



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA



## 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 PREVENCIÓN DE INTRUSOS EN SITIOS WEB, USANDO  
INDICADORES DE COMPROMISO APLICANDO MACHINE LEARNING: CASO  
PRÁCTICO PHISHING GOOGLE CHROME**

**AUTORES:**

ARMAS RUALES, JORGE ANDRES  
SIMBAÑA SHUGULI ANTHONY ALEXANDER

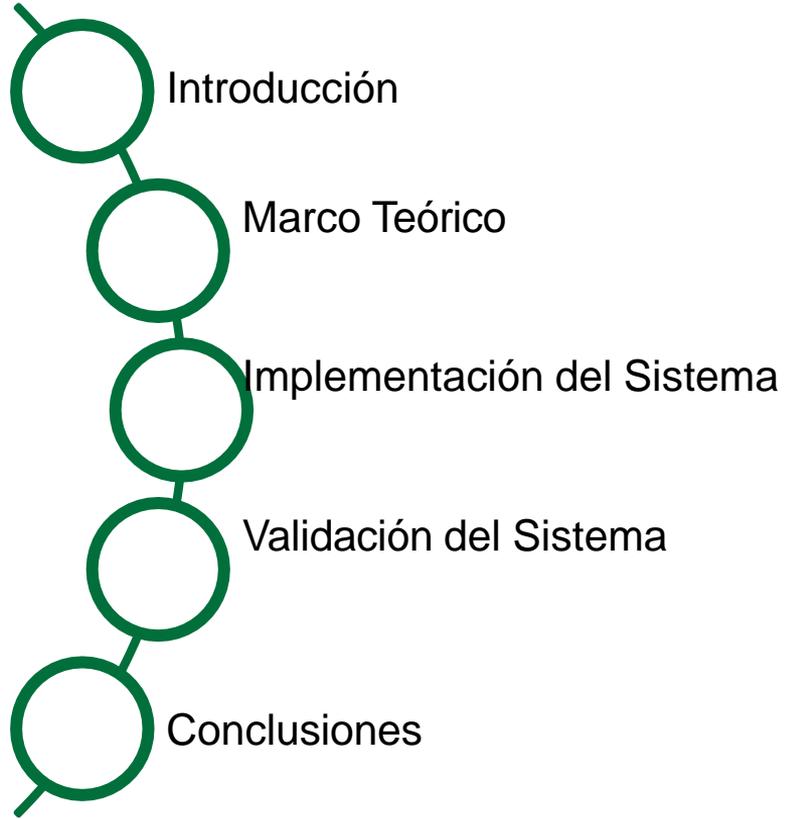
**DIRECTOR:**

Ing. CORRAL DIAZ, MARIA ALEXANDRA

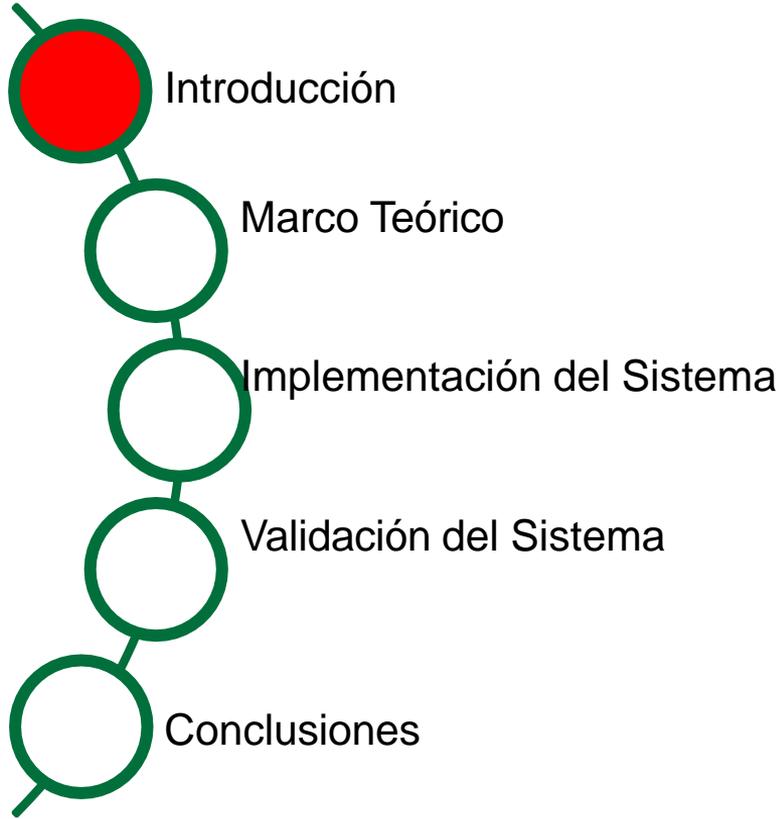
**LATACUNGA AGOSTO, 2023**



# Orden del día



# Orden del día



# Problema

- Con el crecimiento tecnológico, el internet se ha convertido lastimosamente en el principal objetivo de ciberataques.
- Vulnerabilidad a usuarios, sistemas y amenazas que pueden generar daños financieros, robos de identidad , bancarios o personales.
- Para el año 2022, los ataques de Phishing son la segunda causa mas común de vulneración, se tuvo un total de \$4.91 millones de dólares basado en el informe de Cost of a Data Breach Report de

IBM



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

