Sistema de prevención de intrusos en sitios web, usando modelos y/o algoritmosde Machine Learning: caso práctico Phishing Google Chrome

Semblantes Lozada, Geraldyn Nicol

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Software

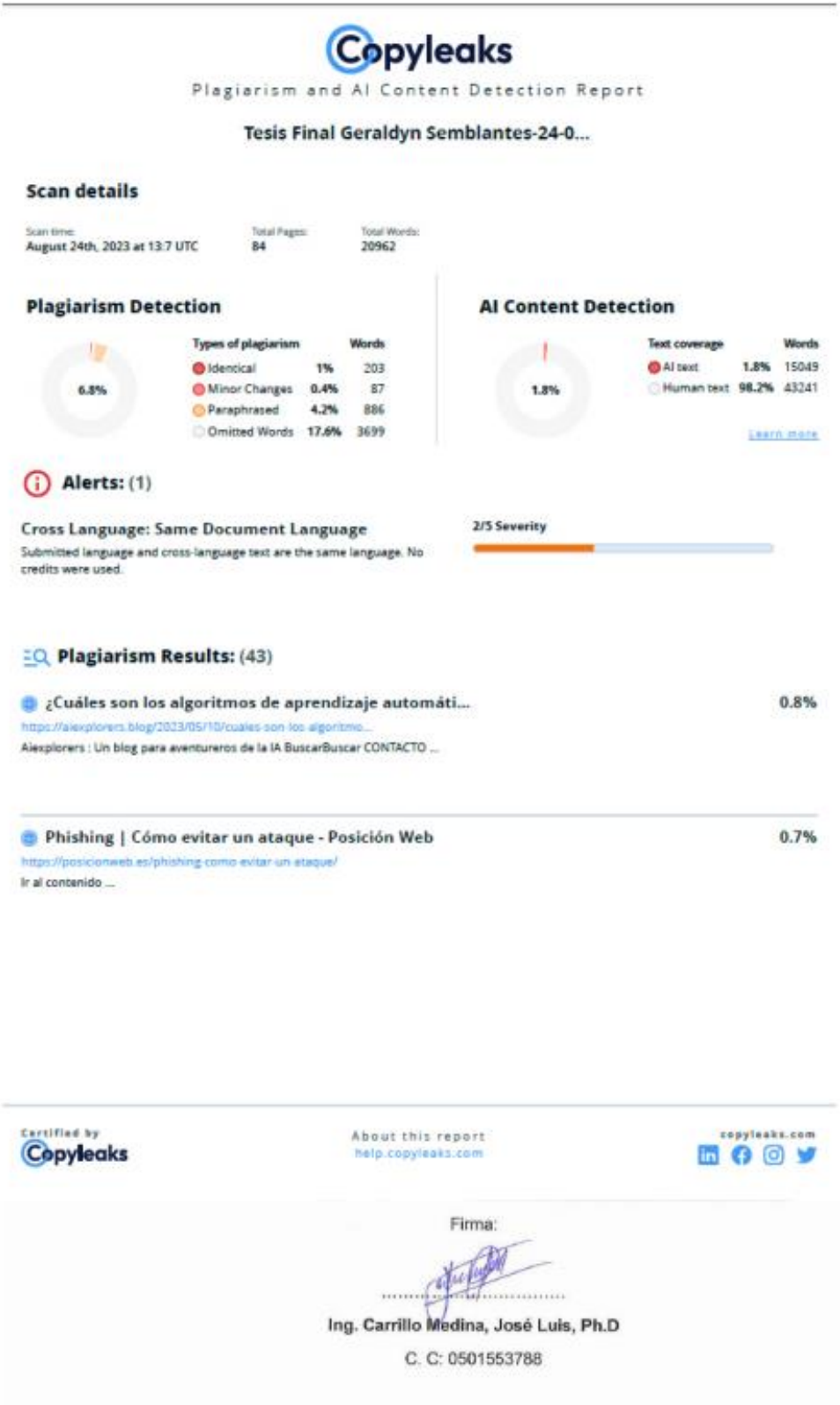
Trabajo de integración curricular, previo a la obtención del título de Ingeniera de Software

Ing. Carrillo Medina, José Luis, Ph.D

24 de agosto del 2023

Latacunga

Reporte de Verificación de Contenido



Copyleaks

Plagiarism and AI Content Detection Report

Tesis Final Geraldyn Semblantes-24-0...

Scan details

Scan time: August 24th, 2023 at 13:7 UTC | Total Pages: 84 | Total Words: 20962

Plagiarism Detection

6.8%

Types of plagiarism		Words
Identical	1%	203
Minor Changes	0.4%	87
Paraphrased	4.2%	886
Omitted Words	17.6%	3699

AI Content Detection

1.8%

Text coverage		Words
AI text	1.8%	15049
Human text	98.2%	43241

Learn more

Alerts: (1)

Cross Language: Same Document Language

Submitted language and cross-language text are the same language. No credits were used.

2/5 Severity

Plagiarism Results: (43)

¿Cuáles son los algoritmos de aprendizaje automáti... 0.8%

https://alexplorers.blog/2023/05/10/cuales-son-los-algoritmo...

Alexplorers : Un blog para aventureros de la IA BuscarBuscar CONTACTO ...

Phishing | Cómo evitar un ataque - Posición Web 0.7%

https://posicionweb.es/phishing-como-evitar-un-ataque/

Ir al contenido ...

Certified by Copyleaks | About this report help.copyleaks.com | copyleaks.com

Firma:

Ing. Carrillo Medina, José Luis, Ph.D

C. C: 0501553788

Departamento de Ciencias de la Computación

Carrera de Ingeniería en Software

Certificación

Certifico que el trabajo de integración curricular: "**Sistemas de prevención de intrusos en sitios web, usando modelos y/o algoritmos Machine Learning: Caso práctico Phishing Google Chrome**" fue realizado por la señorita **Semblantes Lozada, Geraldyn Nicol;** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Latacunga, 24 de agosto del 2023

Firma:

.....

Ing. Carrillo Medina, José Luis, Ph.D

C. C: 0501553788

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Software

Responsabilidad de Autoría

Yo, **Semblantes Lozada, Geraldyn Nicol**, con cédula de ciudadanía n° 0503132995, declaro que el contenido, ideas y criterios del trabajo de integración curricular: "**Sistemas de prevención de intrusos en sitios web, usando modelos y/o algoritmos Machine Learning: Caso práctico Phishing Google Chrome**", es mi de autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas

Latacunga, 24 de agosto de 2023

Firma:

.....

Semblantes Lozada, Geraldyn Nicol

C.C.: 0503132995

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Software

Autorización de Publicación

Yo **Semblantes Lozada, Geraldyn Nicol**, con cédula de ciudadanía n°0503132995, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de integración curricular: "**Sistemas de prevención de intrusos en sitios web, usando modelos y/o algoritmos Machine Learning: Caso práctico Phishing Google Chrome"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Latacunga, 24 de agosto del 2023

Firma

.....

Semblantes Lozada, Geraldyn Nicol

C.C.:0503132995

Dedicatoria

Quiero dedicar este proyecto a mis padres, José y Victoria, y a toda mi familia que me ha apoyado en cada uno de mis pasos académico, siendo un apoyo y motivación para seguir adelante.

También dedico este trabajo a mis compañeros, que me han ayudado y confiado en mi durante estos años de vida universitaria.

Y dedico este trabajo de titulación al ingeniero José Carrillo, quien me ha guiado y aconsejado durante toda la realización de este proyecto.

