DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA DE SOFTWARE

TRABAJO DE INTEGRACIÓN CURRICULAR, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO/A DE SOFTWARE

TEMA:

SISTEMA DE DETECCIÓN DE INTRUSOS EN SITIOS WEB, USANDO MODELOS Y/O ALGORITMOS DE MACHINE LEARNING: CASO PRÁCTICO PHISHING GOOGLE CHROME

AUTOR:
SEMBLANTES LOZADA, GERALDYN NICOL

DIRECTOR:
Dr. CARRILLO MEDINA, JOSÉ LUIS, (mCL)

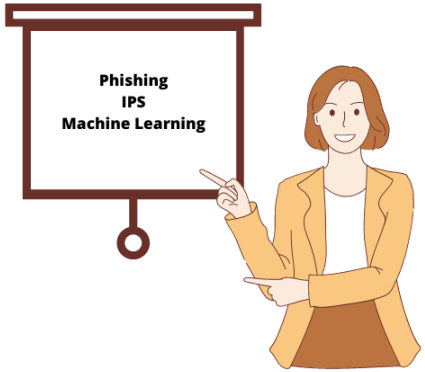
LATACUNGA AGOSTO, 2023

Orden del día

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones

Orden del día

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones



Problema

- El internet en la vida diaria de las personas sin una conciencia de ciberseguridad.
- Empresas como Facebook, Google, entidades financieras, gobiernos y miles de usuarios son victimas de ataques.
- Los ataques en el internet (Cyber-Ataques), pueden ser Malware, Botnes, Ramsomware, Brute Force Attack y Phishing. En el año 2022 se genero una perdida económica de 4,24 millones de dólares

Solución

- Se propone desarrollar un Sistema de Prevención de Intrusos (IPS) para sitios web con Phishing.
- EL IPS se lo desarrollará en forma de una extensión para el navegador Google Chrome.
- Se utilizarán modelos y/o algoritmos de Machine Learning, entrenados con un conjunto de características que son usadas con frecuencia para detectar sitios web con phishing y así implementar la extensión IPS.

Objetivo General

Desarrollar un sistema de prevención de intrusos en sitios web, usando modelos y/o algoritmos de Machine Learning: Caso Práctico Phishing Google Chrome

Objetivos Específicos

Conocer el estado del arte sobre métodos y técnicas para la prevención de intrusos en sitios web, basado en phishing por motores de búsqueda - Google Chrome.

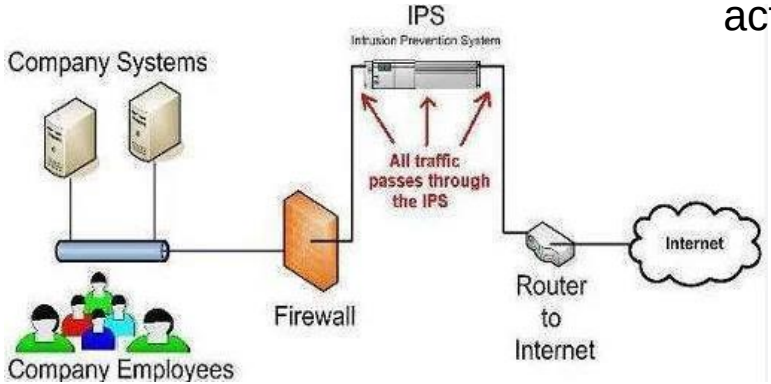
Implementar un sistema de prevención de intrusos en sitios web, a través del desarrollo de una extensión para Google Chrome, empleando técnicas de Machine Learning.

Validar los resultados, analizar los errores y ajustar los modelos del sistema de prevención de intrusos.

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones

Sistema de Prevención de Intrusos (IPS)

- Proceso detección y gestión de acciones de respuesta contra el intruso



- Supervisan en tiempo real el tráfico de paquetes con actividades maliciosas.
- Generan de alertas, para eliminar o bloquear el tráfico en tiempo real que pasa por la red

Phishing (Ciber-ataque)

- Técnica de Ingeniería social

- Los ciberdelincuentes se hacen pasar por entidades legítimas para obtener información confidencial de los usuarios

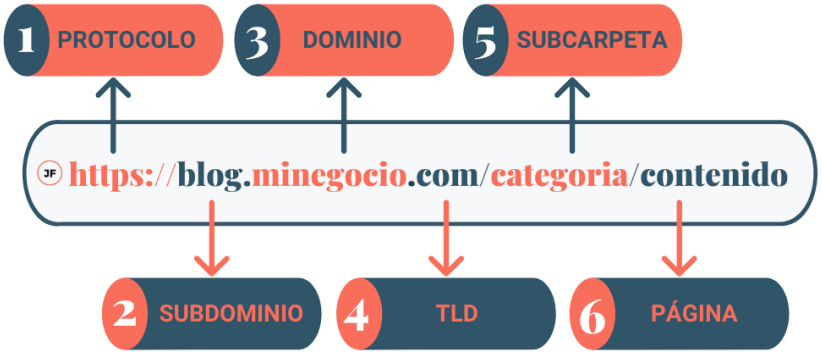
- Su naturaleza es dinámica y está en constante evolución

Características para la detección de intrusos – Phishing

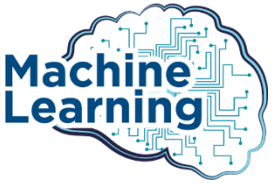
- S empleo 30 características o recursos de comprobación: basadas en el contenido del sitio web y en la URL

Sitio web con Phishing

Estructura de una URL



Modelos y/o algoritmos de Machine Learning



Rama de la inteligencia artificial con el objetivo principal hacer que las máquinas puedan tomar decisiones o hacer predicciones basadas en patrones presentes en los datos de entrenamiento

Modelos y/o algoritmos de Machine Learning

Algoritmo de aprendizaje supervisado. Alcanza una precisión máxima de 96,08% en la prevención de phishing.