# 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, los cuales aprenderán en base a un conjunto de características basadas en Indicadores de Compromiso (IOC) 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 indicadores de compromiso aplicando Machine Learning para mejorar la seguridad en la red al proteger información sensible: Caso Práctico Phishing Google Chrome.



# Objetivos Específicos



Analizar el estado del arte sobre indicadores de compromiso y como estos pueden ayudar para la prevención de intrusos en paginas o sitios web, apoyado por phishing en motores de búsqueda- Google Chrome

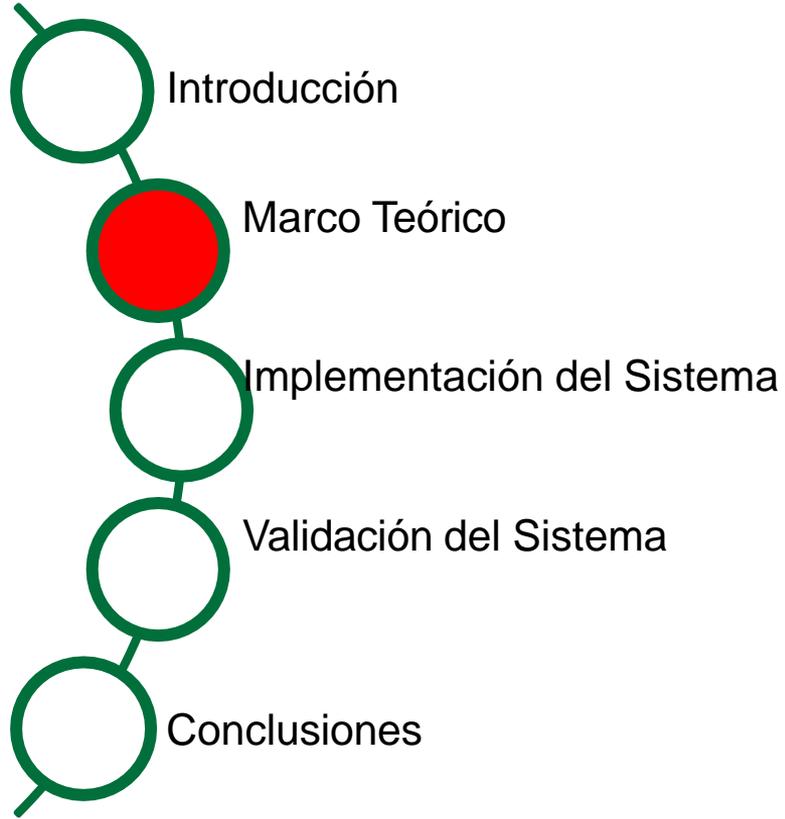


Desarrollar una extensión de Google Chrome utilizando técnicas de Machine Learning para mejorar la prevención y gestión de seguridad en sitios web



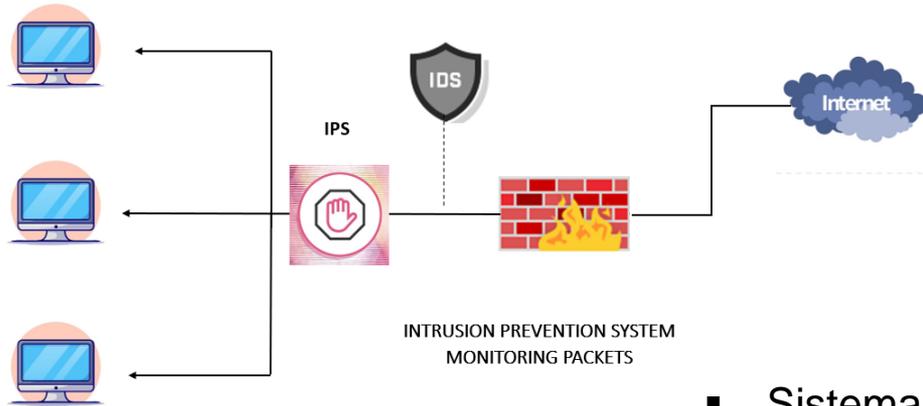
Comprobar los resultados obtenidos, analizar y ajustar los errores encontrados en los indicadores de compromiso del sistema de prevención de intrusos





# Sistema de Prevención de Intrusos (IPS)

- Sistema de software o hardware que identifica y previene actividades maliciosas.