Geraldyn Nicol Semblantes Lozada

Ecuador, agosto de 2023

Agradecimiento

Empiezo expresando gratitud a Dios por ayudarme en cada paso que doy en mi vida. Tengo que agradecer a mis padres, José Semblantes y Victoria Lozada, por enseñarme el valor de la responsabilidad, la constancia y el esfuerzo, y por ser una ayuda en la totalidad de mis minutos problemáticos. Ellos son la explicación de cada una de mis victorias.

También quiero dar las gracias a mis compañeros por los buenos momentos que pasamos en la universidad, por las risas y por las tardes compartidas. Estoy muy agradecida con ustedes por haber hecho de mi vida universitaria no sólo un periodo de estudio, sino también de euforia y juerga.

Doy las gracias a cada uno de los profesores que me han enseñado durante estos ocho semestres de estudio, gracias por prepararme para ser un estudiante decente. Les doy las gracias por haberme formado de manera experta y con valores para ser un individuo que aporte a la sociedad. Particularmente al diseño José Carrillo necesito ofrecer mi agradecimiento por ofrecerme la oportunidad de ser parte de este proyecto. Su recomendación, dirección y devoción han sido imprescindible para su finalización.

Geraldyn Nicol Semblantes Lozada

Ecuador, agosto de 2023

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

Con el uso expansivo de internet en los últimos años, los usuarios deben tener una conciencia de seguridad para evitar ataques por parte de intrusos en la red, estos son denominados ciberataques. Un ciberataque muy común hoy en día es el phishing, este tipo de ataque puede poner en riesgo la integridad y datos confidenciales de los usuarios. La ciberseguridad ha ido evolucionando hasta los días de hoy en donde el Machine Learning entra como un actor principal, este se utiliza como un instrumento fundamental para reconocer y eliminar los peligros que se encuentra en la red como el phishing. Así pues, este proyecto se centra en la creación de un Sistema de prevención (IPS) que utiliza modelos de Machine Learning o cálculos potenciales para prevenir el phishing en forma de una extensión de Google Chrome, siguiendo una filosofía de mejora rápida Scrum para su desarrollo e implementación. Además, se hizo empleo de dos herramientas de simulación phishing Zphisher y Pyphisher para realizar pruebas al sistema, tanto en entornos contralados como en entornos reales con el fin de garantizar la efectivad del sistema. Los resultados obtenidos presentan niveles de aceptación dentro de los rangos investigados en la revisión literaria inicial.

Palabras clave: Machine Learning, sistema de prevención de intrusos, phishing, sitios web.

Abstract

With the expansive use of the Internet in recent years, users must have a security awareness to avoid attacks by intruders on the network, these are called cyber-attacks. A very common cyber-attack nowadays is phishing, this type of attack can jeopardize the integrity and confidential data of users. Cybersecurity has been evolving until today where Machine Learning enters as a major player, this is used as a fundamental tool to recognize and eliminate the dangers found on the network such as phishing. Thus, this project focuses on the creation of a Prevention System (IPS) that uses Machine Learning models or potential calculations to prevent phishing in the form of a Google Chrome extension, following a Scrum rapid improvement philosophy for its development and implementation. In addition, two phishing simulation tools Zphisher and Pyphisher were used to test the system, both in controlled environments and in real environments in order to ensure the effectiveness of the system. The results obtained show acceptance levels within the ranges investigated in the initial literature review.

Key words: Machine Learning, intrusion prevention system, phishing, web sites.

Capítulo I

Introducción

Propósito y contextualización del tema

En los últimos años, la tecnología e internet se han convertido en una parte integral de la vida cotidiana. Actualmente, hay millones de usuarios en Internet, pero no hay garantías de uso continuo de Internet. La seguridad tiene sus propios riesgos, ya que los usuarios pueden ser muy vulnerables a muchas amenazas en línea (ataques cibernéticos).

El ataque más común hoy en día es el phishing, un tipo de ataque en el que los usuarios son engañados por correos electrónicos, sitios web, etc. fingiendo ser legítimos para obtener información de sus credenciales (Watson *et al.*, 2005).

Entre tipos de ataques Phishing relevantes encontramos: i) El ataque *Phishing de identidad* hace que el usuario entregue sus credenciales a los intrusos, esto pone en riesgo su seguridad y confidencialidad, a través de sitio engañosos (MacKay, 2018). ii) Uso de *correos electrónicos falsos*, en donde el atacante intenta convencer al usuario a través un correo falso que se trata legítimo mediante pequeñas modificaciones (IT Digital Media Group, 2018).

En 2021, el costo medio pagado por las empresas estadounidenses fue de 14,8 millones de dólares, en comparación con los 3,8 millones de dólares en 2015. La restauración de correos electrónicos comerciales comprometidos (BEC) cuesta unos 6 millones de dólares cada año, con 1,17 millones dedólares en pagos ilegales a los atacantes. Por otro lado, el coste deproteger credenciales contra ataques Phishing se ha disparado, aumentando de 382.920 dólares en 2015 a 692.531 dólares en 2021 (Jones, 2021).

Hoy en día, los ciberataques han vuelto extremadamente preocupantes, especialmente

aquellos que tienen como objetivo el robo de datos sensibles, estos ataques conllevan riesgos significativos a la seguridad como: i) El robo de cuentas bancarias, ii) Extorsión, iii) Venta ilegal de información personal entre otros. Según los datos proporcionados por el Instituto Infosec, la cantidad de ataques de phishing ha aumentado desde 2016 (Moramarco, 2016).

Esto ha provocado un aumento de la complejidad de la metodología habitual de los atacantes. Los mensajes, sitios o correos utilizados en estos ataques suelen parecerse a los de las asociaciones auténticas, lo que hace mucho más difícil protegerse contra este tipo de peligro (Ollmann, 2004).

Debido a esto, se han implementado la ciberseguridad que según Asmaa y el profesor Sharada (2021), la ciberseguridad de se refiere a las acciones y prácticas utilizadas para proteger los sistemas, las redes y los datos de posibles ataques cibernéticos, esta incluye la adopción de políticas, procedimientos y tecnologías que buscan detectar, prevenir y responder a ataques o intrusiones.

Así han surgido, algunos sistemas de técnicas contra del phishing, por ejemplo, a) Identificación de asaltos de phishing mediante estrategias dinámicas, b) Descubrimiento y anticipación de ataques de phishing mediante IDS e IPS, c) Barra de herramientas de seguridad del servidor web, d) Phishing Honeypots, entre otras (Adil *et al.*, 2020). Uno de ellos son el sistema de detección de intrusos (IDS) es un software que detecta tráfico de red dañino, no autorizado o malicioso (Balamurugan & Saravanan, 2019). El objetivo de la detección de intrusos es proporcionar supervisión, auditoría, análisis forense y notificación de actividades maliciosas en la red.

En términos sencillos, se puede indicar que los IDS pueden ser perfectamente adecuados para supervisar los ataques a la red y alertar a los administradores de las amenazas emergentes, sin

embargo, debido a su velocidad, rendimiento y limitaciones pasivas, los sistemas de seguridad tradicionales han dejado una brecha abierta, lo que ha permitido a los Sistemas de Prevención de Intrusiones (IPS) surgir como la principal arma de defensa proactiva (Koziol, 2003).

Un sistema de prevención de intrusos (IPS) no sólo identifica la información maligna provocada por malware, botnets, infecciones y ataques designados, sino que también puede hacer todo lo posible para prevenir el riesgo para los clientes web (Fortinet, 2023). Entre las funciones claves que realiza un IPS son: i) Detectar y tomar acciones preventivas contra ataques maliciosos, ii) Detener el ataque por sí mismo, iii) Mejorar el entorno de seguridad, iv) Modificar el contenido del ataque (Chakraborty, 2013).

