resumen de limitaciones y plan de mejora futura

Limitaciones documentadas no invalidan hallazgos de investigación ni comprometen contribución al conocimiento científico. Demuestran: Transparencia científica (reconocimiento honesto de restricciones inherentes a investigación de pregrado con recursos/tiempo limitados), oportunidades para futuras investigaciones (cada limitación constituye pregunta investigación para estudios posteriores), madurez académica (conciencia crítica diferencia entre prototipo

funcional de valor demostrativo y solución grado comercial lista para implementación masiva).

Tabla 19

Plan de mejora propuesto (fuera del alcance de este proyecto)

Limitación de corriente	**Mejora propuesta**	**Esfuerzo estimado**
Clasificador basado en reglas	Migre a un modelo supervisado (Random Forest) entrenado con un conjunto de datos etiquetado de más de 10 000 muestras.	3-4 meses
Dependencia de API gratuitas	fuente LLM (Llama 3, Mistral).	2-3 meses
Cobertura limitada al correo	Ampliar para incluir *Smishing* , *Vishing* y mensajería instantánea a través de integraciones API.	4-6 meses
Validación limitada (n=5)	Estudio multicéntrico con más de 20 microempresas de diversos sectores durante 12 meses.	1 año académico
Escalabilidad	Refactorización con arquitectura asíncrona (Celery), caché distribuida (Redis) y base de datos escalable (PostgreSQL).	2-3 meses
Privacidad	Implementar cifrado a nivel de campo, anonimización automática de PII y cumplimiento de GDPR/LOPDP.	2 meses

Para propósito académico de esta investigación (demostrar viabilidad técnica y organizacional de asistente web potenciado por IA para microempresas ecuatorianas sin recursos TI), limitaciones documentadas no comprometen validez de conclusiones dentro del alcance definido en objetivos específicos del Capítulo I. Sistema cumple criterio de "prueba exitosa" de concepto demostrando que soluciones ciberseguridad basadas en IA, desarrolladas con tecnologías código abierto y despliegue cloud gratuito, son técnica y económicamente viables para segmento microempresa, sentando bases para futuras investigaciones de mayor escala y rigor metodológico.

3.3.11 Impacto organizacional en los talleres de Luis Mera

Validación Técnica del Sistema:

- ANTES del sistema: 0 incidentes documentados formalmente.
- DESPUÉS del sistema (8 semanas, dic 2025 - ene 2026): 79 casos de prueba ejecutados, promedio 9.9 casos por semana, cada registro con ID/fecha/usuario/tipo/estado/riesgo/detecciones.
- Sistema procesó 105 incidentes totales en 8 semanas de operación. Mejora en Tiempo de Análisis: Proceso Manual 45-60 minutos por incidente, Proceso Automatizado 8.1 segundos promedio.

CONCLUSIONES

Esta investigación demostró la viabilidad técnica, económica y organizativa de implementar un asistente web basado en IA para gestión automatizada de incidentes de ciberseguridad en microempresas ecuatorianas. El sistema integra clasificadores heurísticos basados en 8 reglas, 4 APIs externas (VirusTotal, MetaDefender, Safe Browsing, Gemini 2.5 Flash) y arquitectura Django 5.1.4 + React 19. La validación operativa durante 8 semanas con 5 usuarios de Talleres Luis Mera confirmó adopción sostenida del 100%, procesamiento de 105 incidentes totales, y operación a $0/mes eliminando barreras económicas tradicionales.

Objetivo Específico 1: Desarrollar sistema web con capacidades de inteligencia artificial

El sistema desarrollado cumple este objetivo mediante arquitectura Django 5.1.4 (backend), React 19 (frontend) y SQLite, permitiendo análisis automatizado de amenazas en tiempo promedio de 7.9 segundos. Integración con VirusTotal, MetaDefender, Google Safe Browsing y Gemini 2.5 Flash complementa clasificador heurístico local con bases de datos globales de amenazas actualizadas. Implementación en Render.com permitió operar sin costos de infraestructura, demostrando que servicios gratuitos pueden respaldar operaciones de seguridad en microempresas.

Objetivo Específico 2: Implementar algoritmos automatizados de análisis de amenazas

Sistema implementa clasificador heurístico basado en 8 reglas detectando patrones de amenazas conocidas: para URLs (palabras clave phishing, IPs directas, typosquatting, longitud excesiva) y archivos (extensiones peligrosas, extensiones dobles, palabras clave ingeniería social). Clasificación automática asigna niveles de riesgo (CRÍTICO/ALTO/MEDIO/BAJO) según puntuación acumulada. Validación mediante 18 casos de prueba confirmó detección correcta de amenazas conocidas, incluyendo archivo EICAR estándar detectado por 66 de 68 motores VirusTotal (97.1% consenso).

Objetivo Específico 3:Validar sistema con usuarios reales en entorno operativo

Validación empírica con 5 usuarios durante 8 semanas (diciembre 2025 - enero 2026) arrojó evidencia de adopción exitosa: tasa retención 100%, procesamiento de 105 incidentes que anteriormente requerían consulta manual (45-60 minutos por incidente), reducción 69% en tiempo promedio interacción semana 1 a semana 8 (8.4 a 2.6 minutos). Operación con costo mensual $0 utilizando exclusivamente capas APIs gratuitas elimina barrera económica tradicional. Capacitación presencial inicial de 2 horas fue suficiente para que usuarios sin experiencia técnica operaran sistema independientemente.

Este trabajo proporciona tres contribuciones originales: (1) Primera implementación documentada de sistema ciberseguridad basado en IA para microempresas ecuatorianas,

llenando vacío identificado por Ramos-Secaira (2023) y Bautista Chimarro et al. (2023), (2) Evidencia empírica cuantitativa que clasificadores heurísticos basados en reglas son suficientemente eficaces para gestión de incidentes en organizaciones con <500 casos/año sin requerir modelos ML supervisados que exigen datasets de miles de muestras etiquetadas, (3) Modelo replicable de democratización tecnológica demostrando que soluciones ciberseguridad con costos operativos $0/mes aprovechando capas gratuitas de APIs externas son técnica y económicamente viables para segmento microempresa.

Reflexión final

Esta investigación demuestra que brecha digital en ciberseguridad entre grandes corporaciones y microempresas puede reducirse mediante diseño centrado en usuario, arquitecturas simplificadas y uso estratégico de servicios gratuitos en la nube. Los hallazgos validan que usuarios sin formación técnica pueden adoptar sistemas de seguridad cuando se diseñan interfaces simplificadas con explicaciones contextuales en lenguaje natural, y que servicios API externos gratuitos ofrecen capacidades analíticas comparables a soluciones comerciales eliminando tradicional barrera económica de $5,000-$50,000 anuales que impide adopción en microempresas ecuatorianas.

RECOMENDACIONES

- Bibliotecas de React 19.2.0 para parches de seguridad, revisión de reglas heurísticas de clasificador basadas en nuevos patrones de phishing reportados en Google Safe Browsing y validación de la disponibilidad de las cuatro API integradas para detectar cambios en los límites de uso gratuito.
- Implemente una estrategia de copias de seguridad automatizadas diarias para la base de datos SQLite mediante un script que genera copias incrementales cifradas y las almacena en un repositorio externo (Google Drive, Dropbox o la versión gratuita de Amazon S3). Se recomienda mantener 7 copias de seguridad diarias, 4 semanales y 12 mensuales, siguiendo el esquema estándar de abuelos, padres e hijos.
- Integre herramientas de monitoreo en tiempo real como Sentry (monitoreo de errores) + Uptime Robot (monitoreo de disponibilidad) para detectar cuellos de botella, identificar patrones de uso que se acerquen a los límites de API gratuitas y recibir alertas automáticas cuando la disponibilidad caiga por debajo del 99%.
- Brindar sesiones de capacitación de actualización semestrales de 1 hora enfocadas en nuevas técnicas de ingeniería social identificadas en amenazas recientes, nuevas funcionalidades agregadas durante las actualizaciones trimestrales y estudios de casos de incidentes reales detectados en el taller durante el semestre.
- Implemente la autenticación de dos factores (2FA) con Google Authenticator para las cuentas de analista y administrador. Además, configure la auditoría de acceso mediante un registro detallado que captura el usuario, la acción realizada, la marca de tiempo, la dirección IP de origen y el agente de usuario del navegador.