- Un IPS requiere verificar la detección de un ataque para su respectivo bloqueo. .

- Sistema de prevención de intrusos basados en firmas (SIDS).

- Sistema de prevención de intrusos basado en anomalías (AIDS).



# Phishing (Ciber-ataque )

- Pretende robar información privada, posiblemente con fines ilegales.



- Técnica de Ingeniería social

- Los sitios web con phishing han evolucionado para no ser identificados.

# Características para la prevención de intrusos – Phishing

- Se determinaron los recursos de comprobación basados en Indicadores de Compromiso con la ayuda de una revisión de la literatura.
- Se seleccionaron 40 características: 30 características basadas en el contenido del sitio web y en la URL y 10 características basadas en los IOC



# Indicadores de Compromiso (IOC)

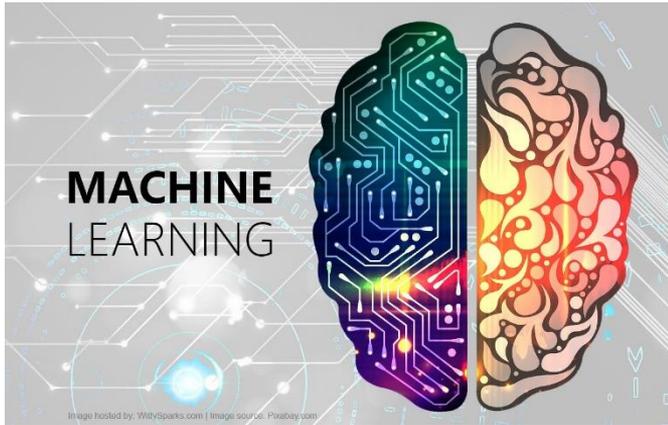


Son métricas o señales que indican la presencia de una brecha de seguridad o una posible intrusión en un sistema o aplicación.

Son fundamentales para prevenir actividades maliciosas.



# Modelos y/o algoritmos de Machine Learning



Su propósito es capacitar a computadoras para que puedan adquirir conocimiento a partir de un conjunto grande de datos, con el fin de la toma de decisiones (predecir o clasificar información) por si sola sin la necesidad de programarlas.



# Modelos y/o algoritmos de Machine Learning

Algoritmo de aprendizaje supervisado. Alcanza una precisión máxima de 72% en la detección de phishing usando IOC

**Decision Tree**



Algoritmo de aprendizaje supervisado. Alcanza una precisión máxima de 83% en la detección de phishing usando IOC

**Random Forest**



Clasificador meta-estimador. Alcanza una precisión máxima del 83,58% en la detección de phishing usando IOC

**Ada Boost**



Algoritmo de aprendizaje supervisado. Alcanza una precisión máxima del 84.66% en la detección de phishing usando IOC

**Redes Bayesianas**



Algoritmo de aprendizaje supervisado. Alcanza el 82,86% en la detección de phishing usando IOC