El principal motivo de los atacantes es hacerse con datos sensibles o propiedad intelectual, por lo que les interesa todo lo que puedan obtener de los datos de los clientes, como información de los empleados, registros financieros, etc. El IPS está especificado para proporcionar protección a los activos, recursos, datos y redes (Asmaa & Prof. Sharad, 2021).

Los IPS no sólo detectan Sitios Web y correo electrónico maliciosos, sino que también, bloquean los sitios que contienen información maliciosa y los denuncia, con la finalidad de mitigar la amenaza y proteger la información personal del usuario (Ollmann, 2004).

IPS puede ser aludido como la expansión de IDS con actividades de control de acceso para salvaguardar los PCs del abuso. El IPS es una respuesta inteligente para identificar y prevenir actividades malintencionadas, protegiendo tanto al cliente como a la organización. Estos impiden que los intrusos accedan a datos delicados sobre un cliente o asociación para garantizar su confidencialidad y reducir la posibilidad de tergiversación u otros resultados relacionados con un ciberataque (Hr *et al*., 2020).

En términos sencillos, los IDS podrían ser completamente satisfactorios para observar los ataques a organizaciones y hacer que los clientes sean conscientes de los peligros presentes, sin embargo, su velocidad, ejecución y restricciones han dado paso a los IPS como arma de protección proactiva contra los peligros en desarrollo producidos por las nuevas innovaciones por los nuevos avances (Hr *et al*., 2020).

Los IPS de Phishing incorporan el curso tanto de la identificación de ejercicios de interrupción o peligros como de la supervisión de las actividades de reacción sobre estos peligros digitales (Hr *et al*., 2020).

Justificación e Importancia

Los ataques de phishing siguen siendo una de las amenazas más comunes y peligrosas en el Internet. Los agresores están utilizando técnicas cada vez más complejas para engañar a los clientes de la Web para que tomen datos delicados, por ejemplo, datos de inicio de sesión, cuentas bancarias y números tarjetas como de Mastercard y de Visa.

Según un informe de la empresa de seguridad de redes Symantec, en 2021, se impidieron más de 5.800 millones de asaltos phishing y se reconocieron más de 400.000 sitios de phishing mes a mes en 2021 (Symantec, 2021).

Los ataques de phishing se llevan a cabo a través de correos electrónicos, mensajes de texto, publicaciones en redes sociales y sitios web falsos que simulan ser legítimos para engañar a los usuarios y hacerles revelar su identidad, los usuarios de Internet deben tener cuidado y tomar medidas para protegerse contra este tipo de amenazas (Chong & Shim, 2019).

Desarrollar una extensión de Google Chrome para prevenir los ataques de phishing es

básico para combatir contra estos peligros digitales. Esta ampliación ofrece seguridad proactiva, formación, actualizaciones constantes, similitud y seguridad tanto a nivel individual como corporativo.

> La importancia de una extensión de Google Chrome para contrarrestar los ataques de phishing radica en varios puntos de vista clave, por ejemplo, i) Trabajar en la seguridad las extensiones proporcionan una defensa adicional contra el Phishing y ayudan a los usuarios a identificar y evitar Sitios Web maliciosos (Wanget *et. al.,* 2019). ii) Una advertencia temprana y una identificación proactiva, una extensión IPS contra el phishing puede distinguir y hacer que los clientes sean conscientes de posibles sitios de phishing de forma progresiva (Kumar *et al.*, 2020).
>
> Las extensiones de los navegadores de Internet pueden ofrecer datos lógicos y alarmas visuales que ayuden a los usuarios a reconocer los aspectos dudosos de los sitios y a actuar con prudencia (Williams *et al.*, 2019).

La propuesta de una extensión de Google Chrome destinada a contrarrestar los ataques de phishing es de suma importancia en el entorno web actual. Esta ampliación permitiría detectar y controlar sitios web engañosos que buscan imitar a los reales para adquirir datos delicados, por ejemplo, contraseñas, cuentas bancarias y otra información privada.

Objetivos

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 deldesarrollo 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

Metodología

El objetivo principal de este proyecto es construir un sistema de prevención de phishing en sitios web utilizando modelos y/o algoritmos de Machine Learning: Google Chrome Phishing Case Study, para este fin el método utilizado en este proyecto consta de tres etapas.

En la primera etapa del proyecto, se realizará un estudio de la literatura pertinente al tema para fomentar un marco teórico para examinar qué son los sistemas de prevención de intrusos (IPS), su funcionamiento y su motivación. Del mismo modo, probar y comprobar los modelos y/o algoritmos de Machine Learning. Para llevar a cabo esta etapa, se inspecciona el conjunto de datos de referencia y contenido de SCOPUS para obtener la información esperada.

En la segunda etapa se implementa la extensión IPS observando tres funcionalidades puntuales que debe cumplir el sistema: i) La primera permite notificar al usuario si el sitio web contiene Phishing o es Legítima, ii) La segunda notifica cual es la característica encontrada para determinar dicho ataque, iii) Y la tercera el bloqueo del sitio web y su cierre. Estas características se desarrollan utilizando recursos de verificación (conjuntos de datos) que permiten a los modelos y/o algoritmos aprender si un sitio web es legítimo o no. El dataset utilizado inicialmente proviene del estudio "Sistema de detección de intrusos

para sitios web, utilizando modelos y/o algoritmos de Machine Learning: Phishing Google Chrome case study" (Castillo Veloz & Chuquitarco Velasco, 2023), así como también, se creará un nuevo dataset. Los modelos y/o algoritmos de aprendizaje automático son obtenidos de la investigación planteada en la primera fase, mismos que al ponerlos a prueba, se selecciona el que ofrece el mejor rendimiento de acuerdo con las funcionalidades establecidas en la implementación de la extensión IPS. También se generará un nuevo dataset, el cual será agregado al dataset inicial del estudio anterior, para le mejora de predicción del sistema y que permitan aprender al modelo seleccionado a prevenir ataques Phishing en sitios web. Se hará uso de la plataforma de Data Science Kaggle para encontrar el conjunto de datos que se adapte mejor al sistema.

En la tercera etapa, se lleva a cabo una evaluación del aplicativo utilizando ambientes controlados y reales. El objetivo principal es validar los resultados obtenidos, esta evaluación garantiza la adecuación y productividad del IPS antes de su ejecución.

Capítulo II

Marco Teórico

En este capítulo se lleva a cabo una investigación teórica sobre los sistemas de prevención de intrusos (IPS), los factores de compromiso (características), los modelos y/o algoritmos de Machine Learning utilizados para sistemas de prevención de intrusos, las herramientas usadas para la creación del sistema y la metodología que se utilizara para el desarrollo del sistema.

Para esto se preparó una revisión de la literatura utilizando una base de datos de revistas indexadas conocida como SCOPUS. Primero se determina una cadena de búsqueda, que incluye términos relevantes para el tema. Luego, se introdujo la cadena de búsqueda en la base de datos indexada, anteriormente mencionada, y se realizó una revisión exhaustiva para seleccionar los artículos adecuados. Los criterios de selección incluyeron: i) Relación directa con el tema, ii) Un número de citas igual o superior a 7.

Sistema de Prevención de Intrusos (IPS)

Un sistema de prevención de intrusiones (IPS) abarca el proceso tanto de detección de actividades deintrusión o amenazas (ciberataques), como de gestión de las acciones de respuesta sobre esas intrusiones y amenazas detectadas en toda la red (Fortinet, 2023).

Los IPS Phishing supervisan en tiempo real el tráfico de paquetes con actividades maliciosas o que coincidan con perfiles específicos y activan la generación de alertas, llevando así a eliminar o bloquear el tráfico en tiempo real que pasa por la red.Las principales contramedidas de los IPS consisten en detener un ataque en curso se producen mediante el bloqueo de campos específicos que se consideren poco seguros, además, del bloqueo total del tráfico proveniente de la web maliciosa (Chakraborty, 2013).