Decision Tree

Algoritmo de aprendizaje supervisado. Alcanza una precisión máxima de 97,10% en la prevención de phishing.

Random Forest

Clasificador meta-estimador. Alcanza una precisión máxima del 92,91% en la prevención de phishing.

Redes Neuronales Artificiales

Algoritmo de aprendizaje supervisado. Precisión variable

Aprendizaje Profundo

Algoritmo de aprendizaje supervisado. Alcanza el 94,97% en la prevención de phishing.

Support Vector Machines

Algoritmo optimizador. Precisión variable

Mezclas Gaussianas

Modelos y/o algoritmos de Machine Learning

Algoritmo de aprendizaje supervisado. Precisión variable

K-Means

Algoritmo de aprendizaje supervisado. Precisión variblea

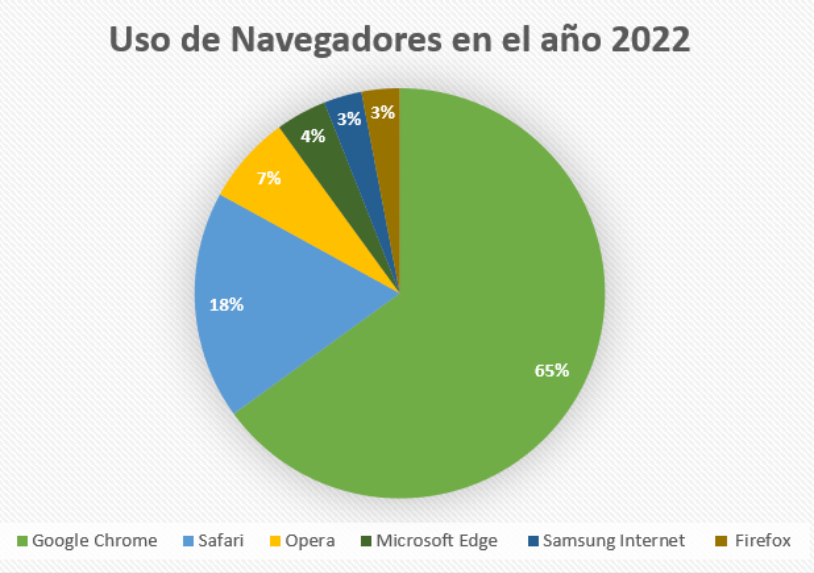
Naive Bayes

Algoritmo optimizador. Precisión variable

Redes Bayesianas

Extensiones Google Chrome

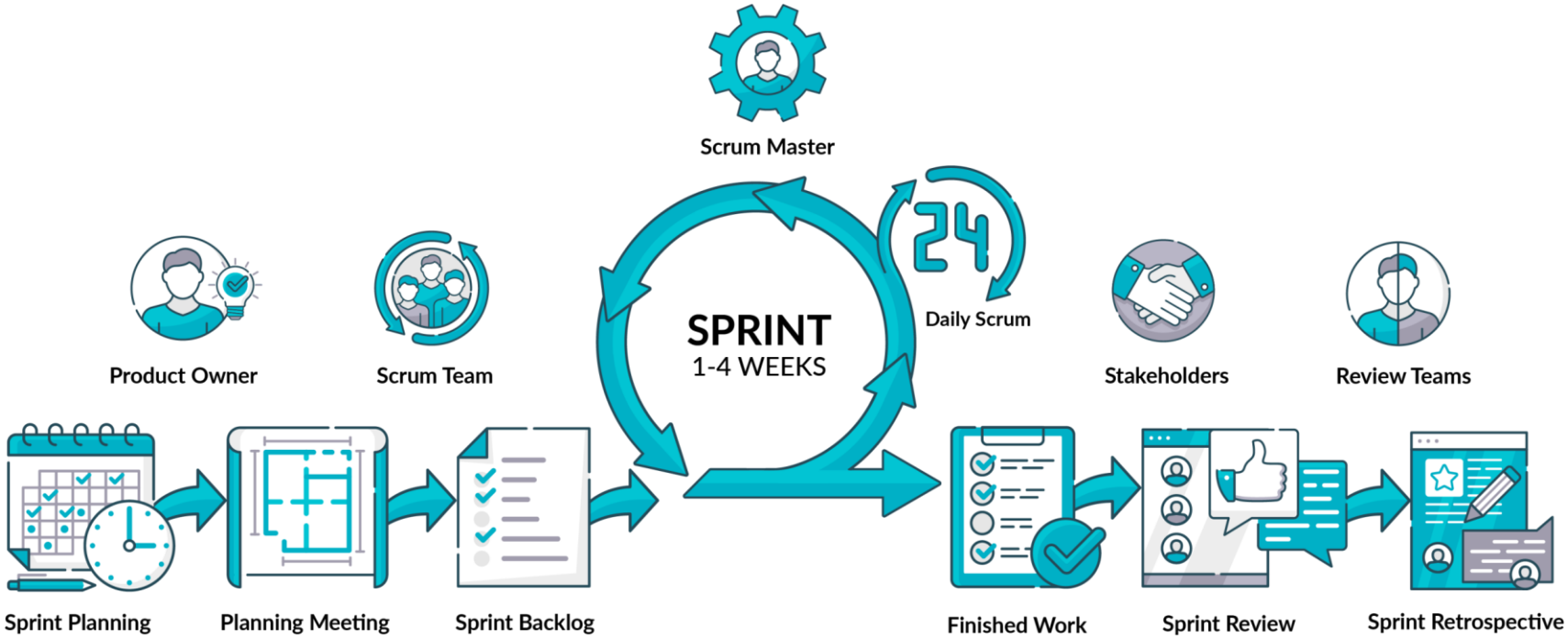
- Módulo de software usado para extender las funcionalidades del navegador Google Chrome.
- Diseñadas para proporcionar nuevas características, personalización y mejoras en la experiencia de navegación para los usuarios.
- Google Chrome el navegador mas usado en 2022.



- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones

Metodología de desarrollo

- Metodología Scrum



Recuperado de What is Scrum. (2022). App Inlet. https://appinlet.com/what-is-scrum/

Análisis del sistema

- Historias de Usuario:

Historia de usuario 01	Historia de usuario 02
Quiero que la extensión utilice el mejor algoritmo y/o modelo de Machine Learning para la prevención de phishing en sitios web.	**Quiero** un conjunto de datos que incluya características que posibiliten la distinción entre sitios web legítimos y aquellos con contenido de phishing.
Para que la extensión realice predicciones con una buena precisión.	**Para** entrenar el modelo de Machine Learning.

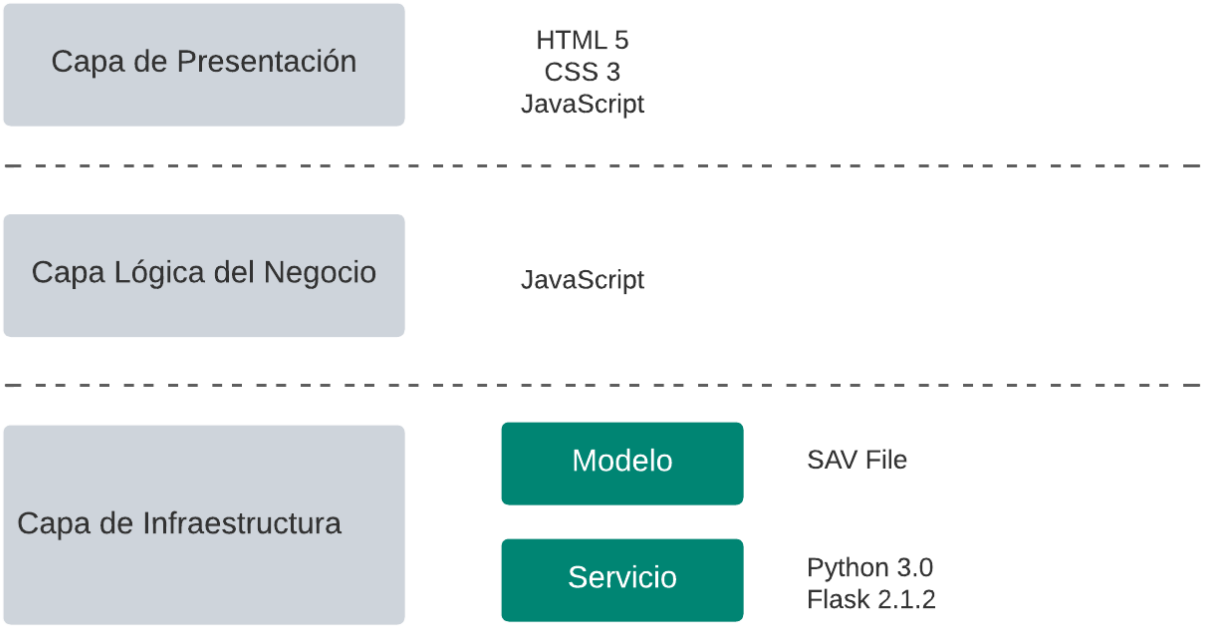
Análisis del sistema

- Historias de Usuario:

Historia de usuario 03
Quiero una extensión para el navegador Google Chrome que sea capaz de detectar y prevenir si un sitio web presenta contenido de phishing.
Para garantizar mi seguridad al navegar por sitios web usando Google Chrome, y tener la capacidad de identificar aquellos que son seguros y, en caso contrario, evitar permanecer en aquellos que puedan representar una amenaza.