**Support Vector Machines**



Algoritmo optimizador. Alcanza el 84,8% en la detección de phishing usando IOC

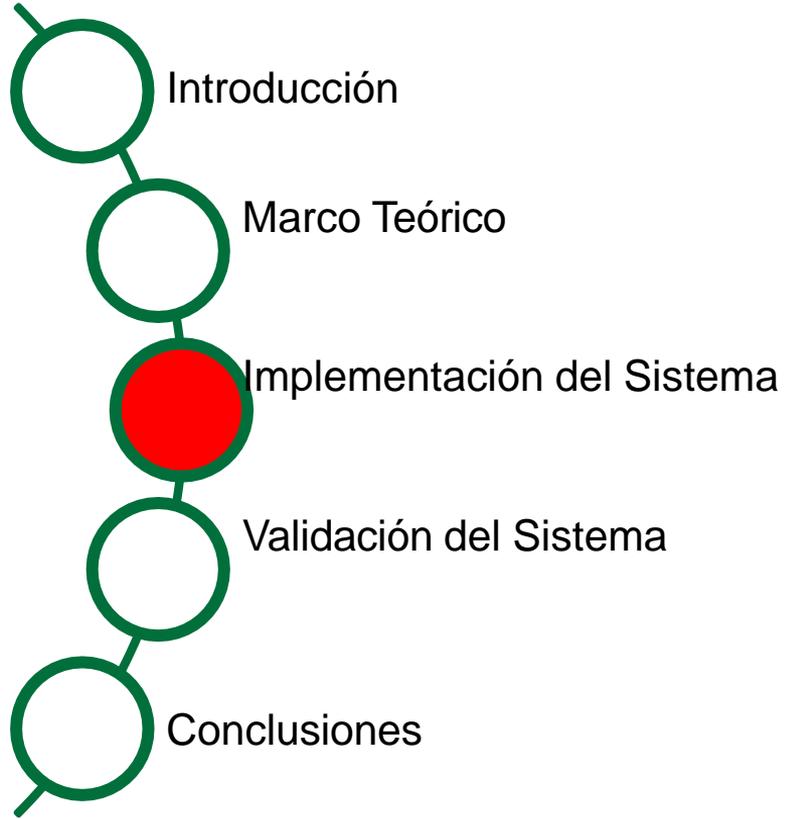
**Naïve Bayes**



# Extensiones Google Chrome

- Son pequeñas aplicaciones desarrolladas para mejorar la funcionalidad y personalización del navegador web Google Chrome
- Google Chrome es el navegador más usado.
- Permite adaptar al navegador a sus necesidades específicas





# Análisis del sistema

- Historias de Usuario:



## Historia de usuario 01

**Quiero** una extensión para el navegador Google Chrome que pueda proporcionarme información acerca de la presencia de phishing en un sitio web. Además, incorporar métodos específicos de prevención de ataques Phishing mediante IPS, detección basada en firmas y anomalías

**Para** disponer de un método específico de prevención de ataques phishing, mediante IPS, detección basada en firmas y anomalías con el objetivo de aumentar protección y reducir la probabilidad de ser víctimas de ataques.



# Lista de Tareas



1

LA EXTENSIÓN UTILIZA EL ALGORITMO Y/O MODELO MÁS EFECTIVO DE MACHINE LEARNING PARA DETECTAR EL PHISHING EN SITIOS WEB.

2

SE CREA EL DATASET QUE INCLUYE CARACTERÍSTICAS CON INDICADORES DE COMPROMISO QUE POSIBILITEN LA IDENTIFICACIÓN DE SITIOS WEB CON PHISHING DE LOS SITIOS LEGÍTIMOS.

3

EL MODELO DE MACHINE LEARNING SE ALOJA EN UN SERVIDOR PARA QUE PUEDA LLEVAR A CABO LAS PREDICCIONES MEDIANTE UN SERVICIO.



# Diseño del sistema

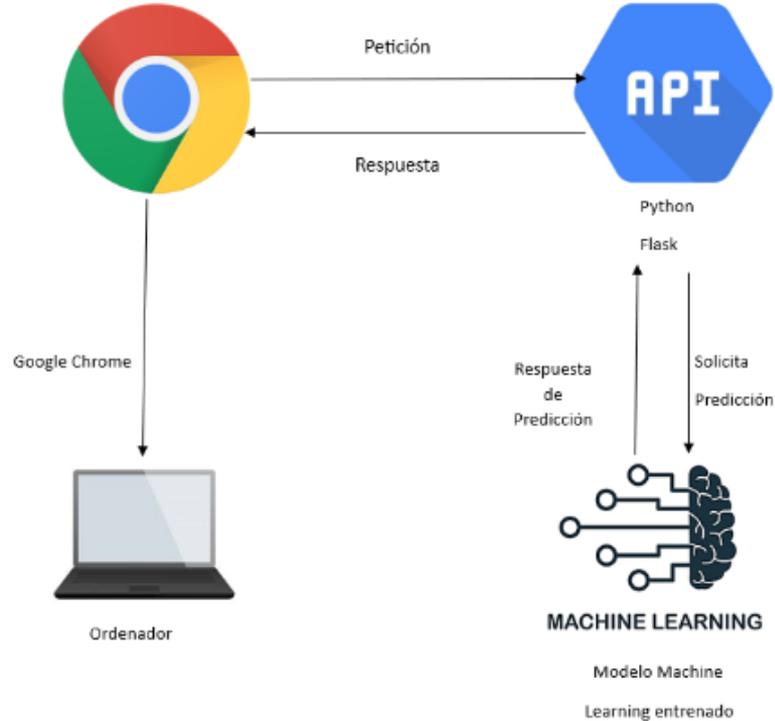
- Arquitectura Lógica con las tecnologías a usar.