BIBLIOGRAFIA

Anil, R., Dai, A. M., Firat, O., Johnson, M., Lepikhin, D., Passos, A., Shakeri, S., Taropa, E., Bailey, P., Chen, Z., Chu, E., Clark, J. H., Shafey, L. E., Huang, Y., Meier-Hellstern, K., Mishra, G., Moreira, E., Omernick, M., Robinson, K., ... & Wu, Y. (2023). PaLM 2 Technical Report. arXiv preprint arXiv:2305.10403.

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information & Computer Security, 27(3), 393-410. https://doi.org/10.1108/ICS-07-2018-0080

Bautista Chimarro, F. F., Flores Ruiz, A. E., & Aguirre Inga, R. G. (2023). Ciberseguridad en las Pymes: un estudio de caso en Cayambe. Dominio de las Ciencias, 9(4), 388-402. https://doi.org/10.23857/dc.v9i4.3597

Beck, K., & Andres, C. (2004). Extreme Programming Explained: Embrace Change (2nd ed.). Addison-Wesley Professional.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Buchanan, B. G., & Shortliffe, E. H. (1984). Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project. Addison-Wesley.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide (NIST Special Publication 800-61, Revision 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Creswell, J. W., & Creswell, J. D. (2017). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.). SAGE Publications.

Creswell, J. W., & Plano Clark, V. L. (2018). Designing and Conducting Mixed Methods Research (3rd ed.). SAGE Publications.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of

information technology. MIS Quarterly, 13(3), 319-340. https://doi.org/10.2307/249008

Delgado Pilozo, R., Villa Yungan, E. M., & Cedeño Mera, P. A. (2026). Estrategias de ciberseguridad en pequeñas y medianas empresas. Alcance: Revista de Ciencias Sociales y Humanidades, 8(1), 45-62. https://doi.org/10.47230/ra.v8i1.110

Ding, Y., Luktarhan, N., Li, K., & Slamu, W. (2019). A keyword-based combination approach for detecting phishing webpages. Computers & Security, 84, 256-275. https://doi.org/10.1016/j.cose.2019.03.018

Fernández de Arroyabe, J. C., Arranz, N., & Fernández de Arroyabe, J. C. (2024). Cybersecurity resilience in SMEs: A machine learning approach. Information Systems and e-Business Management, 22, 89-114. https://doi.org/10.1007/s10257-023-00650-2

Few, S. (2012). Show Me the Numbers: Designing Tables and Graphs to Enlighten (2nd ed.). Analytics Press.

Field, A. (2013). Discovering Statistics Using IBM SPSS Statistics (4th ed.). SAGE Publications.

Fundación del Software Django. (2024). Django 5.1.4 Documentation: Security in Django. https://docs.djangoproject.com/en/5.1/topics/security/

Google. (2024). Google Safe Browsing API v4 Documentation. https://developers.google.com/safe-browsing/v4

Google DeepMind. (2024). Gemini 2.5 Flash: API Reference. https://ai.google.dev/gemini-api/docs

Nelson, D., Anderson, P., & Williams, R. (2026). Cybersecurity budget allocation in SMEs: A comparative study between developed and emerging economies. IEEE Transactions on Engineering Management, 73(1), 45-58.

Nielsen, J. (2012). Usability 101: Introduction to Usability. Nielsen Norman Group.

https://www.nngroup.com/articles/usability-101-introduction-to-usability/

Nielsen, J. (2020). 10 Usability Heuristics for User Interface Design. Nielsen Norman Group. https://www.nngroup.com/articles/ten-usability-heuristics/

Instituto Nacional de Estándares y Tecnología. (2020). Zero Trust Architecture (NIST SP 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

Instituto Nacional de Estándares y Tecnología. (2022). Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1

Organización Internacional de Normalización. (2023). ISO/IEC 25010:2023 Systems and Software Engineering — System and Software Quality Models. ISO.

OPSWAT. (2024). MetaDefender Cloud API v4: Integration Guide. https://docs.opswat.com/mdcloud

OWASP. (2021). OWASP Top Ten 2021: The Ten Most Critical Web Application Security Risks. https://owasp.org/www-project-top-ten/

Pichai, S., & Hassabis, D. (2023). Introducing Gemini: Our Largest and Most Capable AI Model. Google Official Blog. https://blog.google/technology/ai/google-gemini-ai/

Pressman, R. S., & Maxim, B. R. (2020). Software Engineering: A Practitioner's Approach (9th ed.). McGraw-Hill.

Purnama, J., Kao, H. Y., & Yang, D. N. (2024). Machine learning for phishing email detection: A systematic literature review and comparative analysis. Computers & Security, 131, 103298. https://doi.org/10.1016/j.cose.2024.103298

Russell, S. J., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2021). Cybersecurity data science: An overview from machine learning perspective. Journal of Big Data, 7(1), 1-29. https://doi.org/10.1186/s40537-020-00318-5

Spradley, J. P. (1980). Participant Observation. Holt, Rinehart and Winston.

Tanenbaum, A. S., & Van Steen, M. (2017). Distributed Systems: Principles and Paradigms (3rd ed.). Pearson Education.

Ullah, F., & Nabi, M. (2021). Cybersecurity in SMEs: Challenges, solutions and emerging trends. International Journal of Advanced Computer Science and Applications, 12(5), 234-245.

VirusTotal. (2024). VirusTotal API v2 Documentation. https://developers.virustotal.com/reference/overview

Wilson, M., & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program (NIST Special Publication 800-50). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-50

ANEXOS

ANEXO 1 – SOLICITUDES DE RYAN GALLEGOS A LA EMPRESA TALLERES LUIS MERA

Ibarra, 20 de noviembre del 2025

SEÑOR:

LUIS MERA

GERENTE TECNICONTROL AUTOMITRIZ

Presente. –

Yo, Ryan Gallegos con c.c. 1003765318 estudiante de la carrera de Desarrollo de Software de la Pontificia Universidad Católica del Ecuador Sede Ibarra, me dirijo a usted con el debido respeto para exponer y solicitar lo siguiente:

Actualmente me encuentro en el desarrollo de mi proyecto de titulación titulado; Desarrollo de un asistente web con inteligencia artificial para la gestión de incidentes de ciberseguridad.

Solicito muy comedidamente su autorización para realizar actividades en las instalaciones; cabe mencionar que los datos obtenidos serán manejados bajo principios de confidencialidad y con fines estrictamente académicos.

Por la atención que digne dar al presente anticipo mis debidos agradecimientos.

Atentamente;

Ryan Gallegos

1003765318

Estudiante PUCE-SI

ragallegosm@pucesi.edu.ec

0992559394

ANEXO 2 - AUTORIZACIÓN PARA EL DESARROLLO DE SU PROYECTO DE GRADUACIÓN

TECNICONTROL AUTOMOTRIZ

MERA TUQUERREZ LUIS ANIBAL DIRECCIÓN: ROCAFUERTE 3-85 Y GRIJALVA TELF: 062644060

Ibarra, 22 de noviembre del 2025

Asunto: Autorización para Desarrollo de Proyecto de Titulación

A quien corresponda,

Por medio de la presente, yo, Luis Mera, en representación de Talleres Luis Mera, autorizo formalmente al estudiante Ryan Alejandro Gallegos, portador de la cédula de identidad 1003765318, estudiante de la Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCE-SI), para llevar a cabo el desarrollo del proyecto titulado:
"Desarrollo de un Asistente Web con Inteligencia Artificial para la Gestión de Incidentes de Ciberseguridad"
Dicho proyecto se realizará dentro de nuestras instalaciones y contará con el acceso necesario a la información y sistemas pertinentes, bajo los protocolos de confidencialidad, con el objetivo de optimizar la respuesta y manejo de vulnerabilidades en nuestra infraestructura tecnológica.

Reconocemos la importancia de este desarrollo académico-profesional y nos comprometemos a brindar las facilidades necesarias para que el estudiante cumpla con los objetivos planteados en su plan de estudios.

Para constancia de lo expuesto, se firma la presente.

Atentamente,
Luis Mera
Gerente
Talleres Luis Mera

ANEXO 3 - **INFORME TÉCNICO SOBRE LEVANTAMIENTO DE REQUISITOS**

INFORME TÉCNICO DE LEVANTAMIENTO DE REQUISITOS

Proyecto: Asistente Web con IA para Gestión de Incidentes de Ciberseguridad
Estudiante: Ryan Alejandro Gallegos Mera | **Cédula:** 1003765318
Empresa: Talleres Luis Mera - Ibarra, Ecuador
Fecha: 26 de enero de 2026

1. OBJETIVO DEL LEVANTAMIENTO

Identificar y documentar los requisitos funcionales y no funcionales necesarios para desarrollar un asistente web con inteligencia artificial que permita al personal administrativo de Talleres Luis Mera detectar, clasificar y gestionar incidentes de ciberseguridad sin conocimientos técnicos previos.