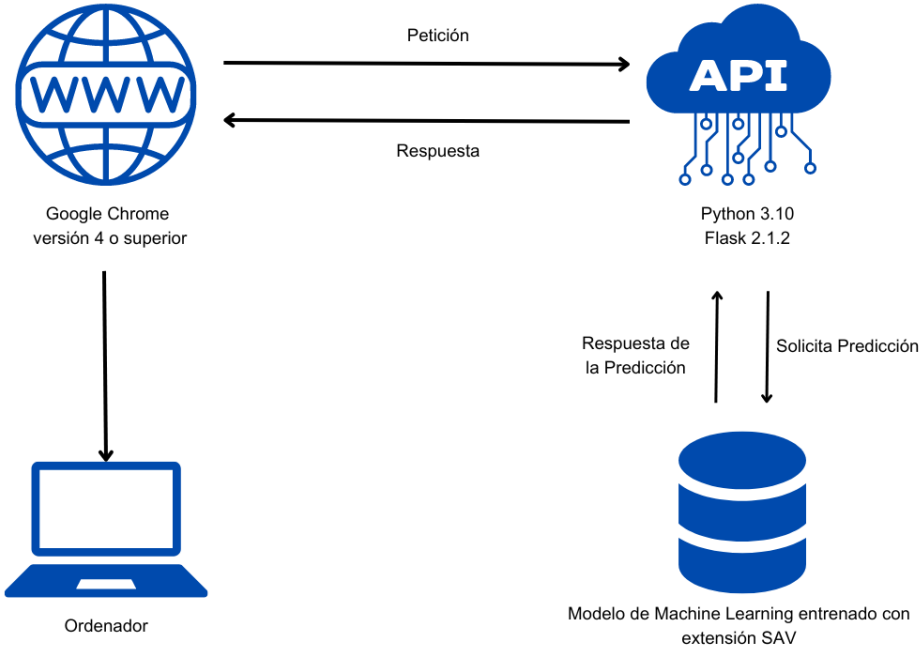
Arquitectura del sistema

- Arquitectura en Capas con las tecnologías a usar.



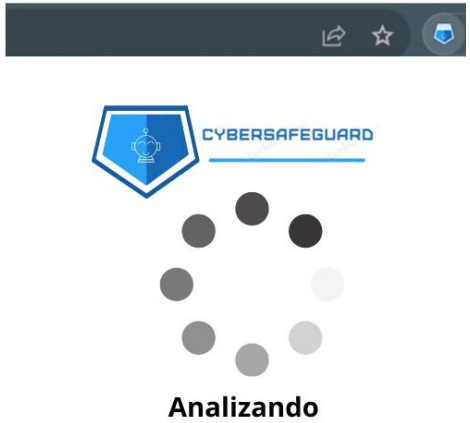
Diseño del sistema

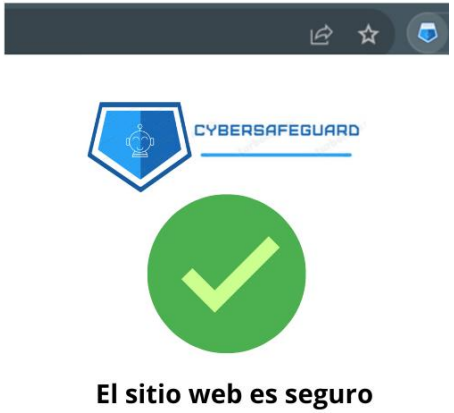
- Arquitectura Física



Diseño del sistema

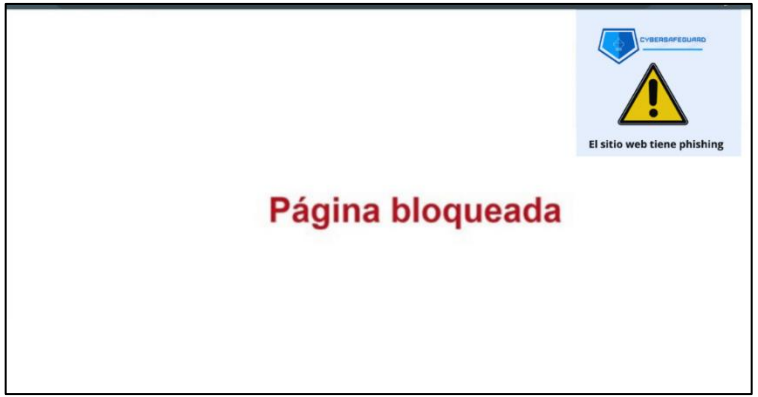
- Mockups





Diseño del sistema

- Mockups



Desarrollo del Sistema

- Resultado del Sprint 1: Selección del mejor modelo de Machine Learning

Algoritmos/Modelos	Accuracy	Precision	Recall
Decision Tree	0,9608	0,9630	0,96686
Mezclas Gausianas	0,01	0	0
Random Forest	0,9710	0,9668	0,9818
Naïve Bayes	1,00	0	0
Redes Bayesianas	1,00	0	0
SVM	0,9497	0,9419	0,9695
ANN	0,9291	0,9225	0,9527
Deep Learning	0,8013	0,8472	0,9155

Dataset utilizado: Phishing URL

https://www.kaggle.com/datasets/aktank/url-detection

Desarrollo del Sistema

- Resultado del Sprint 2: Creación del Dataset

-1
Phishing

0
Sospechoso

1
Legítimo

Ord.	haveIp	lengthUrl	haveAtSymbol	sslState	domainAge	slashDouble	anchorUrl
0	1	1	1	1	-1	1	-1
1	1	1	1	1	-1	1	-1
2	1	1	1	1	-1	1	-1
3	1	-1	1	1	-1	1	1
4	1	1	1	1	-1	1	-1