		Tecnologías			
		HTML	CSS	JS	
Capa de Presentación	Front-End				- HTML - CSS - JavaScript
Capa Lógica de Negocio	Back-End				- JavaScript
Capa de Infraestructura	Modelo				- SAV File
					
	Servicio				- Python - Flask
 python™  <b>Flask</b>					



# Diseño del sistema

- Arquitectura Física



# Diseño del sistema

- Mockups



Preempt Phishing



Analizando..



Preempt Phishing



El sitio web es legítimo



Preempt Phishing



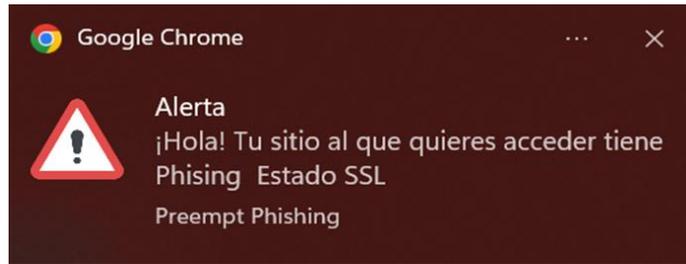
El sitio web tiene phishing



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

# Diseño del sistema

- Mockups



# Desarrollo del Sistema

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

Algoritmos/Modelos	Accuracy	Precision	Recall	f1
Random Forest	0,8400	0,8572	0,9630	0,9000
Multi-layer Perceptron classifier	0,7957	0,8466	0,9074	0,8717
Decision Tree	0,8132	0,8515	0,9289	0,8867
Ada Boost	0,6864	0,8358	0,9096	0,8678
SVM	0,7794	0,8286	0,9088	0,8607
Mezcla de Gaussianas – GMM	0,6094	0,9113	0,8482	0,8747
Naive Bayes	0,2139	0,0330	0,6864	0,04896
Redes Bayesianas	0,2096	0,0428	0,6677	0,0539
Redes Multicapa: MLP	0.8001	0,9154	0,8472	0,8763



# Desarrollo del Sistema

- Resultado del Sprint 2: Creación del Dataset

-1  
Phishing

1  
Legítimo

Ord.	havelp	lengthUrl	haveAtSymbol	sslState	domainAge	slashDouble
0	1	1	1	1	1	-1
1	1	1	1	1	1	-1
2	1	1	1	1	1	-1
3	1	1	-1	1	1	-1
4	1	1	1	1	1	-1
5	1	1	1	1	1	-1