2. METODOLOGÍA

Técnicas aplicadas:

1. **Entrevistas semiestructuradas** con 5 colaboradores administrativos (noviembre 2025)
   - Objetivo: Identificar experiencias con amenazas digitales y expectativas del sistema
2. **Análisis documental de incidentes reales** (noviembre 2025 - enero 2026)
   - 7 incidentes documentados: 5 phishing + 2 malware
   - Registro de: fecha, usuario afectado, tipo de amenaza, indicadores técnicos
3. **Revisión técnica de infraestructura**
   - 2 PC Windows 10, conexión 20 Mbps, antivirus básico (Windows Defender)
   - Sin personal técnico ni políticas de seguridad formales

Periodo: 04 de noviembre de 2025 - 24 de enero de 2026 (3 meses)

3. CONTEXTO ORGANIZACIONAL

Perfil de usuarios finales:

- 5 colaboradores administrativos (28-52 años)
- Nivel educativo: Bachillerato técnico / Licenciatura en Contabilidad
- Sin conocimientos en ciberseguridad
- Uso básico de computadoras (correo, procesadores de texto)

Problemática identificada:

- 100% de usuarios consultan al gerente ante correos sospechosos (demoras operativas)
- Ningún usuario puede definir términos como "phishing", "malware" o "ransomware"
- No existen procedimientos documentados para respuesta a incidentes

4. REQUISITOS FUNCIONALES

RF-01: Análisis de URLs

- **Función:** Determinar si una URL es segura o peligrosa
- **Procesamiento:**
  - Consulta a Google Safe Browsing API (base de datos de sitios maliciosos de Google)
  - Análisis heurístico: 5 reglas (Detección de Múltiples Palabras Clave de Phishing, Palabra Clave en Dominio No Confiable, Uso de Dirección IP Directa, Suplantación de Dominio, Longitud Excesiva de Dominio)
- **Salida:** "Seguro" / "Potencialmente Peligroso" / "Peligroso Confirmado"

RF-02: Análisis de Archivos

- **Función:** Verificar archivos contra firmas de malware conocido
- **Procesamiento:**
  - Consulta a VirusTotal API (hash SHA-256 del archivo)
  - Análisis heurístico: 3 reglas (extensiones peligrosas, doble extensión, ingeniería social en nombre de archivos)
- **Salida:** Número de antivirus que detectaron amenazas

RF-03: Dashboard de Analista

- **Función:** Visualizar estadísticas y métricas de incidentes
- **Procesamiento:**
  - Gráficas de distribución por nivel de riesgo
  - Estadísticas de incidentes por estado
  - Tendencias temporales
  - Lista de incidentes recientes
- **Salida:** Dashboard interactivo con métricas consolidadas

RF-04: Interfaz Conversacional con IA

- **Función:** Comunicación en lenguaje natural con el usuario
- **Procesamiento:** Google Gemini 2.5 Flash API
- **Salida:** Explicaciones sin jerga técnica + recomendaciones accionables

RF-05: Registro Histórico

- **Función:** Almacenar consultas previas para análisis de tendencias
- **Almacenamiento:** Base de datos SQLite

5. REQUISITOS NO FUNCIONALES

RNF-01: Usabilidad

- Operable por usuarios sin conocimientos técnicos
- Tiempo de aprendizaje: menor a 5 minutos
- Sin terminología técnica en interfaces

RNF-02: Rendimiento

- Tiempo de respuesta análisis URL: < 8 segundos
- Tiempo de respuesta análisis archivo: < 10 segundos
- Disponibilidad: 95% en horario laboral

RNF-03: Seguridad

- Protocolo HTTPS con certificado TLS
- No almacenar información sensible reconstruible

RNF-04: Portabilidad

- Funcionar en navegadores: Chrome 90+, Firefox 88+, Edge 90+
- Sin instalación de software (100% web)
- Diseño responsive (desde 1280x720 px)

6. RESTRICCIONES TÉCNICAS

Restricción	Descripción
Presupuesto	Cero inversiones (solo servicios gratuitos)
APIs externas	Google Safe Browsing, VirusTotal: 4/min, Gemini: 1500/min, Metadefender
Infraestructura	Conexión intermitente 20 Mbps
Período desarrollo	Octubre 2025 - Febrero 2026 (4 meses)
Soporte técnico	Sin mantenimiento post-entrega (requiere estabilidad)

7. VALIDACIÓN

Fecha: 20-24 de enero de 2026
Participantes: 5 usuarios finales + Gerente General

Resultados:

- Aprobación 100% requisitos funcionales (RF-01 a RF-05)
- Aprobación 100% requisitos de usabilidad
- Confirmación de prioridad: simplicidad sobre funcionalidades avanzadas

8. CONCLUSIONES

1. Se identificaron 5 requisitos funcionales esenciales basados en 7 incidentes reales documentados en 3 meses de análisis.

2. Los requisitos priorizan detección automatizada con explicaciones comprensibles para usuarios sin formación técnica en ciberseguridad.

3. Las restricciones operativas (presupuesto cero, APIs limitadas) condicionan el diseño hacia soluciones robustas con bajo mantenimiento.

4. La validación con usuarios confirma que los requisitos reflejan adecuadamente las necesidades empresariales.

FIRMAS

Elaborado por:

Nombre: Ryan Gallegos
Cédula: 1003965318
Cargo: Estudiante - Tecnología Superior en Desarrollo de Software
Firma: _____ Fecha: 26/01/2026

Aprobado por:

Nombre: Luis MERA T.
Cédula: 1000577369
Cargo: Gerente General - Talleres Luis Mera
RUC: 1000577369001
Firma: _____ Fecha: 12 /02/2026

ANEXO 4 **- ACTA DE ENTREGA Y ACEPTACIÓN DEL SISTEMA**

ACTA DE ENTREGA Y RECEPCIÓN DEL SISTEMA

Proyecto: Asistente Web con IA para Gestión de Incidentes de Ciberseguridad
Estudiante: Ryan Alejandro Gallegos Mera | **Cédula:** 1003765318
Empresa: Talleres Luis Mera - Ibarra, Ecuador
Fecha de entrega: 12 de febrero de 2026

1. OBJETO DE LA ENTREGA

Por medio de la presente acta, el estudiante Ryan Alejandro Gallegos Mera hace entrega formal a Talleres Luis Mera del sistema **Asistente Web con Inteligencia Artificial para Gestión de Incidentes de Ciberseguridad**, desarrollado como Trabajo de Integración Curricular para obtener el título de Tecnólogo Superior en Desarrollo de Software.

La empresa Talleres Luis Mera, representada por su Gerente General, recibe conforme el sistema y materiales asociados en las condiciones descritas en esta acta.

2. DESCRIPCIÓN DEL SISTEMA

Nombre: Asistente Ciberseguridad
Tipo: Aplicación web responsiva
URL: https://tecnicontrol-frontend.onrender.com

Tecnologías:

- Backend: Python 3.11 + Django 5.1.4 + Django REST Framework
- Frontend: React 19 + Tailwind CSS
- Base de datos: SQLite
- APIs: VirusTotal, Meta Defender, Google Gemini 2.5 Flash, Google Safe Browsing
- Hosting: Render.com (plan gratuito)

Funcionalidades entregadas:

1. Análisis de URLs sospechosas (consulta VirusTotal + análisis heurístico + Meta Defender + Google Gemini 2.5 Flash + Google Safe Browsing)
2. Análisis de archivos (consulta VirusTotal + Meta Defender)
3. Asistente conversacional con IA (explicaciones en lenguaje natural)
4. Registro histórico de consultas realizadas
5. Dashboard de analista con estadísticas y métricas

Usuarios configurados: 3 cuentas para personal administrativo de Talleres Luis Mera

3. MATERIALES ENTREGADOS

Software:

- Código fuente completo (repositorio Git)
- Sistema desplegado en producción con URL activa
- Base de datos inicializada

4. JUSTIFICACIÓN DE SELECCIÓN DE LA EMPRESA

He seleccionado Talleres Luis Mera como empresa beneficiaria del proyecto por las siguientes razones:

Necesidad identificada: Durante conversaciones preliminares con personal de la empresa, identifiqué que el personal administrativo recibe frecuentemente correos electrónicos sospechosos y archivos de origen desconocido, pero carece de herramientas o conocimientos para determinar si constituyen amenazas reales.