Características

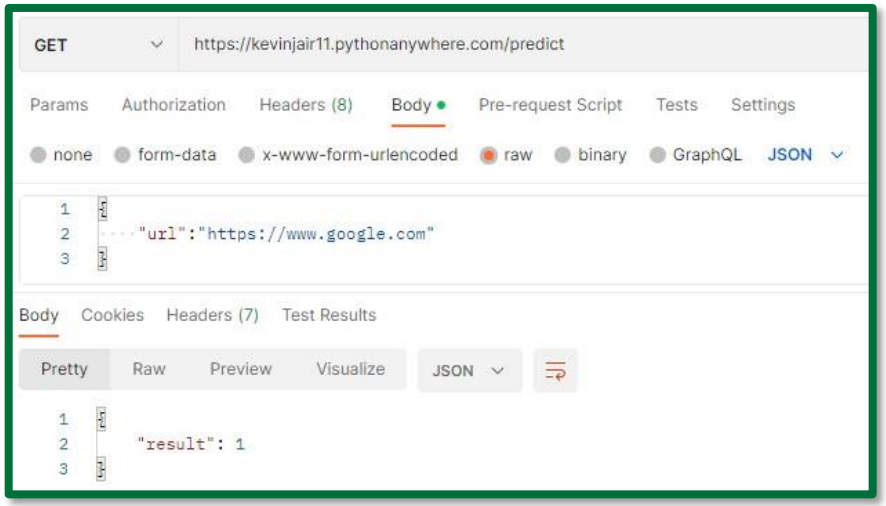
Dataset creado:

https://drive.google.com/file/d/1BEE9-4bGuQYk9M40JzqNGZJxUINjAM60/view?usp=sharing