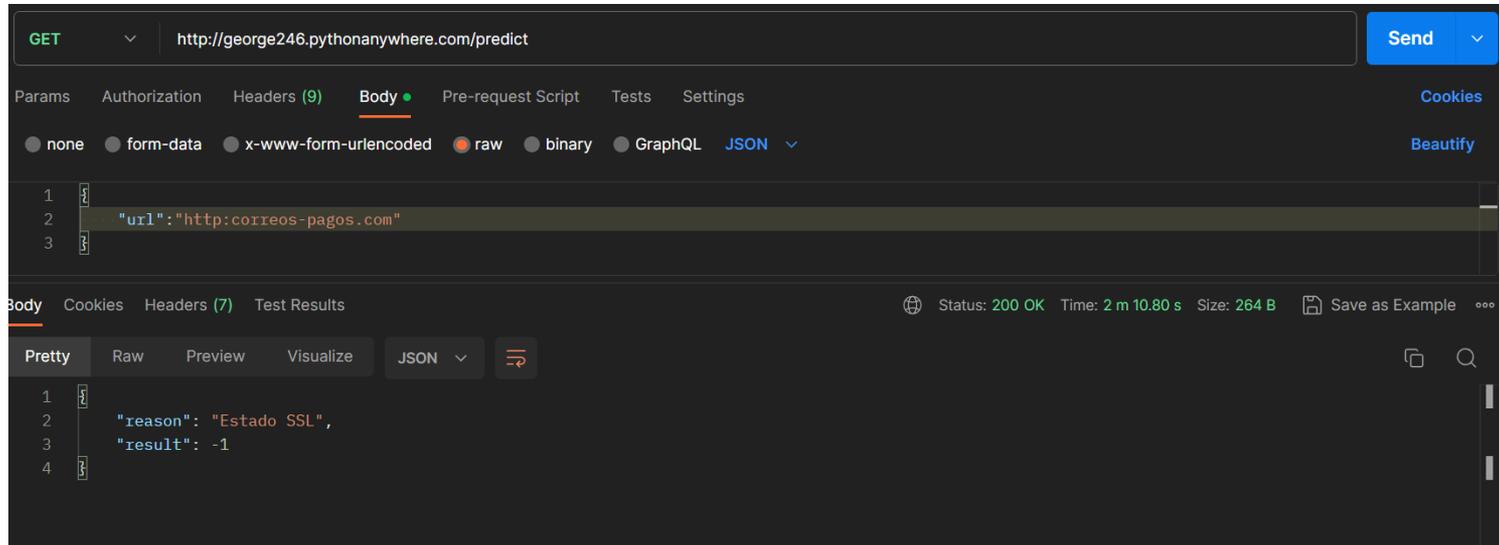
Características



# Desarrollo del Sistema

- Resultado del Sprint 3: Creación de la API

Sitio web con Phishing



The screenshot shows a REST client interface with the following details:

- Method:** GET
- URL:** http://george246.pythonanywhere.com/predict
- Body (Request):**

```
{
  "url": "http://correos-pagos.com"
}
```
- Status:** 200 OK
- Time:** 2 m 10.80 s
- Size:** 264 B
- Body (Response):**

```
{
  "reason": "Estado SSL",
  "result": -1
}
```



# Desarrollo del Sistema

- Resultado del Sprint 3: Creación de la API



Sitio web Legítimo

The screenshot displays a REST client interface with the following details:

- Method:** GET
- URL:** `http://george246.pythonanywhere.com/predict`
- Body:** `{"url": "https://www.google.com"}`
- Response:** `{"reason": "Clic Derecho", "result": 1}`
- Status:** 200 OK
- Time:** 2 m 10.98 s
- Size:** 265 B



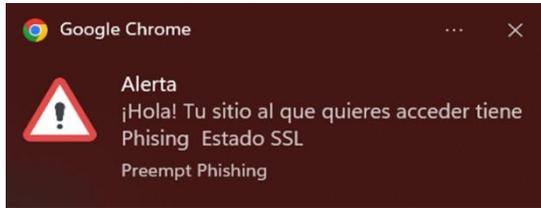
# Desarrollo del Sistema

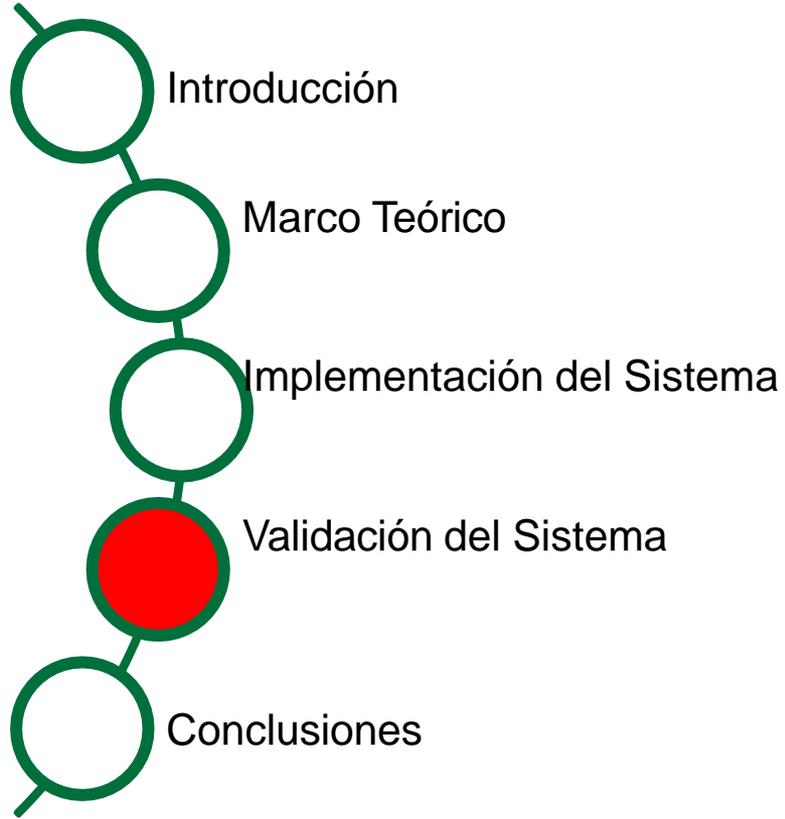
- Resultado del Sprint 4: Desarrollo de la Extensión de Google Chrome