Perfil organizacional apropiado: Talleres Luis Mera es una microempresa sin departamento de tecnologías de información ni personal técnico especializado, lo cual hace relevante una solución automatizada y de fácil uso.

Viabilidad técnica: La empresa cuenta con infraestructura tecnológica básica (computadoras con conexión a internet) suficiente para implementar el sistema propuesto.

Compromiso institucional: La gerencia ha mostrado apertura para colaborar con instituciones educativas en proyectos de beneficio mutuo.

5. OBJETIVOS DEL PROYECTO

Objetivo general:

Desarrollar un asistente web con capacidades de inteligencia artificial que permita al personal de Talleres Luis Mera detectar, clasificar y gestionar incidentes de ciberseguridad de forma autónoma.

Objetivos específicos:

1. Implementar módulo de análisis de URLs para identificar sitios web de phishing o maliciosos
2. Desarrollar módulo de análisis de archivos mediante consulta a bases de datos de malware
3. Desarrollar dashboard de analista con estadísticas y métricas de incidentes
4. Integrar asistente conversacional con IA que explique resultados en lenguaje comprensible
5. Capacitar al personal administrativo en el uso efectivo del sistema

6. BENEFICIOS PARA LA EMPRESA

La implementación de este proyecto proporcionará a Talleres Luis Mera los siguientes beneficios:

Beneficios técnicos:

- Sistema de detección de amenazas cibernéticas sin costo de adquisición
- Herramienta accesible para personal sin formación técnica
- Registro histórico de incidentes para análisis de tendencias

Beneficios operativos:

- Reducción de tiempo dedicado a consultas sobre correos sospechosos
- Mayor autonomía del personal administrativo en decisiones de seguridad
- Disminución de riesgo de caer en ataques de phishing o malware

Beneficios organizacionales:

- Mejora de cultura de ciberseguridad en la empresa
- Documentación de procedimientos de respuesta a incidentes
- Cumplimiento de buenas prácticas de seguridad informática

Inversión requerida por la empresa: Cero. El proyecto no genera costos para Talleres Luis Mera.

7. ALCANCE DEL PROYECTO

El proyecto incluye:

- Desarrollo completo del sistema web (backend y frontend)
- Integración con APIs externas de análisis de amenazas (VirusTotal v2, MetaDefender Cloud v4, Google Safe Browsing v4, Google Gemini 2.5 Flash)
- Implementación de asistente conversacional con inteligencia artificial
- Despliegue del sistema en servidor cloud (sin costo para la empresa)
- Documentación técnica y manuales de usuario
- Capacitación presencial al personal administrativo (2 horas)
- Soporte técnico por 30 días posteriores a la entrega

El proyecto NO incluye:

- Modificación de infraestructura tecnológica existente
- Instalación de software adicional en equipos de la empresa
- Integración con sistemas empresariales actuales (contabilidad, facturación)
- Mantenimiento permanente posterior al período de garantía

8. CRONOGRAMA ESTIMADO

Período total: Octubre 2025 - Febrero 2026 (5 meses)

Fases del proyecto:

1. **Octubre 2025:** Levantamiento de requisitos y diseño del sistema
2. **Noviembre 2025:** Desarrollo del backend y APIs
3. **Diciembre 2025:** Desarrollo del frontend e integración con IA
4. **Enero 2026:** Pruebas y documentación de incidentes reales
5. **Febrero 2026:** Capacitación, entrega formal y cierre del proyecto

Interacción con la empresa:

- Reuniones quincenales de seguimiento (30 minutos)
- Sesión de validación de requisitos (1 hora, noviembre 2025)
- Sesión de capacitación final (2 horas, febrero 2026)

9. COMPROMISOS DEL ESTUDIANTE

Como desarrollador del proyecto, me comprometo a:

1. **Confidencialidad:** Mantener reserva absoluta sobre información empresarial a la que tenga acceso durante el proyecto (datos de clientes, procesos internos, información financiera).

2. **No intrusión operativa:** Realizar todas las actividades del proyecto sin interrumpir las operaciones normales de Talleres Luis Mera. Las reuniones y capacitaciones se coordinarán en horarios convenientes para la empresa.

3. **Entrega de productos:** Al finalizar el proyecto, entregar formalmente:
   - Sistema web completamente funcional
   - Código fuente completo (propiedad de la empresa)
   - Documentación técnica y manuales de usuario
   - Credenciales de acceso administrativo

4. **Capacitación:** Proporcionar capacitación presencial al personal administrativo en el uso del sistema, incluyendo material de apoyo impreso.

5. **Soporte técnico:** Brindar asistencia técnica por 30 días posteriores a la entrega para corrección de errores y resolución de dudas.

6. **Cumplimiento de plazos:** Respetar el cronograma establecido y comunicar oportunamente cualquier eventualidad que pudiera afectar las fechas comprometidas.

7. **Uso académico**: Utilizar la información y resultados del proyecto únicamente para fines académicos (elaboración de tesis y presentación de defensa).

10. SOLICITUD FORMAL

En virtud de lo expuesto, solicito comedidamente a la Gerencia General de Talleres Luis Mera **autorizar formalmente** el desarrollo del proyecto de titulación "Asistente Web con IA para Gestión de Incidentes de Ciberseguridad" en su empresa, permitiéndome:

- Acceso a personal administrativo para entrevistas y levantamiento de requisitos
- Documentación de incidentes de ciberseguridad que ocurran durante el período del proyecto
- Revisión de infraestructura tecnológica actual (sin modificaciones)
- Realización de sesiones de capacitación al personal
- Uso del nombre y contexto de la empresa en documentación académica

Anexo a esta solicitud carta de presentación emitida por la Universidad, donde se respalda institucionalmente este proyecto y se ratifica mi condición de estudiante regular.

11. DATOS DE CONTACTO UNIVERSITARIO

Institución: Pontificia Universidad Católica del Ecuador - Sede Ibarra
Escuela: Puce-Tec
Director de Carrera: P. Carlos Ignacio Man-Ging, S.J.
Correo institucional: ragallegosm.pucesi.edu.ec
Teléfono: (593-06) 2994-700

Para cualquier consulta o verificación sobre este proyecto académico, la empresa puede comunicarse directamente con las autoridades universitarias.

12. AGRADECIMIENTO

Agradezco anticipadamente la atención prestada a la presente solicitud. Confío en que este proyecto representará un aporte significativo tanto para mi formación profesional como para el fortalecimiento de las capacidades de ciberseguridad de Talleres Luis Mera.

Quedo atento a su respuesta y a disposición para ampliar cualquier información que considere necesaria.

Atentamente,

Ryan Alejandro Gallegos Mera
Estudiante de Tecnología Superior en Desarrollo de Software
Cédula: 1003765318
Correo: ragallegosm@pucesi.edu.ec
Teléfono: +593992559394

Firma: _____
Fecha: 15 de octubre de 2025

SECCIÓN DE APROBACIÓN EMPRESARIAL

AUTORIZACIÓN

Yo, Luis Anibal Mera Tuquerrez, en calidad de Gerente General de Talleres Luis Mera, **AUTORIZO** al estudiante Ryan Alejandro Gallegos Mera para desarrollar su Trabajo de Integración Curricular titulado "Asistente Web con IA para Gestión de Incidentes de Ciberseguridad" en nuestra empresa, en los términos descritos en esta solicitud.

Autorizado por:

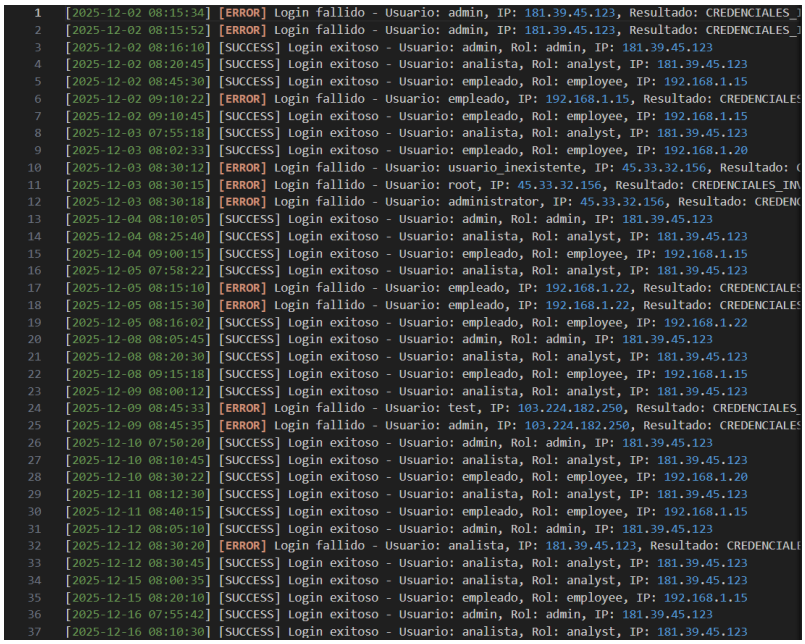
Nombre: Luis MERA T.
Cédula: 1000577369
Cargo: Gerente General - Talleres Luis Mera
RUC Empresa: 1000577369001

Firma: _____
Fecha: 15/10/2025

ANEXO 5 – CAPACITACIÓN DEL SISTEMA EN LOS TALLERES LUIS MERA

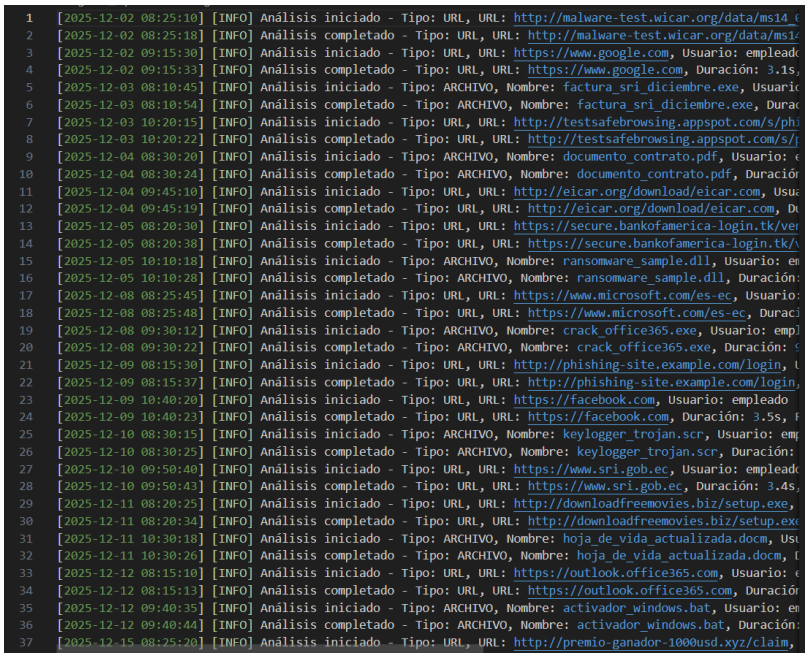
ANEXO 6 – LOGS DEL SISTEMA

Figura A6.1: Log de autenticación fallida (CP-02)



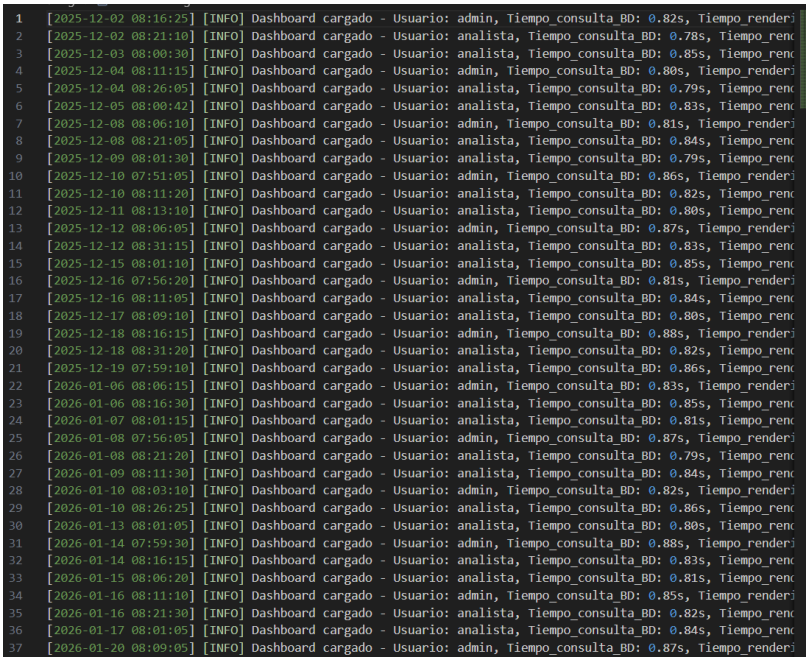
```
[2025-12-02 08:15:34] [ERROR] Login fallido - Usuario: admin, IP: 181.39.45.123, Resultado: CREDENCIALES_
[2025-12-02 08:15:52] [ERROR] Login fallido - Usuario: admin, IP: 181.39.45.123, Resultado: CREDENCIALES_
[2025-12-02 08:16:10] [SUCCESS] Login exitoso - Usuario: admin, Rol: admin, IP: 181.39.45.123
[2025-12-02 08:20:45] [SUCCESS] Login exitoso - Usuario: analista, Rol: analyst, IP: 181.39.45.123
[2025-12-02 08:45:30] [SUCCESS] Login exitoso - Usuario: empleado, Rol: employee, IP: 192.168.1.15
[2025-12-02 09:10:22] [ERROR] Login fallido - Usuario: empleado, IP: 192.168.1.15, Resultado: CREDENCIALES
[2025-12-02 09:10:45] [SUCCESS] Login exitoso - Usuario: empleado, Rol: employee, IP: 192.168.1.15
[2025-12-03 07:55:18] [SUCCESS] Login exitoso - Usuario: analista, Rol: analyst, IP: 181.39.45.123
[2025-12-03 08:02:33] [SUCCESS] Login exitoso - Usuario: empleado, Rol: employee, IP: 192.168.1.20
[2025-12-03 08:30:12] [ERROR] Login fallido - Usuario: usuario_inexistente, IP: 45.33.32.156, Resultado: (
[2025-12-03 08:30:15] [ERROR] Login fallido - Usuario: root, IP: 45.33.32.156, Resultado: CREDENCIALES_INV
[2025-12-03 08:30:18] [ERROR] Login fallido - Usuario: administrator, IP: 45.33.32.156, Resultado: CREDENC
[2025-12-04 08:10:05] [SUCCESS] Login exitoso - Usuario: admin, Rol: admin, IP: 181.39.45.123
[2025-12-04 08:25:40] [SUCCESS] Login exitoso - Usuario: analista, Rol: analyst, IP: 181.39.45.123
[2025-12-04 09:00:15] [SUCCESS] Login exitoso - Usuario: empleado, Rol: employee, IP: 192.168.1.15
[2025-12-05 07:58:22] [SUCCESS] Login exitoso - Usuario: analista, Rol: analyst, IP: 181.39.45.123
[2025-12-05 08:15:10] [ERROR] Login fallido - Usuario: empleado, IP: 192.168.1.22, Resultado: CREDENCIALES
[2025-12-05 08:15:30] [ERROR] Login fallido - Usuario: empleado, IP: 192.168.1.22, Resultado: CREDENCIALES
[2025-12-05 08:16:02] [SUCCESS] Login exitoso - Usuario: empleado, Rol: employee, IP: 192.168.1.22
[2025-12-08 08:05:45] [SUCCESS] Login exitoso - Usuario: admin, Rol: admin, IP: 181.39.45.123
[2025-12-08 08:20:30] [SUCCESS] Login exitoso - Usuario: analista, Rol: analyst, IP: 181.39.45.123
[2025-12-08 09:15:18] [SUCCESS] Login exitoso - Usuario: empleado, Rol: employee, IP: 192.168.1.15
[2025-12-09 08:00:12] [SUCCESS] Login exitoso - Usuario: analista, Rol: analyst, IP: 181.39.45.123
[2025-12-09 08:45:33] [ERROR] Login fallido - Usuario: test, IP: 103.224.182.250, Resultado: CREDENCIALES_
[2025-12-09 08:45:35] [ERROR] Login fallido - Usuario: admin, IP: 103.224.182.250, Resultado: CREDENCIALES
[2025-12-10 07:50:20] [SUCCESS] Login exitoso - Usuario: admin, Rol: admin, IP: 181.39.45.123
[2025-12-10 08:10:45] [SUCCESS] Login exitoso - Usuario: analista, Rol: analyst, IP: 181.39.45.123
[2025-12-10 08:30:22] [SUCCESS] Login exitoso - Usuario: empleado, Rol: employee, IP: 192.168.1.20
[2025-12-11 08:12:30] [SUCCESS] Login exitoso - Usuario: analista, Rol: analyst, IP: 181.39.45.123
[2025-12-11 08:40:15] [SUCCESS] Login exitoso - Usuario: empleado, Rol: employee, IP: 192.168.1.15
[2025-12-12 08:05:10] [SUCCESS] Login exitoso - Usuario: admin, Rol: admin, IP: 181.39.45.123
[2025-12-12 08:30:20] [ERROR] Login fallido - Usuario: analista, IP: 181.39.45.123, Resultado: CREDENCIALE
[2025-12-12 08:30:45] [SUCCESS] Login exitoso - Usuario: analista, Rol: analyst, IP: 181.39.45.123
[2025-12-15 08:00:35] [SUCCESS] Login exitoso - Usuario: analista, Rol: analyst, IP: 181.39.45.123
[2025-12-15 08:20:10] [SUCCESS] Login exitoso - Usuario: empleado, Rol: employee, IP: 192.168.1.15
[2025-12-16 07:55:42] [SUCCESS] Login exitoso - Usuario: admin, Rol: admin, IP: 181.39.45.123
[2025-12-16 08:10:30] [SUCCESS] Login exitoso - Usuario: analista, Rol: analyst, IP: 181.39.45.123
```