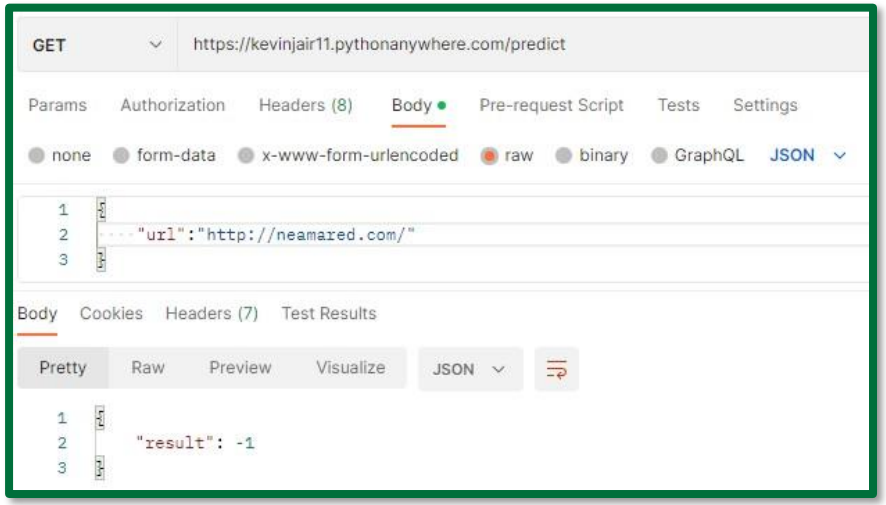
Desarrollo del Sistema

- Resultado del Sprint 3: Creación de la API

Sitio web con Phishing

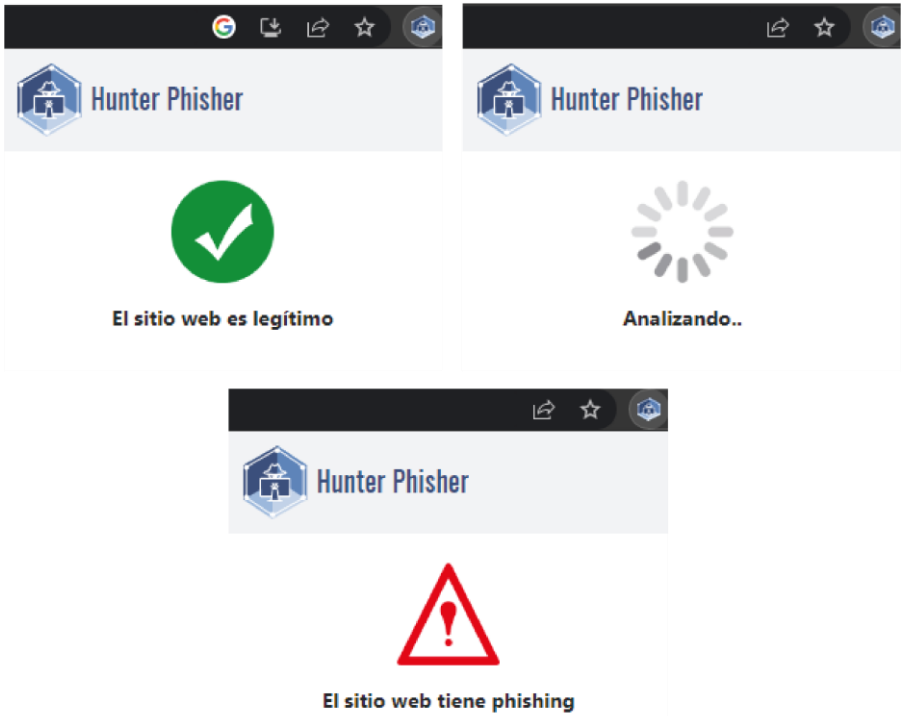


Sitio web Legítimo

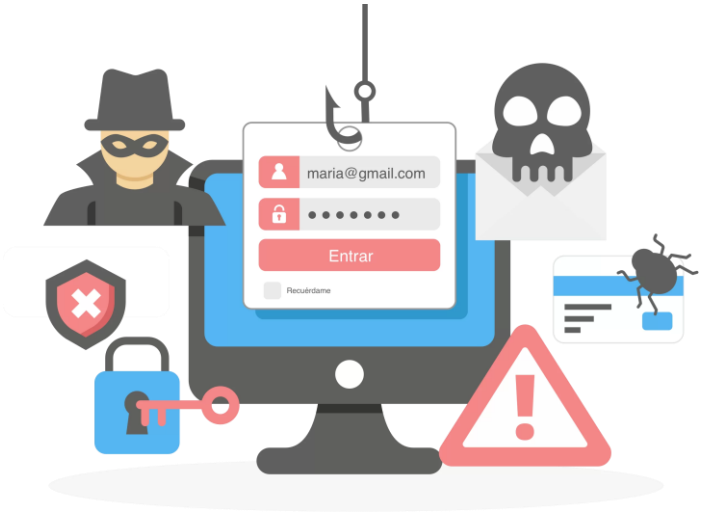


Desarrollo del Sistema

- Resultado del Sprint 4: Desarrollo de la Extensión de Google Chrome

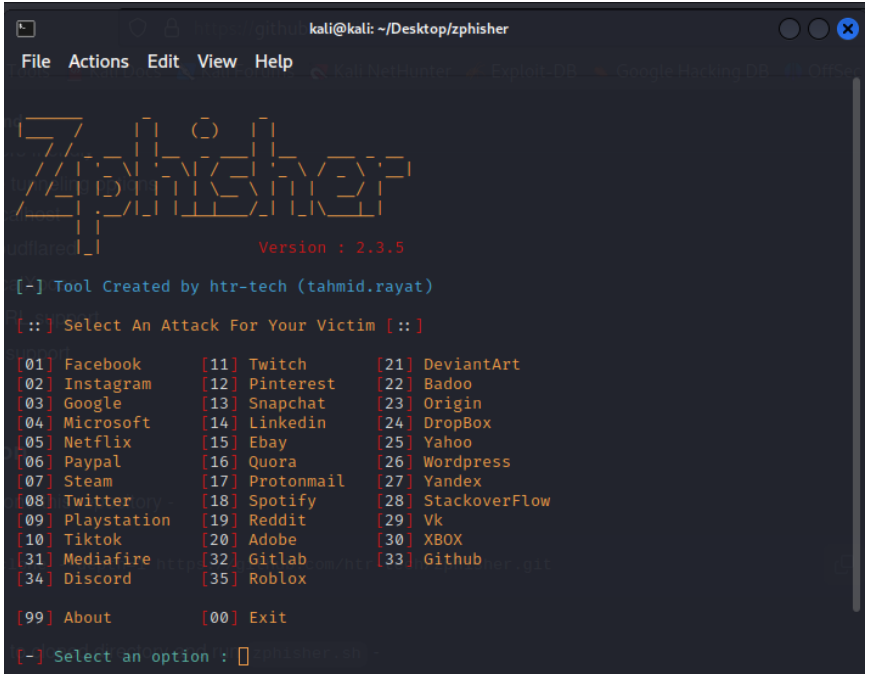


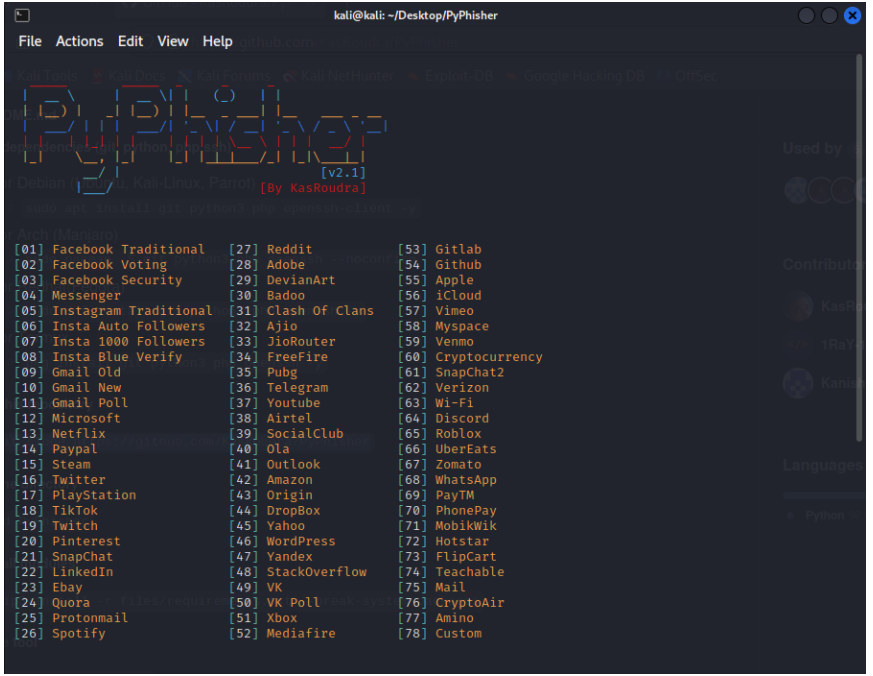
- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones



Validación del Sistema

- Uso de la herramienta Zphisher y Pyphisher(ambiente simulado)