# Desarrollo del Sistema

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





# Validación del Sistema

- Uso de la herramienta Zphisher (ambiente simulado)



```
klxm05@kalixm: ~/zphisher
File Actions Edit View Help

Zphisher
Version : 2.3.4

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook           [11] Twitch              [21] DeviantArt
[02] Instagram          [12] Pinterest           [22] Badoo
[03] Google              [13] Snapchat            [23] Origin
[04] Microsoft           [14] LinkedIn            [24] DropBox
[05] Netflix             [15] Ebay                [25] Yahoo
[06] Paypal              [16] Quora               [26] Wordpress
[07] Steam               [17] Protonmail          [27] Yandex
[08] Twitter             [18] Spotify             [28] StackoverFlow
[09] Playstation        [19] Reddit              [29] Vk
[10] Tiktok               [20] Adobe               [30] XBOX
[31] Mediafire           [32] Gitlab              [33] Github
[34] Discord

[99] About              [00] Exit

[-] Select an option : █
```



# Validación del Sistema

- Uso de la herramienta MaxPhiser (ambiente simulado)



```

[-----]
[ M A X P H I S E R ]
[-----]
[By KasRoudra]
[v1.1]

[01] Facebook Traditional   [27] Reddit                 [53] Gitlab
[02] Facebook Voting       [28] Adobe                   [54] Github
[03] Facebook Security    [29] DevianArt               [55] Apple
[04] Messenger             [30] Badoo                   [56] iCloud
[05] Instagram Traditional [31] Clash Of Clans         [57] Vimeo
[06] Insta Auto Followers  [32] Ajio                    [58] Myspace
[07] Insta 1000 Followers  [33] JioRouter               [59] Venmo
[08] Insta Blue Verify     [34] FreeFire                [60] Cryptocurrency
[09] Gmail Old              [35] Pubg                    [61] SnapChat2
[10] Gmail New              [36] Telegram                [62] Verizon
[11] Gmail Poll             [37] Youtube                 [63] Wi-Fi
[12] Microsoft              [38] Airtel                  [64] Discord
[13] Netflix                [39] SocialClub              [65] Roblox
[14] Paypal                 [40] Ola                     [66] UberEats
[15] Steam                  [41] Outlook                 [67] Zomato
[16] Twitter                [42] Amazon                  [68] WhatsApp
[17] PlayStation            [43] Origin                  [69] PhonePay
[18] TikTok                 [44] DropBox                 [70] MobikWik
[19] Twitch                 [45] Yahoo                   [71] FlipCart
[20] Pinterest              [46] WordPress               [72] Teachable
```



# Validación del Sistema

- Proceso de ejecución de pruebas



Con el MaxPhisher generamos el ataque Phishing



Con la extension Google Chrome se escanea el ataque y lo verifica



Se guarda los resultado obtenidos



# Validación del Sistema MaxPhisher

- Se probó con 102 sitios web: 51 sitios web con phishing y 51 sitios web legítimos.

SITIO WEB	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING		PRUEBAS SITIOS WEB LEGÍTIMOS	
		RESULTADO ESPERADO	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Netflix	Tradicional Login Page	Phishing	Phishing	Legítimo	Phishing



# Validación del Sistema Zphisher



- Se probó con 70 sitios web: 35 sitios web con phishing y 35 sitios web legítimos.

SITIO WEB	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING		PRUEBAS SITIOS WEB LEGÍTIMOS	
		RESULTADO ESPERADO	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Netflix	Tradicional Login Page	Phishing	Phishing	Legítimo	Legítimo



# Validación del Sistema



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

The image shows a browser window displaying the Netflix login page. The URL is `netflix.com/ec/login`. The page features a grid of movie and TV show thumbnails in the background. In the center, there is a login form with the heading "Inicia sesión". The form includes input fields for "Email o número de teléfono" and "Contraseña", a red "Iniciar sesión" button, and a "Recuérdame" checkbox. Below the form, there is a link for "¿Primera vez en Netflix? Suscríbete ahora" and a reCAPTCHA notice: "Esta página está protegida por Google reCAPTCHA para comprobar que no eres un robot. Más info." A white security overlay titled "Preempt Phishing" is positioned in the upper right of the browser window. It features a green checkmark icon and the text "El sitio web es legítimo".



# Validación del Sistema



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

The screenshot shows a web browser window with the address bar displaying `sip-motorola-lauren-explicit.trycloudflare.com/login.html`. The main content is a Netflix login page with the "NETFLIX" logo and a "Sign In" form. The form includes fields for "Email" and "Password", a "Sign In" button, a "Remember me" checkbox, and a "Login with Facebook" link. A "Preempt Phishing" alert is overlaid on the page, featuring a warning icon and the text "El sitio web tiene phishing". A Chrome notification bubble is also visible, stating "Alerta ¡Hola! Tu sitio al que quieres acceder tiene Phising Edad del Dominio Preempt Phishing".