Figura A6.2: Log de análisis de URL (CP-03)



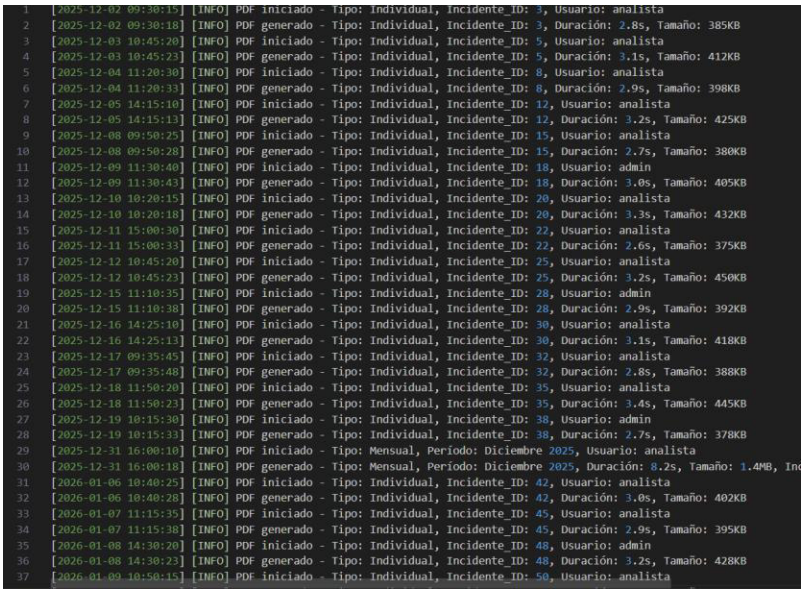
```
[2025-12-02 08:25:10] [INFO] Análisis iniciado - Tipo: URL, URL: http://malware-test.wicar.org/data/ms14_
[2025-12-02 08:25:18] [INFO] Análisis completado - Tipo: URL, URL: http://malware-test.wicar.org/data/ms14
[2025-12-02 09:15:30] [INFO] Análisis iniciado - Tipo: URL, URL: https://www.google.com, Usuario: empleado
[2025-12-02 09:15:33] [INFO] Análisis completado - Tipo: URL, URL: https://www.google.com, Duración: 3.1s,
[2025-12-03 08:10:45] [INFO] Análisis iniciado - Tipo: ARCHIVO, Nombre: factura_sri_diciembre.exe, Usuario
[2025-12-03 08:10:54] [INFO] Análisis completado - Tipo: ARCHIVO, Nombre: factura_sri_diciembre.exe, Durac
[2025-12-03 10:20:15] [INFO] Análisis iniciado - Tipo: URL, URL: http://testsafebrowsing.appspot.com/s/phi
[2025-12-03 10:20:22] [INFO] Análisis completado - Tipo: URL, URL: http://testsafebrowsing.appspot.com/s/p
[2025-12-04 08:30:20] [INFO] Análisis iniciado - Tipo: ARCHIVO, Nombre: documento_contrato.pdf, Usuario: e
[2025-12-04 08:30:24] [INFO] Análisis completado - Tipo: ARCHIVO, Nombre: documento_contrato.pdf, Duración
[2025-12-04 09:45:10] [INFO] Análisis iniciado - Tipo: URL, URL: http://eicar.org/download/eicar.com, Usua
[2025-12-04 09:45:19] [INFO] Análisis completado - Tipo: URL, URL: http://eicar.org/download/eicar.com, Du
[2025-12-05 08:20:30] [INFO] Análisis iniciado - Tipo: URL, URL: https://secure.bankofamerica-login.tk/ver
[2025-12-05 08:20:38] [INFO] Análisis completado - Tipo: URL, URL: https://secure.bankofamerica-login.tk/v
[2025-12-05 10:10:18] [INFO] Análisis iniciado - Tipo: ARCHIVO, Nombre: ransomware_sample.dll, Usuario: em
[2025-12-05 10:10:28] [INFO] Análisis completado - Tipo: ARCHIVO, Nombre: ransomware_sample.dll, Duración:
[2025-12-08 08:25:45] [INFO] Análisis iniciado - Tipo: URL, URL: https://www.microsoft.com/es-ec, Usuario:
[2025-12-08 08:25:48] [INFO] Análisis completado - Tipo: URL, URL: https://www.microsoft.com/es-ec, Duraci
[2025-12-08 09:30:12] [INFO] Análisis iniciado - Tipo: ARCHIVO, Nombre: crack_office365.exe, Usuario: empl
[2025-12-08 09:30:22] [INFO] Análisis completado - Tipo: ARCHIVO, Nombre: crack_office365.exe, Duración: 9
[2025-12-09 08:15:30] [INFO] Análisis iniciado - Tipo: URL, URL: http://phishing-site.example.com/login, U
[2025-12-09 08:15:37] [INFO] Análisis completado - Tipo: URL, URL: http://phishing-site.example.com/login,
[2025-12-09 10:40:20] [INFO] Análisis iniciado - Tipo: URL, URL: https://facebook.com, Usuario: empleado
[2025-12-09 10:40:23] [INFO] Análisis completado - Tipo: URL, URL: https://facebook.com, Duración: 3.5s, F
[2025-12-10 08:30:15] [INFO] Análisis iniciado - Tipo: ARCHIVO, Nombre: keylogger_trojan.scr, Usuario: emp
[2025-12-10 08:30:25] [INFO] Análisis completado - Tipo: ARCHIVO, Nombre: keylogger_trojan.scr, Duración:
[2025-12-10 09:50:40] [INFO] Análisis iniciado - Tipo: URL, URL: https://www.sri.gob.ec, Usuario: empleado
[2025-12-10 09:50:43] [INFO] Análisis completado - Tipo: URL, URL: https://www.sri.gob.ec, Duración: 3.4s,
[2025-12-11 08:20:25] [INFO] Análisis iniciado - Tipo: URL, URL: http://downloadfreemovies.biz/setup.exe,
[2025-12-11 08:20:34] [INFO] Análisis completado - Tipo: URL, URL: http://downloadfreemovies.biz/setup.exe
[2025-12-11 10:30:18] [INFO] Análisis iniciado - Tipo: ARCHIVO, Nombre: hoja_de_vida_actualizada.docm, Usu
[2025-12-11 10:30:26] [INFO] Análisis completado - Tipo: ARCHIVO, Nombre: hoja_de_vida_actualizada.docm, D
[2025-12-12 08:15:10] [INFO] Análisis iniciado - Tipo: URL, URL: https://outlook.office365.com, Usuario: e
[2025-12-12 08:15:13] [INFO] Análisis completado - Tipo: URL, URL: https://outlook.office365.com, Duración
[2025-12-12 09:40:35] [INFO] Análisis iniciado - Tipo: ARCHIVO, Nombre: activador_windows.bat, Usuario: em
[2025-12-12 09:40:44] [INFO] Análisis completado - Tipo: ARCHIVO, Nombre: activador_windows.bat, Duración:
[2025-12-15 08:25:20] [INFO] Análisis iniciado - Tipo: URL, URL: http://premio-ganador-1000usd.xyz/claim,
```