Validación del Sistema

- Proceso de ejecución de pruebas

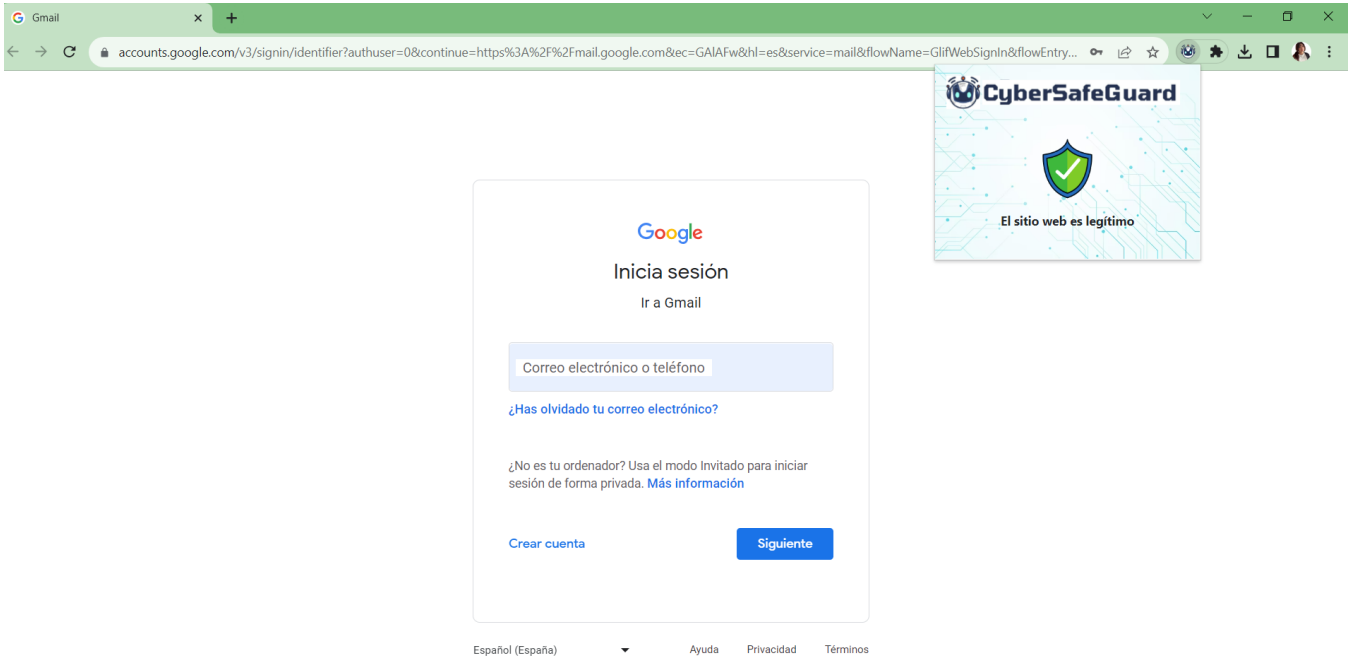
Validación del Sistema

- Se probó con 129 sitios web: 43 sitios web con phishing y 43 sitios web legítimos.

SITIO WEB	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
		RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Facebook	*Traditional Login Page*	Phishing	Phishing	Phishing	Legítimo	Legítimo
	Advanced Voting Poll Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
	Fake Security Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
	Facebook Messenger Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo

Validación del Sistema

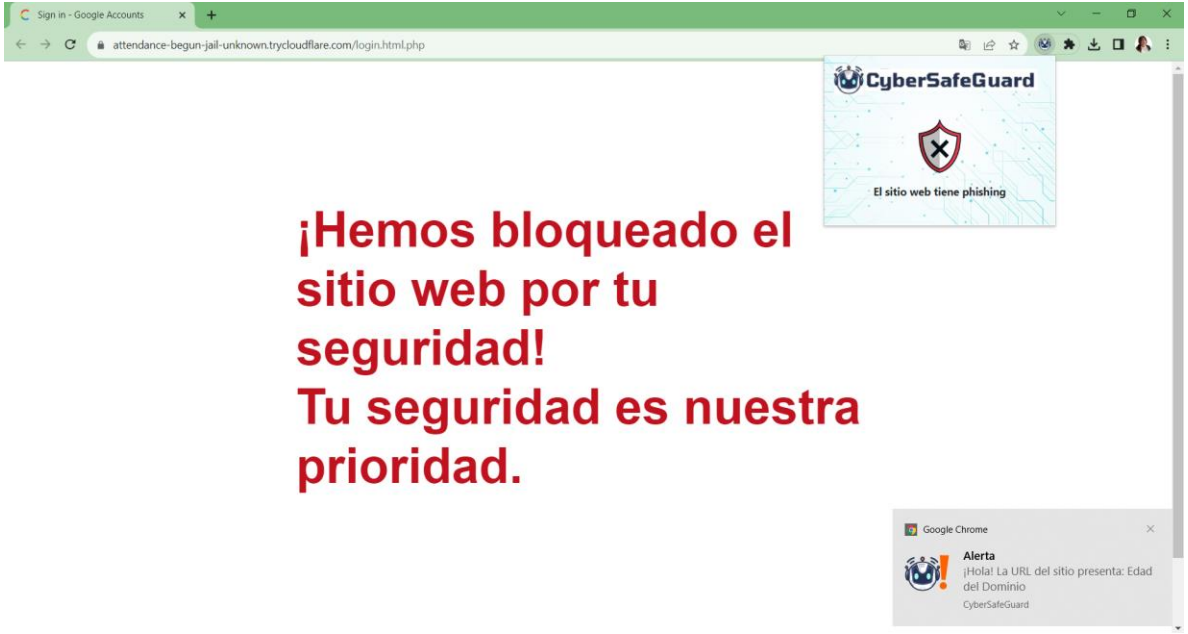
- Se muestra un análisis de un sitio web cuando es legítimo