Los IPS pueden ser denominados la extensión de IDS con ejercicios de control de acceso para proteger los ordenadores de la explotación. IPS es un sistema inteligente no solo de detectar ataques a la red, sino también de tomar acciones preventivas para proteger a los usuarios, evitando que intrusos accedan a información sensible, protegiendo así la integridad de esa información y reduciendo la posibilidad de ser estafado. En términos simples, los IDS pueden ser perfectamente adecuado para la supervisión de ciberataques y para alertar a los administradores de amenazas emergentes, pero su velocidad, rendimiento y limitaciones pasivas han abierto la puerta a los IPS, para desafiarlos como un arma de defensa proactiva por excelencia y así hacer frente a los crecientes ciberataques generadas por las nuevas tecnologías (Adil *et al*., 2020).Un elemento muy importante que va de la mano de los IPS es el Machine Learning que se ha convertido en una herramienta importante para detectar y prevenir los diferentes tipos de ciberataques que han aparecido hoy en día (AWS, 2023).

Entre los ciberataques más comunes encontramos el malware, que es un tipo de software diseñado para dañar o comprometer los sistemas, en este ataque el Machine Learning se usa para detectarlos y clasificarlos, a través del análisis de características y comportamientos maliciosos en archivos y procesos del sistema, esta técnica permite identificar de manera más eficiente las variantes de malware y tomar medidas preventivas para proteger los sistemas de posibles ataques (Kolosnjaji *et al*., 2016).

Un ciberataque extremadamente normal en estos días debido a la utilización ampliada de la web y el correo electrónico, es el phishing, un tipo de ataque en el que los ciberdelincuentes imitan los sitios web genuinas para obtener datos clasificados de los usuarios (MacKay, 2018).

En el phishing los atacantes crean sitios web falsos que imitan la apariencia de sitios legítimos, como por ejemplo sitios financieros online o tiendas online (Khonji *et al*., 2013). Los usuarios son redirigidos a estos sitios falsos a través de enlaces en correos electrónicos, mensajes de texto o

anuncios engañosos, una vez en el sitio falso, se pide a los usuarios que introduzcan su información personal o financiera, que luego se captura (Fernandes *et al.*, 2016).

Un ejemplo reciente es el ataque de phishing contra clientes de Gmail en 2017, el asalto consistió en unas cuentas de correo electrónico que actuaban como la aplicación Docs de Google, en una actividad que se conoce como phishing. La página ilegítima se diseñó para engañar a los usuarios y hacerles creer que estaban ingresando sus datos en un sitio legítimo, cuando en realidad, los datos ingresados eran capturados por los atacantes con fines maliciosos. Este tipo de ataque, conocido como "phishing de inicio de sesión", busca obtener acceso no autorizado a cuentas y datos sensibles de los usuarios mediante tácticas engañosas (Cárdenas, 2017).

El phishing puede dañar la confianza de los usuarios hacia una organización si los atacantes se hacen pasar por ella para llevar a cabo actividades maliciosas (Ciberseguridad, 2021).Un sistema de prevención de intrusos phishing ayuda a proteger la marca y la confianza de los usuarios al prevenir ataques y mantener la integridad de los usuarios (Liao & Hsieh, 2016). El Machine Learning se emplea para prevenir estos ataques mediante el análisis de características y patrones en los correos electrónicos y sitios web sospechosos (Fernandes *et al.*, 2016).

Características para prevención de intrusos – Phishing

Es importante mencionar que se utilizó el mismo conjunto de datos (factores de compromiso) utilizado en el proyecto anterior “Sistema de detección de intrusos en sitios web, usando modelos y/o algoritmos de Machine Learning: caso práctico Phishing Google Chrome” (Castillo Veloz & Chuquitarco Velasco, 2023), con el fin asegurar la consistencia y comparabilidad de los resultados. En este estudio el cual se realizó una revisión de la literatura para poder detectar que características son las más comunes y con qué frecuencia se presentan las mismas. Las características elegidas se presentan en

orden descendente segúnsu frecuencia, en total se obtuvieron 30 características las cuales se muestran en la Tabla 1, las características son obtenidas de los sitios web basadas en una URL.

Tabla 1

Características de URL phishing

Ord.	Características	Descripción	Artículos
1	Presencia de dirección IP	Los atacantes de phishing pueden usar direcciones IP en lugar de la URL del dominio, con el fin de ocultar la identidad del sitio (Alshabib *et al*., 2022), (Vira Yudha & Wisnu Wardhani, 2021),	(Alshabib *et al*., 2022), (Castillo Veloz & Chuquitarco Velasco, 2023), (Vira Yudha & Wisnu Wardhani, 2021).
2	Longitud de la URL	Las URL de sitios web legítimos generalmente tienen menos de 54 caracteres, mientras que aquellas que superan los 75 caracteres tienen una alta probabilidad de ser consideradas phishing (Muhammad *et al*., 2020).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Muhammad *et al*., 2020).
3	Presencia del símbolo @	La presencia del símbolo "@" en una URL puede hacer que el navegador web ignore todo lo que está antes de dicho símbolo. Esta técnica incrementa que el sitio web sea	(Bruce, 2020), (Castillo Veloz & Chuquitarco Velasco, 2023).

Ord.	Características	Descripción	Artículos
		phishing (Bruce, 2020).	
4	Estado SSL	Los sitios ilegítimos no presentan certificación SSL. Esto se verifica significa es que un sitio legítimo (Iglesias, 2017).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Iglesias, 2017).
5	Edad del dominio	Es phishing con un tiempo menor a 6 (Mat Rani *et al*., 2023).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Mat Rani *et al*., 2023).
6	Redirección de doble Barra	Si las barras dobles “//” en la URL es mayor a 7, es considerado un sitio web de phishing (Vargas, 2020).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Vargas, 2020).
7	URL de anclaje	El método consiste en contar la cantidad de veces que las etiquetas "<a>" con enlaces en un sitio web dirigen a un dominio diferente al del propio sitio. Si esta cantidad supera el 31%, se considera sospechosa de phishing (Castro Moreno, 2022).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Castro Moreno, 2022).
8	Prefijo / Sufijo	En los sitios web de phishing, se utiliza el símbolo "-" para añadir prefijos y sufijos en las URL, mientras que los sitios web	(Castillo Veloz & Chuquitarco Velasco, 2023), (Deshpande *et al*., 2021)

Ord.	Características	Descripción	Artículos
		legítimos no lo utilizan (Deshpande *et al*., 2021).	
9	Enlaces en etiquetas	Se analiza todas las etiquetas presentes en el sitio web y las direcciones a las que redirigen. Si alguna de las estas se encuentra en una lista negra, es phishing (Mohammad *et al*., 2015).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Mohammad *et al*., 2015).
10	Deshabilitar clic derecho	En los sitios web legítimos, es común encontrar la opción de clic derecho desactivada para evitar que los usuarios realicen cambios en el código fuente del sitio (Mohammad *et al*., 2015).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Mohammad *et al*., 2015).
11	Uso de ventana emergente	Las ventanas emergentes que aparecen en la pantalla pidiendo información al usuario y desaparecen con un solo clic son una señal de un posible sitio web con phishing (Tyagi *et al*., 2018).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Tyagi *et al*., 2018).
12	Favicon	Es un icono usado para identificar el sitio web. Si es diferente del dominio indicado en la URL,	