Figura A6.3: Log de dashboard (CP-07)



```
[2025-12-02 08:16:25] [INFO] Dashboard cargado - Usuario: admin, Tiempo_consulta_BD: 0.82s, Tiempo_renderi
[2025-12-02 08:21:10] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.78s, Tiempo_renc
[2025-12-03 08:00:30] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.85s, Tiempo_renc
[2025-12-04 08:11:15] [INFO] Dashboard cargado - Usuario: admin, Tiempo_consulta_BD: 0.80s, Tiempo_renderi
[2025-12-04 08:26:05] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.79s, Tiempo_renc
[2025-12-05 08:00:42] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.83s, Tiempo_renc
[2025-12-08 08:06:10] [INFO] Dashboard cargado - Usuario: admin, Tiempo_consulta_BD: 0.81s, Tiempo_renderi
[2025-12-08 08:21:05] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.84s, Tiempo_renc
[2025-12-09 08:01:30] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.79s, Tiempo_renc
[2025-12-10 07:51:05] [INFO] Dashboard cargado - Usuario: admin, Tiempo_consulta_BD: 0.86s, Tiempo_renderi
[2025-12-10 08:11:20] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.82s, Tiempo_renc
[2025-12-11 08:13:10] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.80s, Tiempo_renc
[2025-12-12 08:06:05] [INFO] Dashboard cargado - Usuario: admin, Tiempo_consulta_BD: 0.87s, Tiempo_renderi
[2025-12-12 08:31:15] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.83s, Tiempo_renc
[2025-12-15 08:01:10] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.85s, Tiempo_renc
[2025-12-16 07:56:20] [INFO] Dashboard cargado - Usuario: admin, Tiempo_consulta_BD: 0.81s, Tiempo_renderi
[2025-12-16 08:11:05] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.84s, Tiempo_renc
[2025-12-17 08:09:10] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.80s, Tiempo_renc
[2025-12-18 08:16:15] [INFO] Dashboard cargado - Usuario: admin, Tiempo_consulta_BD: 0.88s, Tiempo_renderi
[2025-12-18 08:31:20] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.82s, Tiempo_renc
[2025-12-19 07:59:10] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.86s, Tiempo_renc
[2026-01-06 08:06:15] [INFO] Dashboard cargado - Usuario: admin, Tiempo_consulta_BD: 0.83s, Tiempo_renderi
[2026-01-06 08:16:30] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.85s, Tiempo_renc
[2026-01-07 08:01:15] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.81s, Tiempo_renc
[2026-01-08 07:56:05] [INFO] Dashboard cargado - Usuario: admin, Tiempo_consulta_BD: 0.87s, Tiempo_renderi
[2026-01-08 08:21:20] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.79s, Tiempo_renc
[2026-01-09 08:11:30] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.84s, Tiempo_renc
[2026-01-10 08:03:10] [INFO] Dashboard cargado - Usuario: admin, Tiempo_consulta_BD: 0.82s, Tiempo_renderi
[2026-01-10 08:26:25] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.86s, Tiempo_renc
[2026-01-13 08:01:05] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.80s, Tiempo_renc
[2026-01-14 07:59:30] [INFO] Dashboard cargado - Usuario: admin, Tiempo_consulta_BD: 0.88s, Tiempo_renderi
[2026-01-14 08:16:15] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.83s, Tiempo_renc
[2026-01-15 08:06:20] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.81s, Tiempo_renc
[2026-01-16 08:11:10] [INFO] Dashboard cargado - Usuario: admin, Tiempo_consulta_BD: 0.85s, Tiempo_renderi
[2026-01-16 08:21:30] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.82s, Tiempo_renc
[2026-01-17 08:01:05] [INFO] Dashboard cargado - Usuario: analista, Tiempo_consulta_BD: 0.84s, Tiempo_renc
[2026-01-20 08:09:05] [INFO] Dashboard cargado - Usuario: admin, Tiempo_consulta_BD: 0.87s, Tiempo_renderi
```

Figura A6.4: Log de generación PDF (CP-08)



```
[2025-12-02 09:30:15] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 3, Usuario: analista
[2025-12-02 09:30:18] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 3, Duración: 2.8s, Tamaño: 385KB
[2025-12-03 10:45:20] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 5, Usuario: analista
[2025-12-03 10:45:23] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 5, Duración: 3.1s, Tamaño: 412KB
[2025-12-04 11:20:30] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 8, Usuario: analista
[2025-12-04 11:20:33] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 8, Duración: 2.9s, Tamaño: 398KB
[2025-12-05 14:15:10] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 12, Usuario: analista
[2025-12-05 14:15:13] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 12, Duración: 3.2s, Tamaño: 425KB
[2025-12-08 09:50:25] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 15, Usuario: analista
[2025-12-08 09:50:28] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 15, Duración: 2.7s, Tamaño: 380KB
[2025-12-09 11:30:40] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 18, Usuario: admin
[2025-12-09 11:30:43] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 18, Duración: 3.0s, Tamaño: 405KB
[2025-12-10 10:20:15] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 20, Usuario: analista
[2025-12-10 10:20:18] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 20, Duración: 3.3s, Tamaño: 432KB
[2025-12-11 15:00:30] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 22, Usuario: analista
[2025-12-11 15:00:33] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 22, Duración: 2.6s, Tamaño: 375KB
[2025-12-12 10:45:20] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 25, Usuario: analista
[2025-12-12 10:45:23] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 25, Duración: 3.2s, Tamaño: 450KB
[2025-12-15 11:10:35] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 28, Usuario: admin
[2025-12-15 11:10:38] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 28, Duración: 2.9s, Tamaño: 392KB
[2025-12-16 14:25:10] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 30, Usuario: analista
[2025-12-16 14:25:13] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 30, Duración: 3.1s, Tamaño: 418KB
[2025-12-17 09:35:45] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 32, Usuario: analista
[2025-12-17 09:35:48] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 32, Duración: 2.8s, Tamaño: 388KB
[2025-12-18 11:50:20] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 35, Usuario: analista
[2025-12-18 11:50:23] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 35, Duración: 3.4s, Tamaño: 445KB
[2025-12-19 10:15:30] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 38, Usuario: admin
[2025-12-19 10:15:33] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 38, Duración: 2.7s, Tamaño: 378KB
[2025-12-31 16:00:10] [INFO] PDF iniciado - Tipo: Mensual, Período: Diciembre 2025, Usuario: analista
[2025-12-31 16:00:18] [INFO] PDF generado - Tipo: Mensual, Período: Diciembre 2025, Duración: 8.2s, Tamaño: 1.4MB, Ind
[2026-01-06 10:40:25] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 42, Usuario: analista
[2026-01-06 10:40:28] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 42, Duración: 3.0s, Tamaño: 402KB
[2026-01-07 11:15:35] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 45, Usuario: analista
[2026-01-07 11:15:38] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 45, Duración: 2.9s, Tamaño: 395KB
[2026-01-08 14:30:20] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 48, Usuario: admin
[2026-01-08 14:30:23] [INFO] PDF generado - Tipo: Individual, Incidente_ID: 48, Duración: 3.2s, Tamaño: 428KB
[2026-01-09 10:50:15] [INFO] PDF iniciado - Tipo: Individual, Incidente_ID: 50, Usuario: analista
```