URL: https://accounts.google.com/

Validación del Sistema

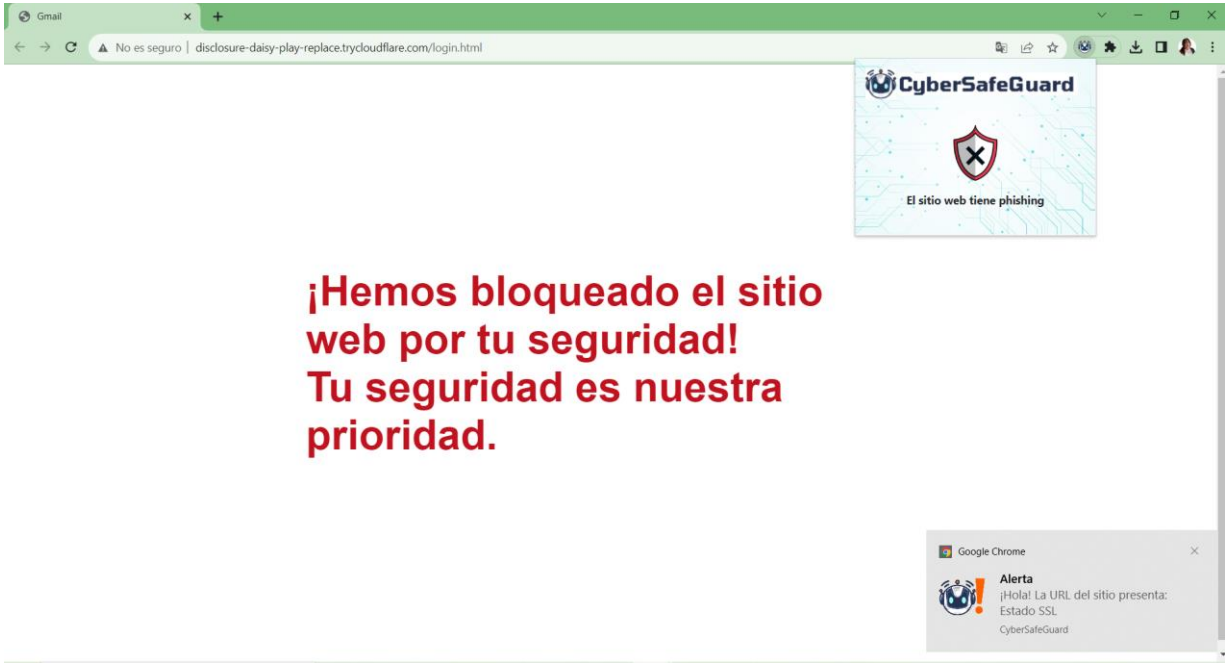
- Se muestra un análisis de un sitio web cuando tiene phishing



URL: https://attendance-begun-jail-unknown.trycloudflare.com

Validación del Sistema

- Se muestra un análisis de un sitio web cuando tiene phishing



URL: https://announcements-statute-constraints-commonwealth.trycloudflare.com

Validación del Sistema

- Obtención de datos para validar el sistema

Matriz de confusión

	POSITIVOS	NEGATIVOS
POSITIVOS	Phishing clasificados correctamente (VP)	Legítimos mal clasificados (FP)
NEGATIVOS	Phishing mal clasificados (FN)	Legítimos clasificados correctamente (VN)

Métricas de evaluación

MÉTRICA DE EVALUACIÓN	FÓRMULA
Accuracy	$\frac{VP + VN}{VP + VN + FP + FN}$
Precision	$\frac{VP}{VP + FP}$
Recall	$\frac{VP}{VP + FN}$

Validación del Sistema

- Obtención de las métricas de evaluación en los 2 modelos

	ETAPA DE ENTRENAMIENTO			CAMPO SIMULADO/REAL		
	ACCURACY	PRECISION	RECALL	ACCURACY	PRECISION	RECALL
Modelo Implementado	97,10%	96,68%	98,18%	73%	81%	60%
Modelo primer Ajuste	98,75%	97,09%	98,21%	94,19%	95,24%	93,02%

Análisis de resultados

- Se probó en un campo simulado/real con Zphisher y Pyphiser.

- Se obtuvo en la métrica Accuracy el valor más alto de 94,19% y el más bajo con 73%, valores que están aproximadamente dentro de los valores encontrados en la literatura (90% al 93,02%) de Accuracy (Alzubi *et al.,* 2018). Por lo tanto, el IPS desarrollado para prevenir ataques Phishing presenta resultados que están dentro del rango aceptable.

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones

Conclusiones

El IPS desarrollado (CyberSafeGuard) se entrenó con un dataset de 32.040 sitios web (25.151 sitios web con Phishing (78,5%) y 6.889 sitios web legítimos (21,5%)).

Se diseñó e implementó ua extensión de prevención de Phishing para Google Chrome.

Para validar el IPS (CyberSafeGuard) implementado se utilizó las herramientas Zphisher y Pyphisher.

Conclusiones

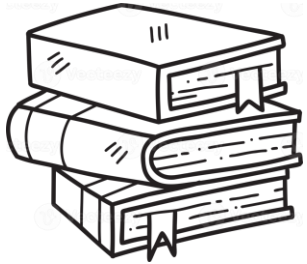
Scrum ha demostrado ser una metodología eficaz para la ejecución de este proyecto

La extensión desarrollada necesita de un entrenamiento periódico para mantenerse al día con las nuevas formas de phishing que puedan surgir, para ser puesta en un entorno real.

Referencias

- What is Scrum. (2022). *App Inlet*. https://appinlet.com/what-is-scrum/

- Alzubi, J., Nayyar, A., & Kumar, A. (2018). Machine learning from theory to algorithms: An overview. *Journal of physics. Conference series*, *1142*, 012012. https://doi.org/10.1088/1742-6596/1142/1/012012



Software
DOMINA EL MUNDO

Gracias por su atención

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA