

Implementación de un sistema de detección de phishing basado
en Machine Learning para la mitigación de amenazas en flujos de
mensajería de correo electrónico mediante el protocolo IMAP para la consultora
Hackick – IT Services & Consulting

INTEGRANTES

Freire Ortega Anderson Alejandro

Osorio Salazar Geovani Alejandro



Sponsor



Hackick, empresa fundada por ingenieros especialistas en el campo de Tecnología, contamos con una amplia experiencia en proyectos de TI, VR, IA, Cloud, Ciberseguridad. Nuestro portafolio de servicios se ajusta a la medida y necesidad de nuestros clientes, mismos que permiten diferenciarnos del mercado tradicional.

CIBERSEGURIDAD

CLOUD COMPUTING

PROTECCIÓN DATOS

SCRIBE4U SERVICE

DEFINICIÓN PROBLEMA

- **Evolución de la Amenaza:** El phishing moderno utiliza IA generativa y dominios legítimos, evadiendo filtros estáticos tradicionales (listas negras/reglas).
- **Brecha en PYMES:** Las pequeñas empresas carecen de soluciones avanzadas por altos costos y complejidad técnica.
- **El Factor Crítico:** El correo es el vector principal para intercambiar datos críticos; un solo error humano compromete toda la cadena de suministro.
- **Insuficiencia Técnica:** Los filtros actuales son reactivos; se requiere una solución proactiva basada en el análisis semántico y estructural del mensaje.



ANÁLISIS DE POSIBLES SOLUCIONES

Criterio	Solución 1: Detección Sidecar (ML)	Solución 2: Proveedor Externo	Solución 3: Concientización Anti-Phishing
Descripción	Arquitectura Sidecar por copia que analiza correos vía IMAP con modelos de Machine Learning supervisado, operando en paralelo al servidor	Plataformas comerciales de seguridad de correo con motores propietarios y bases globales de amenazas	Programas de simulación de phishing y capacitación del usuario final

- Se evaluaron filtros tradicionales, soluciones comerciales y un sistema propio basado en aprendizaje automático. Los filtros tradicionales resultan insuficientes frente a ataques modernos, mientras que las soluciones comerciales presentan altos costos y dependencia de proveedores. El desarrollo de una solución propia basada en machine learning se selecciona como la alternativa más viable por su efectividad, flexibilidad y alineación con las capacidades de Hackick.

ALCANCE

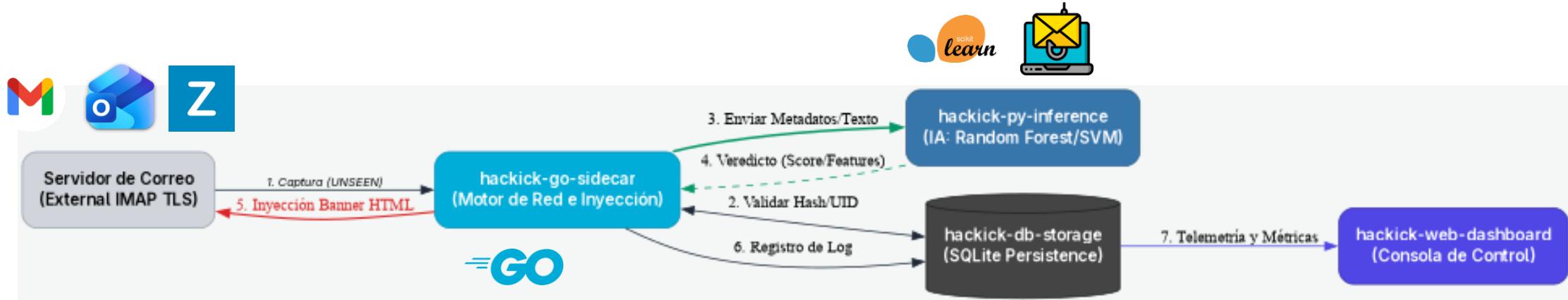
- El proyecto contempla el diseño y desarrollo de un prototipo funcional de un sistema de detección de correos electrónicos de phishing basado en técnicas de aprendizaje automático. La solución analizará correos electrónicos utilizando datasets públicos, aplicando procesos de preprocesamiento, extracción de características y entrenamiento de modelos supervisados.
- El alcance se limita a la detección automatizada de correos sospechosos en entornos de prueba, sin integración directa con servidores de correo en producción ni implementación de mecanismos de respuesta automática ante incidentes.



CAPAS DEL ALCANCE

Capa / Fase	Responsabilidad Técnica	Componentes y Herramientas Clave
I. Inteligencia (ML)	Modelado estadístico y clasificación de amenazas mediante aprendizaje supervisado.	NLTK (NLP), TF-IDF, Random Forest/SVM. Datasets: Kaggle / DataSource.ai.
II. Interconexión (Go)	Gestión de red asíncrona, filtrado selectivo e inyección reactiva de banners.	Golang, IMAP-TLS (UNSEEN), SHA-256 Hashing, Motor de Inyección MIME.
III. Persistencia y Control	Auditoría técnica, integridad de metadatos y visualización de telemetría.	SQLite (ACID), Dashboard (Métricas P, R, F1), Feedback Loop (Human-in-the-loop).
IV. Orquestación	Aislamiento de recursos, alta disponibilidad y portabilidad del entorno.	Docker Compose, Arquitectura Sidecar, Multi-contenedor (Go, Py, DB, Web).

Flujo de un correo electrónico dentro del sistema



OBJETIVOS

General

- Desarrollar un sistema funcional de detección de phishing basado en Machine Learning supervisado bajo una arquitectura Sidecar, garantizando bajo impacto operativo para Hackick.