Ord.	Características	Descripción	Artículos
		puede tratarse de un sitio de phishing (Chiew *et al*., 2018).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Chiew *et al*., 2018).
13	URL anormal	Se lleva a cabo una revisión de la URL para verificar si contiene el nombre del host y si coincide con el dominio mostrado en la URL. Si carece de estas dos características, se considera como un posible caso de phishing (Mohammad *et al*., 2012).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Mohammad *et al*., 2012)
14	Iframe	Las etiquetas Iframe se utilizan para incrustar y redirigir a otro sitio web dentro de un mismo sitio. Pero estas pueden ser utilizadas de formas engañosas para manipular a los usuarios y dirigirlos a sitios web phishing (Srinivasa Rao & Pais, 2017).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Srinivasa Rao & Pais, 2017)
15	Registro DNS	El registro DNS de un sitio web contiene información crucial, sin embargo, los sitios web de phishing tienden a ocultar esta información	(Castillo Veloz & Chuquitarco Velasco, 2023), (Li *et al*., 2016)

Ord.	Características	Descripción	Artículos
		para evitar ser identificados (Li *et al*., 2016).	
16	Índice de Google	Esto se debe a que su objetivo es engañar a los usuarios de manera rápida antes de ser detectados y bloqueados (Patil *et al*., 2018).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Patil *et al*., 2018).
17	Puerto utilizado	Los puertos utilizados por los sitios web seguros suelen ser 8080 y 443 (Shirazi *et al*., 2017)	(Castillo Veloz & Chuquitarco Velasco, 2023), (Shirazi *et al*., 2017).
18	Request URL	Si la dirección URL está fuera del dominio, es un sitio web phishing (Mohammad *et al*., 2012).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Mohammad *et al*., 2012).
19	SFH (Controlador de formulario de servidor)	El SFH revisa los formularios y el botón submit, si retorna un mensaje vacío o no proporciona ninguna respuesta al completar el formulario, esto puede indicar que el sitio web es phishing (Zabihimayvan & Doran, 2019).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Zabihimayvan & Doran, 2019)
20	Recuento de re-dirección del sitio Web	Contea las veces en las que el sitio web redirige la página a una sola dirección o a un sitio web	(Castillo Veloz & Chuquitarco Velasco, 2023), (Singh & Meenu, 2020).

Ord.	Características	Descripción	Artículos
		completamente diferente al de la barra de búsqueda (Singh & Meenu, 2020).	
21	MouseOver	Anteriormente esta función mostraba información del sistema en la parte inferior de la pantalla, pero actualmente es menos común en la mayoría de los sitios web legítimos. Entonces, si el sitio web tiene esta función es sospechoso de phishing (Nagaraj *et al*., 2018).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Nagaraj *et al*., 2018).
22	Tráfico web	Por lo general, cuanto mayor el número de visitas al sitio web, se considera que es más confiable (Mohammad *et al*., 2012).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Mohammad *et al*., 2012)
23	Servicio de acortamiento	Se refiere a la abreviación de la URL siendo esta capaz de redirigir al sitio web original, sin embargo, la mayoría de los sitios web de phishing hacen uso de este tipo de servicios para ocultar la verdadera dirección URL y engañar a los usuarios (Kamalam *et al*., 2022).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Kamalam *et al*., 2022).

Ord.	Características	Descripción	Artículos
24	Duración del registro del dominio	Se hace uso de Whois, donde se verifica los años que un dominio de sitio web ha sido registrado. Si el período de registro es igual o menor a 1 año, se considera un posible phishing (Mcgrath & Gupta, 2008).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Mcgrath & Gupta, 2008).
25	Token HTTPS	El uso el protocolo TLS/SSL y el HTTP seguro (Mahajan & Siddavatam, 2018).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Mahajan & Siddavatam, 2018).
26	Envío de información al correo electrónico	Si el sitio web internamente utiliza algún tipo de servicio "mail() to", puede señal de sitio web phishing (Kumar, 2018).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Kumar, 2018)
27	Rango de página	Si este valor es inferior a 0.2, se considera que el sitio web	(Castillo Veloz & Chuquitarco Velasco, 2023), (Deshpande *et al*., 2021).
28	Informe estadístico	El informe estadístico muestra información sobre sitios web legítimos e ilegítimos. Estos informes permiten analizar y comprender mejor las características y tendencias de los diferentes tipos de sitios web (Singh	(Castillo Veloz & Chuquitarco Velasco, 2023), (Singh & Meenu, 2020)

Ord.	Características	Descripción	Artículos
		& Meenu, 2020). Tiene una alta probabilidad de ser un sitio de phishing (Deshpande *et al*., 2021).	
29	Presencia de Subdominio	Cuanto un sitio web tiene 2 subdominios en su URL puede ser phishing (Butnaru *et al*., 2021).	(Butnaru *et al*., 2021), (Castillo Veloz & Chuquitarco Velasco, 2023).
30	Enlaces que apuntan a la página	Para considerarse legítimo, el sitio web debe contar con al menos 2 enlaces que lo respalden (Chawla, 2022).	(Castillo Veloz & Chuquitarco Velasco, 2023), (Chawla, 2022).

Nota. La tabla muestra las características (factores de compromiso) más relevantes ordenados de manera descendente, con una descripción y los artículos encontrados que mencionan dicha característica.

Modelos y/o algoritmos de Machine Learning

Se define a él Machine Learning como una rama de la inteligencia artificial, enfocada a que las computadoras aprendan y mejoren automáticamente a partir de datos, sin ser programadas, todo esto con el desarrollo algoritmos y modelos (Mitchell, 1997).

Su objetivo principal hacer que las máquinas puedan tomar decisiones o hacer predicciones basadas en patrones presentes en los datos de entrenamiento (Breiman, 2001). El Machine Learning permite a las computadoras analizar y procesar gran cantidad de datos de manera eficiente, lo que ayuda la detección de patrones y la creación de modelos enfocados en predicción (Hastie *et al*., 2017).

En el contexto del aprendizaje automático, los algoritmos y/o modelos son componentes importantes, ya que son utilizados para realizar determinadas tareas de forma automáticas como la clasificación, la regresión, la agrupación y la detección de anomalías. Los algoritmos son procedimientos que aprenden a partir de los datos y generan modelos que pueden realizar tareas específicas. Estos algoritmos pueden ser supervisados, no supervisados o semi-supervisados (Mitchell, 1997). Estos modelos pueden ser lineales, no lineales, probabilísticos o basados en reglas, dependiendo de la complejidad del problema y los datos disponibles (Bishop, 2006). Son herramientas poderosas que permiten a las máquinas aprender y tomar decisiones basadas en datos.

El uso de Machine Learning en IPS permite detectar y prevenir actividades maliciosas en una red o sistema informático. El Machine Learning se utiliza para construir modelos que aprenden el comportamiento normal de una red y pueden detectar desviaciones o anomalías que podrían ser indicativas de actividades intrusivas (AWS, 2023).

Además, se pueden utilizar técnicas como el análisis de secuencias y algoritmos de clasificación, como las redes neuronales artificiales, para identificar actividades intrusivas en tiempo real (Gao *et al.*, 2019). El Machine Learning se utiliza para construir modelos que aprenden el comportamiento normal de los usuarios y los sistemas, y pueden identificar desviaciones o acciones inusuales que podrían ser indicativas de un ataque (Carvalho *et al*., 2017).

Las técnicas de Machine Learning planteadas a usar en la fase de detección, son Árboles de Decisión, Mezcla de Gaussianas, Bosques Aleatorios, Naïve Bayes y Redes Bayesianas (Modelos Probabilísticos), Máquina de Soporte Vectorial, Redes Neuronales Artificiales, algoritmos de Aprendizaje Profundo y K-means detalladas en la Tabla 2.