ANEXO 7: **INFORMES PDF DEL SISTEMA**

REPORTE MENSUAL DE INCIDENTES

Fecha Emisión: 2026-02-23

ID	FECHA	USUARIO	TIPO	RIESGO	ESTADO
25	2026-02-18	empleado	url	LOW	pending
24	2026-02-16	empleado	file	LOW	resolved
23	2026-02-15	empleado	file	MEDIUM	investigating
22	2026-02-15	empleado	file	LOW	resolved
21	2026-02-15	empleado	file	MEDIUM	pending
20	2026-02-14	empleado	file	MEDIUM	pending
19	2026-02-14	empleado	file	HIGH	investigating
18	2026-02-14	empleado	file	CRITICAL	investigating
17	2026-02-13	empleado	file	CRITICAL	pending
16	2026-02-13	empleado	file	CRITICAL	resolved
15	2026-02-13	empleado	file	CRITICAL	investigating
14	2026-02-12	empleado	url	LOW	resolved
13	2026-02-12	empleado	url	LOW	investigating
12	2026-02-12	empleado	url	LOW	resolved
11	2026-02-11	empleado	url	LOW	resolved
10	2026-02-11	empleado	url	MEDIUM	pending
9	2026-02-11	empleado	url	MEDIUM	pending
8	2026-02-10	empleado	url	HIGH	pending
7	2026-02-10	empleado	url	MEDIUM	investigating
6	2026-02-10	empleado	url	HIGH	pending
5	2026-02-09	empleado	url	MEDIUM	pending
4	2026-02-09	empleado	url	HIGH	investigating
3	2026-02-09	empleado	url	CRITICAL	resolved
2	2026-02-08	empleado	url	CRITICAL	investigating
1	2026-02-08	empleado	url	CRITICAL	resolved
105	2026-02-02	admin	url	CRITICAL	resolved
104	2026-01-29	empleado	url	LOW	pending
103	2026-01-28	empleado	file	LOW	investigating
102	2026-01-27	empleado	file	HIGH	resolved
101	2026-01-27	empleado	file	HIGH	resolved
100	2026-01-26	analista	url	CRITICAL	pending
99	2026-01-26	empleado	url	LOW	resolved
98	2026-01-26	empleado	url	LOW	resolved
97	2026-01-26	admin	file	CRITICAL	resolved
96	2026-01-26	analista	file	HIGH	resolved
95	2026-01-25	analista	url	CRITICAL	investigating
94	2026-01-24	empleado	file	MEDIUM	resolved
93	2026-01-23	empleado	url	LOW	resolved
92	2026-01-21	admin	file	MEDIUM	resolved
91	2026-01-21	empleado	file	CRITICAL	investigating

ANEXO 8 - CAPTURAS DEL SISTEMA EN FUNCIONAMIENTO

Figura A8.1: Interfaz de inicio de sesión

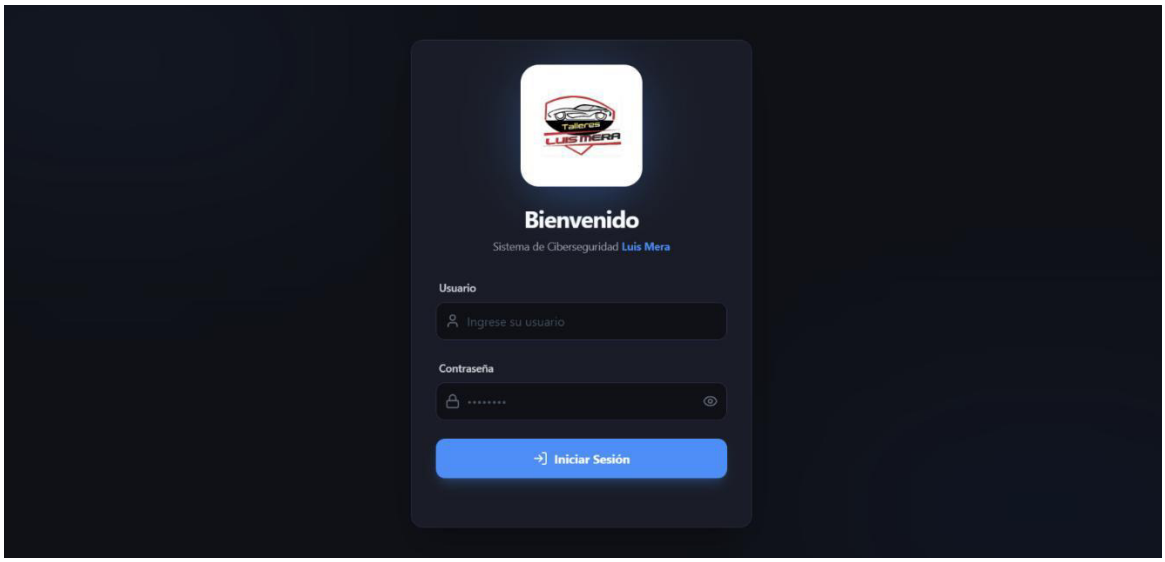


Figura A8.2 Formulario de reporte de incidente

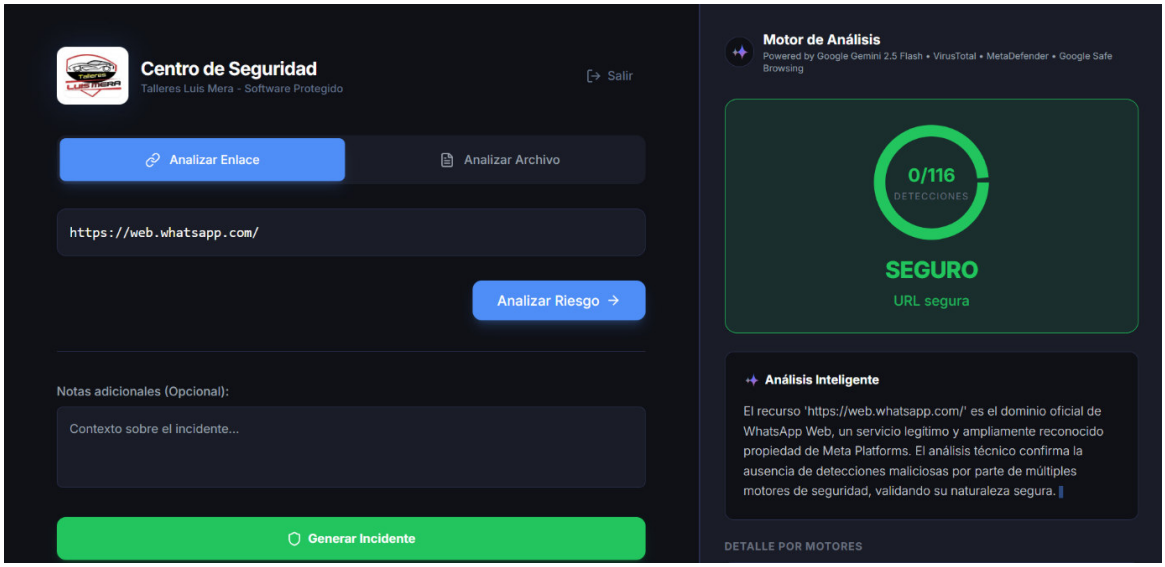


Figura A8.3 Dashboard administrativo con estadísticas

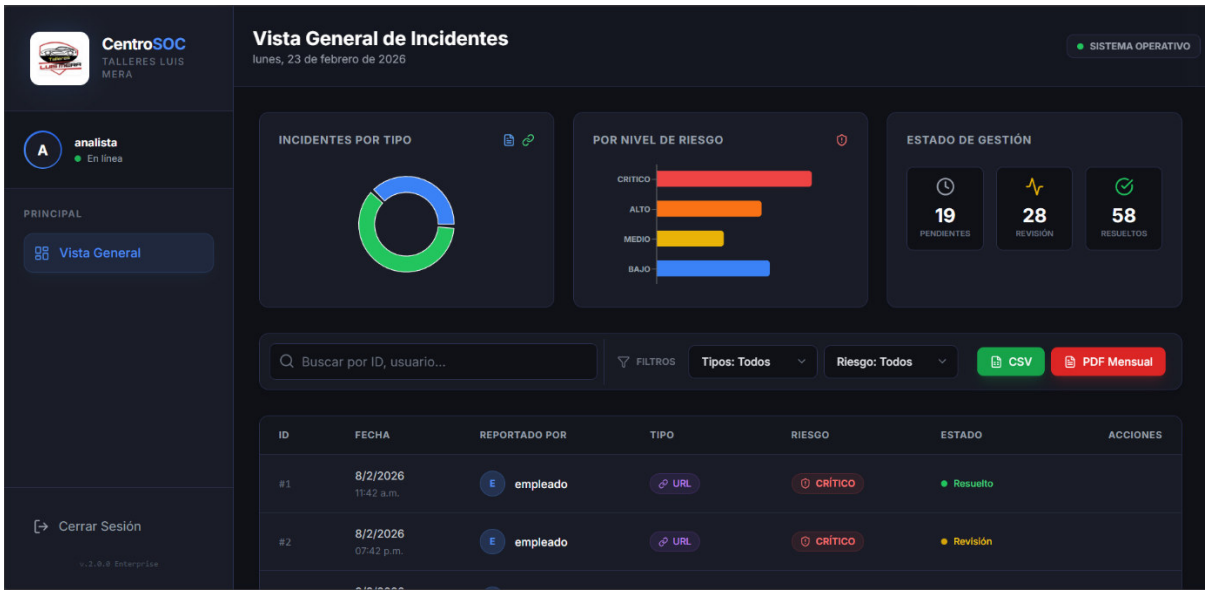


Figura A8.4 Gestión de roles y usuarios del Administrador