Específicos

- **Analizar** patrones estructurales y semánticos en correos electrónicos para establecer la base de conocimiento necesaria en el entrenamiento de modelos.
- **Implementar** un sistema de intercepción de phishing con Go y un motor de clasificación en Python que automatice la identificación de amenazas bajo arquitectura Sidecar.
- **Evaluar** la herramienta mediante métricas de Precision, Recall y F1-score utilizando un dashboard de telemetría y un dashboard de telemetría, validando la robustez de la solución frente a campañas de phishing en entornos controlados

- **Al-Azab, M., & Al-Qurishi, M. (2025).** In-Depth Analysis of Phishing Email Detection: Evaluating the Performance of Machine Learning and Deep Learning Models Across Multiple Datasets. *Applied Sciences*, 15(6), 3396. <https://doi.org/10.3390/app15063396>
- **Burns, B. (2016).** *Designing Distributed Systems: Patterns and Paradigms for Scalable, Reliable Microservices*. O'Reilly Media.
- **Nath, S., & Islam, M. R. (2025).** Benchmarking Machine Learning Techniques for Phishing Detection and Secure URL Classification. *International Journal of Computer Science and Mobile Computing*, 14(1), 45-58.
- **Pedregosa, F., Varoquaux(2011).** Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research*,
- **Nightingale, S. J. (2016).** *Trustworthy Email* (NIST Special Publication 800-177 Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-177r1>

BIBLIOGRAFÍA

- Abbazi & Alsabih (2024): Phishing Email Detection Model Using Deep Learning.
- Verma & Hossain (2013): Semantic feature selection for text with application to phishing detection
- Frontiers (2024): Unveiling suspicious phishing attacks: enhancing detection with an optimal feature vectorization algorithm and supervised machine learning. *Frontiers in Computer Science*.
- MDPI (2025): Machine Learning and Watermarking for Accurate Detection of AI-Generated Phishing Emails. *Electronics*

Carta correo Tutor

Tutor Proyecto Clapstone Summarize

(Estudiante) Geovani Alejandro Osorio Salazar
To: Ricardo Alejandro Redín Gaibor
Cc: (Estudiante) Anderson Alejandro Freire Ortega

Fri 12/12/2025 10:14 AM

Buen Dia,

Estimado Profesor Alejandro Redin Por medio de la presente, deseo consultarle si sería posible contar con usted como tutor de nuestro proyecto de titulación, el cual estoy desarrollando junto a mi compañero Anderson Freire.

El tema aprobado por el comité es el siguiente:
"Sistema de detección de phishing basado en machine learning para correos electrónicos corporativos (Gmail/Outlook) o auto-hosteados."

Agradecemos de antemano su atención y quedamos pendientes de su respuesta.

Atentamente,

Geovani Osorio

NOTA DE CONFIDENCIALIDAD: La información y adjuntos contenidos en este mensaje son confidenciales y de uso exclusivo de la persona o entidad a la cual están dirigidos. Está prohibida cualquier revisión, retransmisión, difusión o cualquier otro uso de esta información, o la realización de cualquier acto en base a esta información por personas o entidades diferentes a su(s) destinatario(s), conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial Suplemento No. 459 de 26 de mayo de 2021. Si ha recibido esta información por error, por favor, póngase en contacto con el remitente y elimine el material de cualquier dispositivo.

Hackick IT Services and Consulting

Quito, Ecuador

15 de diciembre de 2025

Carta Sponsor

Asunto: Aceptación de Patrocinio para Tesis de Grado

A quien corresponda:

Por medio de la presente, Hackick IT Services and Consulting (en adelante, "El Patrocinador") se complace en confirmar la aceptación del patrocinio y la colaboración para la realización de la tesis de grado titulada:

"Sistema de detección de phishing basado en Machine Learning para correos electrónicos corporativos (Gmail/Outlook) u autohosteados"

Presentada por: Anderson Freire y Geovani Osorio

Programa Académico: Ciberseguridad Universidad de las Américas



Ing. Tomás Perugachi
Hackick

FACULTAD DE INGENIERÍA
Y CIENCIAS APLICADAS



POC

HACKICK | Engine Control
ARQUITECTURA SIDECAR POR COPIA V2.4.1

● ENGINE ONLINE Environment: Production-Pilot

PRECISIÓN (P) 98.2% (UMbral Aceptación: >95%)

EXHAUSTIVIDAD (R) 94.5% (UMbral Aceptación: >80%)

F1-SCORE 96.3% (UMbral Aceptación: >93%)

INFERNACIA (MS) 42ms (UMbral Aceptación: <50ms)

ORQUESTACIÓN DOCKER COMPOSE

hackkick-go-sidecar	Network/Injection	Healthy
	CPU: 1.2%	RAM: 45MB
hackkick-py-inference	ML_engine	Healthy
	CPU: 12.5%	RAM: 200MB
hackkick-db-sqlite	Persistence	Activo
	CPU: 8.5%	RAM: 12MB
hackkick-web-ui	dashboard	Healthy
	CPU: 8.2%	RAM: 35MB

AUDITORÍA DE EVENTOS [HACKICK.DB]

[18:10:01] INFO IMAP-Filter: Escaneando mensajes con flag [UNSEEN].
[18:10:15] INFO Go-Sidecar: UID 1024 extraido, SHA-256 verificado en SQLite.
[18:10:16] WARN Inferencia Py: Score 0.982 detectado. Clasificado como Phishing.
[18:10:17] CRIT ACCIÓN: Inyectando Banner HTML en cuerpo MIME.
[18:10:18] INFO Persistencia: Registro actualizado en hackick.db.

VALIDACIÓN GROUND TRUTH

support@amazon-security.com Score: 8.98