Tabla 2

Modelos y/o algoritmos de Machine Learning

Ord.	Método de Prevención	Descripción	Artículos
1	Árboles de Decisión	Decision Tree (Árbol de Decisión) es un modelo de Machine Learning que toma decisiones basadas en una jerarquía de nodos y ramas (Alzubi *et al*., 2018). Cada nodo representa una característica o atributo y cada rama representa una decisión o regla (Breiman *et al*., 2017). El proceso de toma de decisiones se realiza siguiendo el camino desde la raíz del árbol hasta una hoja, donde se llega a una conclusión o predicción (Alzubi *et al*., 2018). La revisión literaria muestra que este modelo tiene una precisión en el rango del 80% al 95% en IPS phishing.	(Breiman *et al*., 2017), (Alzubi *et al*., 2018).

Ord.	Método de Prevención	Descripción	Artículos
2	Mezcla de Gaussianas	Es un algoritmo utilizado para modelar y analizar conjuntos de datos mediante la combinación de múltiples distribuciones gaussianas. Este modelo asume que los datos provienen de una mezcla de varias distribuciones gaussianas y utiliza métodos de estimación y maximización para encontrar los parámetros óptimos de estas distribuciones. El modelo de Mezcla de Gaussianas es un método de aprendizaje automático utilizado para modelar datos mediante la combinación de múltiples distribuciones gaussianas. Se basa en la premisa de que los datos son generados por una mezcla ponderada de diferentes distribuciones gaussianas y utiliza técnicas de estimación y optimización para encontrar los	(Bishop, 2006)

Ord.	Método de Prevención	Descripción	Artículos
		parámetros óptimos de estas distribuciones (Bishop, 2006). La revisión literaria muestra que este algoritmo tiene una precisión variable y no estable en IPS phishing.	
3	Bosques Aleatorios	O Random Forests, es un algoritmo de Machine Learning que se utiliza en problemas de clasificación y regresión. Este método combina múltiples árboles de decisión individuales para formar un "bosque" y luego utiliza sus predicciones para tomar una decisión final (Breiman, 2001). Cada árbol individual se entrena en una parte aleatoria del conjunto de datos de entrenamiento y, en el proceso, se reducen los efectos del sobreajuste y se aumenta la precisión general del modelo (Alzubi *et al*., 2018).	(Alzubi *et al*., 2018), (Breiman, 2001).
4	Naïve Bayes	Consiste en asignar a un objeto	(Hernández Báez,

Ord.	Método de Prevención	Descripción	Artículos
		descrito por un conjunto de atributos o características (Hernández Báez, 2016). La revisión literaria muestra que este algoritmo tiene una precisión variable dependiendo los datos en IPS phishing.	2016).
5	Redes Bayesianas	También conocidas como redes causales probabilísticas, son herramientas estadísticas que representan un conjunto de incertidumbres relacionadas a partir de las relaciones de independencia condicional existentes entre ellas (Sucar & Tonantzintla, 2006). La revisión literaria muestra que este algoritmo tiene una precisión variable dependiendo los datos en IPS phishing.	(Sucar & Tonantzintla, 2006).
6	Máquina de Soporte Vectorial	Support Vector Machines (SVM), un algoritmo de aprendizaje supervisado empleado para	(Cortes & Vapnik, 1995).

Ord.	Método de Prevención	Descripción	Artículos
		clasificación y regresión. Se basa en la construcción de hiperplanos que separan las clases en un espacio de alta dimensión (Cortes & Vapnik, 1995). La revisión literaria muestra que este algoritmo tiene una precisión en el rango de 70%-90% en IPS phishing.	
7	Redes Neuronales Artificiales	Las redes Neuronales Artificiales (ANN), según Bishop (2006) son modelos inspirados en el funcionamiento del cerebro humano. Están formados por nodos interconectados, llamados neuronas, y se utilizan para clasificación, regresión y otras tareas (Bishop, 2006). La revisión literaria muestra que este algoritmo tiene una precisión en el rango de 80%-95% en IPS phishing.	(Bishop, 2006).
8	Aprendizaje Profundo	El Deep Learning funcionan en un proceso de varias capas.	

Ord.	Método de Prevención	Descripción	Artículos
		Cada capa contiene neuronas que realizan un procesamiento sencillo de la salida de la capa anterior de neuronas (Torres, 2018). La revisión literaria muestra que este algoritmo tiene una precisión en el rango de 85%-95% en IPS phishing.	(Torres, 2018)
9	K-means	K-means es un algoritmo de agrupación no supervisado que trata de dividir un conjunto de datos distintos. Para ello, el algoritmo K-means se basa en la suma de las distancias al cuadrado entre los puntos y centroides de cada grupo (MacQueen, 1967). La revisión literaria muestra que este algoritmo tiene una precisión muy variable e imprecisa en IPS phishing.	(MacQueen, 1967).

Nota. Tabla con información de los algoritmos Machine Learning más usados para sistemas de prevención de intrusos.

Métodos para prevención de intrusos – Phishing

Un IPS puede aplicar diferentes métodos para evitar que el usuario sufra de un ataque, en este caso de Phishing. Se realizó una revisión literaria para contextualizar estos métodos, ver su frecuencia y su funcionalidad. Esto se presenta en la Tabla 3.

Tabla 3

Métodos para la prevención de intrusos - Phishing

Ord.	Método de Prevención	Descripción	Artículos
1	Notificación de Amenaza y característica Phishing	Las notificaciones en Google Chrome son mensajes o alertas visuales que se muestran al usuario a través de una pequeña ventana emergente en el escritorio de su computadora o en la barra de notificaciones de su dispositivo móvil (Labbe *et al*., 2006). Estas notificaciones pueden provenir de sitios web, aplicaciones o extensiones instaladas en el navegador, y su objetivo es proporcionar información actualizada, recordatorios o interacciones rápidas con el usuario (*Chrome Extensions getting started*	(Labbe *et al*., 2006), (*Chrome Extensions getting started guides*, s/f)

Ord.	Método de Prevención	Descripción	Artículos
		guides, s/f).	
2	Bloqueo de sitio web	También se denominan herramientas de protección de la privacidad (PP- Tools). A lo largo de los años, estas herramientas se han utilizado para diversos fines, como ocultar contenidos publicitarios o detectar e impedir técnicas de rastreo en páginas web para garantizar la privacidad de los usuarios (Bubukayr & Frikha, 2023). Bloquear un sitio web se refiere a la acción de restringir el acceso o impedir que los usuarios visiten un determinado sitio web con el objetivo de prevenir ciberataques. Esto se logra implementando medidas de seguridad y filtros que impiden que los usuarios accedan a sitios web identificados como peligrosos (Gunnarsson *et al*., 2022).	(Bubukayr & Frikha, 2023), (Kaur

Ord.	Método de Prevención	Descripción	Artículos
		Según Kaur y Singh (2020), "Bloquear un sitio web implica la implementación de controles y restricciones para impedir que los usuarios accedan a un sitio web específico. Esta medida se toma como una forma de prevención contra ciberataques y se basa en la identificación y el filtrado de sitios web maliciosos o potencialmente peligrosos".	& Singh, 2020), (Gunnarsson *et al*., 2022)
3	Cierre de sitio web	Se refiere a la acción de suspender temporal o permanentemente la disponibilidad y acceso público de un sitio web con el objetivo de proteger la seguridad y los datos de los usuarios. Es una respuesta cuando se detecta una amenaza, un ataque en curso o como acción preventiva para evitar posibles ciberataques (Tedyyana & Ghazali, 2021).	(Chen *et al*., 2020), (Tedyyana & Ghazali, 2021).

Ord.	Método de Prevención	Descripción	Artículos
		Según Chen et al. (2020), "El cierre de un sitio web como forma de prevención contra ciberataques implica la decisión de suspender o desconectar temporal o permanentemente la operación y el acceso al sitio web con el fin de salvaguardar la integridad y confidencialidad de los datos, mitigar posibles riesgos de seguridad y evitar la explotación de vulnerabilidades conocidas o emergentes".	(Chen *et al*., 2020), (Tedyyana & Ghazali, 2021).