# 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	FÓRMULA
ACCURACY	$\frac{VP + VN}{VP + VN + FP + FN}$
PRECISION	$\frac{VP}{VP + FP}$
RECALL	$\frac{VP}{VP + FN}$
F1	$F1 = 2 * \frac{\textit{precisión} * \textit{recall}}{\textit{precisión} + \textit{recall}}$



# Validación del Sistema



- Obtención de las métricas de evaluación

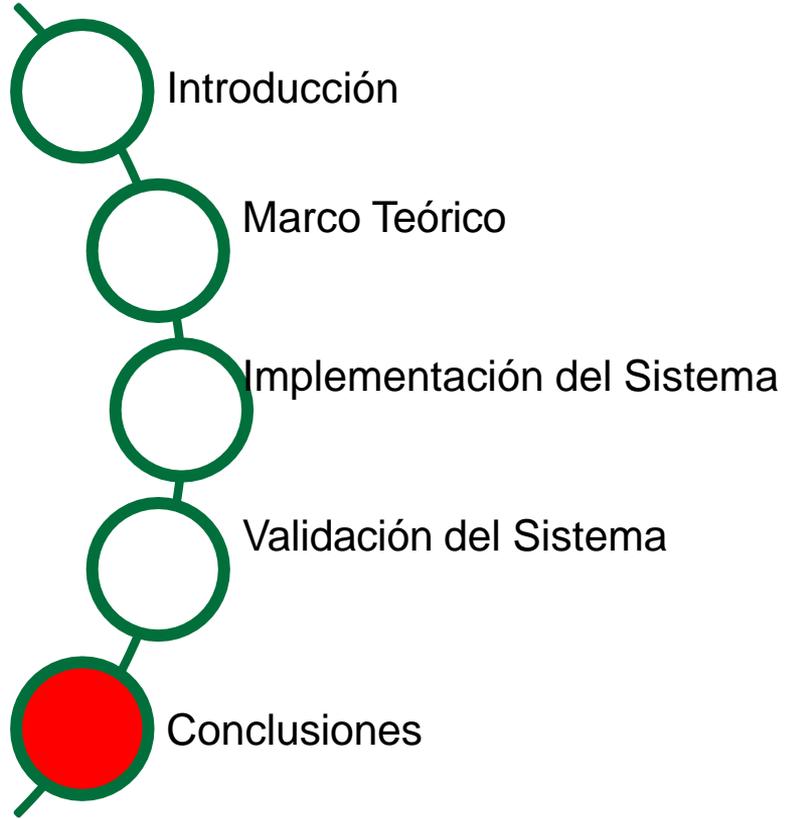
CAMPO DE ENTRENAMIENTO				CAMPO SIMULADO/REAL				
ACCURACY	PRECISION	RECALL	F1	ACCURACY	PRECISION	RECALL	F1	
84%	85.72%	96.3%	90%	Zphihser	84%	82%	85%	83%
				MaxPhiser	86%	92%	82%	86%





- Se probó en un campo simulado/real con Zphisher y MaxPhisher.
- Se obtuvo en la métrica Accuracy el valor más alto de 86% y el más bajo con 84%, valores que están aproximadamente dentro de los valores encontrados en la literatura (83%) de Accuracy (Noor et al., 2019) respectivamente. Por lo tanto, el IPS implementado para evitar ataques Phishing presenta resultados que están dentro del rango aceptable de predicciones.





# Conclusiones

El IPS desarrollado (Preempt Phishing) se entrenó con un dataset de 13,192 sitios web (3,987 sitios web con Phishing (30,22%) y 9,205 sitios web legítimos (69,78%) ).

Se diseñó e implementó un sistema de prevención de Phishing.

Para validar el IPS (Preempt Phishing) implementado se utilizó las herramientas Zphiser y MaxPhiser



# Conclusiones

Utilización de Indicadores de Compromiso para la obtención respectiva en las URL ingresadas para mejorar efectividad en la precisión.

La extensión desarrollada se coloca en marcha en un entorno real, por lo cual para el mejoramiento de la misma se debe de usar un conjunto de datos (datasets) actualizados y realizar el mismo procedimiento.





- Noor, U., Anwar, Z., Amjad, T., y Choo, K. K. R. (2019). A machine learning based FinTech cyber threat attribution framework using high-level indicators of compromise. Future Generation Computer Systems, 96, 227-242



Gracias por su  
atención