Nota. Tabla con información de las técnicas para prevenir intrusos en sitios web.

Extensión Google Chrome

Una extensión de Google Chrome es un módulo de software usado para extender las funcionalidades del navegador Google Chrome (Mehta, 2016). Estas extensiones están diseñadas para proporcionar nuevas características, personalización y mejoras en la experiencia de navegación para los usuarios de Chrome. Pueden agregar botones adicionalesen la barra de herramientas, modificar la apariencia de las páginas web, interactuar con servicios externos o realizar acciones automatizadas dentro del navegador (Iqbal *et al*., 2020).

Las extensiones son pequeños programas de software que pueden modificar y mejorar la funcionalidad de Google Chrome. Pueden agregar nuevas funciones a Chrome o modificar las ya existentes para que se ajusten a tus necesidades. También puedes personalizar Chrome contemas y aplicaciones (Iqbal *et al*., 2020).

Herramientas

Se utilizó Visual Studio Code como entorno de desarrollo integrado (IDE), que es una plataforma ampliamente utilizada para la creación de software, que pone a disposición una variedad de herramientas para desarrolladores de software, incluyendo soporte para múltiples lenguajes de programación, depuración de código, gestión de proyectos, control de versiones y despliegue de aplicaciones (Sotnikov, 2016).

En cuanto al servidor hará uso de PythonAnywhere, una plataforma en la nube que permite a los desarrolladores programar, ejecutar y alojar aplicaciones Python en línea., permite a los desarrolladores escribir, ejecutar y desplegar aplicaciones Python en línea sin la necesidad de configurar y administrar su propia infraestructura de servidor (Lutz, 2014).

Metodología Ágil – Scrum

Para el desarrollo del sistema se desarrollará siguiendo la metodología ágil SCRUM, con el fin de promover una respuesta rápida a entornos cambiantes, cambios en los requisitos de los usuarios, acelerar los plazos de los proyectos, etc. (Malik & Siew, 2009).

La razón principal a usarse SCRUM es debido a su interactividad y agilidad, además de ser una metodología que permite la entrega funcional de módulos, en este caso de las tres funcionalidades propuesta en la Tabla 3.

Scrum tiene unas características peculiares, su proceso de desarrollo se produce a través de Sprints (Schwaber & Sutherland, 2023). En Scrum, los requisitos del producto se organizan en una

lista de elementos llamada Product Backlog y, a través de ciclos de interacción, el equipo se centra en un objetivo específico. Al final de este ciclo, se entrega una versión funcional (incremento) del sistema a al cliente (Rodrigues de Oliveira *et al*., 2023).

Dentro de Scrum existen eventos que son necesarios para conservar un flujo regular durante el desarrollo del proyecto y prevenir posibles inconvenientes y/o situaciones que puedan retardar el proyecto, los eventos son sprint, sprint planning, daily scrum y sprint review (Schwaber & Sutherland, 2023).

Capítulo III

Implementación del Sistema

En este capítulo se detallan los procedimientos llevados a cabo para la creación del sistema de prevención de ataques de phishing utilizando modelos y/o algoritmos de Machine Learning. Este sistema se implementará como una extensión de Google Chrome, con el propósito de informar y proteger al usuario que se encuentra en un sitio web legítimo o peligroso debido a presencia de phishing.

Como funciona el sistema CyberSafeGuard es del siguiente modo: la API recibe la URL del sitio web en el que se encuentra el usuario, esta recupera las características (factores de compromiso) que se muestran en la Tabla 1 presentes en la URL. Una vez realizado este pase se predecirá si el sitio web contiene phishing o no y notificara al usuario el resultado a través de la extensión de CyberSafeGuard. En caso de que el sitio sea ilegítimo se procederá a la notificación al usuario del motivo porque es ilegítimo (factores de compromiso), y finalmente se realizara el bloqueo y cierre automático del sitio web.

Métricas de evaluación

Al sistema CyberSafeGuard se lo aplico métricas para garantizar su correcto funcionamiento. Estas son las siguientes de acuerdo con Xin et al. (2028)

Accuracy: Hace referencia al porcentaje de elementos correctamente clasificados entre positivos y negativos.

Precision: Mide el porcentaje de verdaderos positivos correctos dividido por el número total de predicciones positivas identificadas.

Recall: Calcula el número de todos los elementos detectados correctamente en proporción a todos los elementos que deben detectarse.

La Tabla 4 presenta las fórmulas utilizadas para evaluar el modelo, estas fórmulas representan las métricas de evaluación aplicadas en el contexto del proyecto.

Tabla 4

Fórmulas de métricas de evaluación

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

Nota. Tabla con las fórmulas de evaluación del sistema. Tomado de Machine learning and deep learning methods for cybersecurity, 2018 por Xin *et al*.

En donde:

- VP (Verdaderos Positivos): Número de sitios web con Phishing clasificados correctamente.
- VN: Número de sitios web legítimos clasificados correctamente.
- FP: Número de sitios web legítimos clasificados erróneamente como Phishing.
- FN: Número de sitios web con Phishing clasificados erróneamente como legítimos.

Para evaluar el modelo y/o algoritmo, se utiliza una matriz de confusión (Goetz *et al*., 2015). La Tabla 5, denominada "Matriz de confusión para CyberSafeGuard", muestra cómo se aplicará esta matriz durante la evaluación.

Tabla 5

Matriz de confusión para CyberSafeGuard

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

Nota. Tabla de confusión para evaluación del sistema.

Roles y Técnicas en Scrum

En el contexto de Scrum, las historias de usuario son una técnica utilizada para capturar los requisitos del cliente o usuario desde la perspectiva del valor que aportarán al producto o sistema. Estas historias describen una funcionalidad específica que el usuario necesita para alcanzar un objetivo o resolver un problema. Las historias de usuario son una herramienta ágil para capturar los requisitos de manera colaborativa y centrada en el usuario, lo que facilita la comunicación y el entendimiento entre el equipo de desarrollo y el cliente o usuario final. Además, permiten priorizar el trabajo de acuerdo con el valor que aportará al producto y ayudan a mantener un enfoque en las necesidades reales de los usuarios (Cohn, 2004). Estos roles se presentan en la Tabla 6.

Tabla 6

Designación de roles de Scrum

N°.	**Rol**	**Integrante**	**Descripción**
01	Scrum Master	Geraldyn Nicol Semblantes Lozada	Líder del equipo de Scrum

N°.	Rol	Integrante	Descripción
02	Product Owner	Dr. José Luis Carrillo Medina	Representa a las partes interesadas
03	Team Development	Geraldyn Nicol Semblantes Lozada	Desarrollo y diseño de la aplicación

Nota. Tabla que contiene el rol y nombre de los diferentes actores dentro del proyecto SCRUM, donde se especifican tanto el nombre del rol como el miembro del proyecto que desempeña esa función.

Dado que la proyecto se compone de sólo 1 integrante de trabajo, será Scrum Expert e igualmente participará como desarrollador como se muestra en la Tabla 6.

La Tabla 7 muestra las historias de usuario redactadas, donde se indica el trabajo, los elementos esperados y, además, las funcionalidades y los aspectos más destacados necesarios o potencialmente funcionalidades, y la avocación para su ejecución.

Tabla 7

Historias de usuario

ID	Nombre	Rol	Característica / Funcionalidad	Razón / Resultado
1	H.U. 01	Como usuario	Quiero que la extensión utilice el mejor algoritmo y/o modelo de Machine Learning para la prevención de phishing en sitios web.	Para que la extensión realicepredicciones con una buena precisión.
2	H.U. 02	Como usuario	Quiero características relevantes phishing para la URL.	Para entrenar el modelo De Machine Learning

ID	Nombre	Rol	Característica / Funcionalidad	Razón / Resultado
3	H.U. 03	Como usuario	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.

Nota. Tabla que contiene las historias de usuario con su rol, característica/funcionalidad y razón/ resultado

En la tabla 8 denominada " Sprint Planning del proyecto", se presenta una lista de historias de usuario que se implementarán a lo largo del proyecto. Cada historia de usuario viene acompañada de una estimación de tiempo en días, así como las fechas de inicio y finalización correspondientes. Además, se indica a qué número de sprint pertenece cada historia de usuario mencionada.

Tabla 8

Sprint Planning del proyecto

Historia de usuario	Nombre	Estimación (días)	Fecha de inicio	Fecha de fin	Sprint
1	H.U. 01	20	02/03/2023	29/03/2023	01. Selección del mejor modelo de Machine Learning
2	H.U. 02	20	30/03/2023	26/04/2023	02. Creación del

Historia de usuario	Nombre	Estimación (días)	Fecha de inicio	Fecha de fin	Sprint
					dataset
3	H.U. 03	20	27/04/2023	24/05/2023	03. Desarrollo de la extensión de Google Chrome

Nota. Tabla que contiene los Sprint Planning de cada historia de usuario, con su fecha de inicio y su fecha de fin.

Arquitectura del sistema

Se puede decir que la arquitectura de software es la estructura fundamental de un sistema, que define su organización, componentes, relaciones y modelos de interacción (Bass *et al*., 2022).

Arquitectura Lógica en Capas

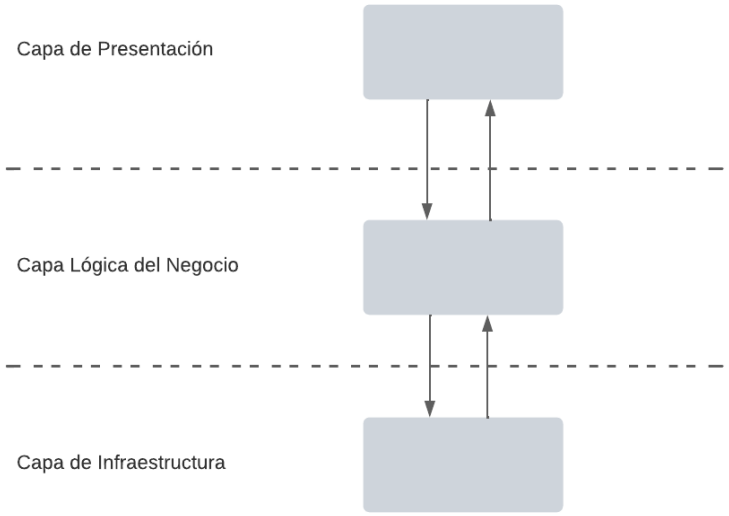
Para el desarrollo de la extensión Google Chrome CyberSafeGuard, se aplicará la arquitectura en capas. La arquitectura en capas divide los componentes del sistema de manera jerárquica, cada capa con su funcionalidad.

Las capas se comunican entre ellas a través de interfaces, lo que facilita el modularidad, la reutilización y el mantenimiento del sistema (Pressman & Maxim, 2019).

Se definió la arquitectura con 3 capas, i) Capa de Presentación, ii) Capa Lógica del Negocio y iii) Capa de Infraestructura, como se muestra en la Figura 1: Figura de la arquitectura lógica del sistema.

Figura 1

Figura de la arquitectura en Capas



Nota. La figura representa la arquitectura en capas del sistema. Siendo está dividida en tres capas: i) Capa de presentación, ii) Capa Lógica de Negocio, iii) Capa de Infraestructuras.

Definición de las tecnologías a usar.

Se trata de las herramientas o lenguajes de programación que se usara dentro del proyecto software (Al, 2005). Se detalla que tecnología se usara en cada capa a continuación

Capa de presentación*.* La capa de presentación es la capa encargada de mostrar la información al usuario y de capturar datos de sus interacciones (Pressman, 2002). Las tecnologías utilizadas son:

Html (Lenguaje de Marcas de Hipertexto): que en español se traduce como "Lenguaje de Marcas de Hipertexto", es un lenguaje de marcado utilizado para crear y estructurar contenido en la web. Es el estándar utilizado para diseñar y presentar páginas web, permitiendo la inclusión de enlaces, imágenes, videos, formularios y otros elementos interactivos (Ducket, 2011).

CSS (Cascading Style Sheets): es un lenguaje de hojas de estilo utilizado en el desarrollo web

para controlar el diseño y la presentación visual de documentos HTML. Permite definir cómo se deben mostrar los elementos HTML en una página web, incluyendo aspectos como el tamaño, color, fuente, márgenes, espaciado y disposición de los elementos (*CSS tutorial*, 2023).

JavaScript (JS): es un lenguaje de programación de alto nivel, orientado a objetos (Urrutia, 2020)

Capa lógica del negocio. La capa lógica del negocio es responsable de recibir las solicitudes originarias de la capa de presentación y enviarlas a la capa de infraestructura para realizar las predicciones necesarias. Una vez que los resultados sean obtenidos, esta capa se encargará de enviar la respuesta de vuelta a la capa inicial o de presentación, para que pueda ser mostrada al usuario. La tecnología usada en esta capa es:

JavaScript (JS): es un lenguaje de programación de alto nivel, orientado a objetos (Urrutia, 2020)

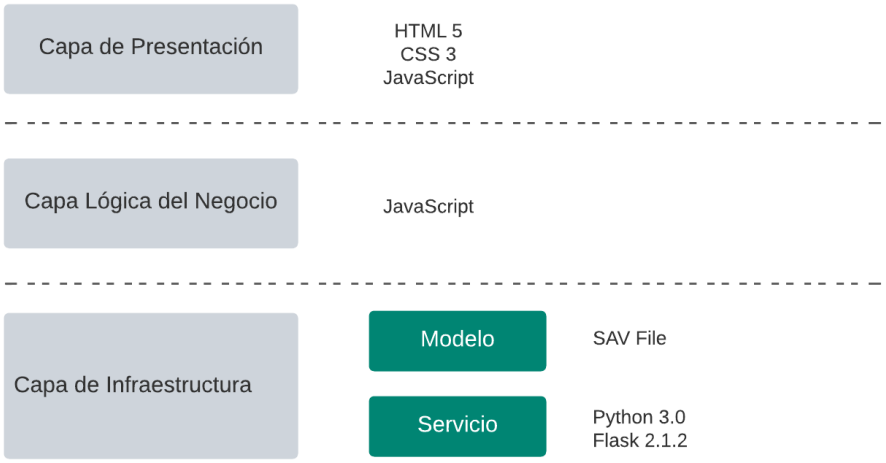
Capa de infraestructura. Los elementos principales de esta capa son: el modelo entrenado, que se guarda como un archivo SAV; y un servicio que facilita la predicción de un sitio web al ser enviado a través de la extensión de Google Chrome. La capa incluye los componentes necesarios para interactuar con la API.

Python: leguaje de programación de alto nivel, usado en aprendizaje automático (Beazley, 2009).

Flask: Es un framework web ligero y minimalista para el lenguaje de programación Python, diseñado para facilitar la creación rápida y sencilla de aplicaciones web (Grinberg, 2018).

Figura 2

Figura tecnologías a usar en cada Capa.



Nota. En la Capa de Presentación se utilizarán los lenguajes y frameworks HTML 5, CSS 3 y JavaScript. En la Capa Lógica de Negocio se utilizará el lenguaje de programación JavaScript y en la Capa de Infraestructura en cuanto a Modelo se usará SAV File y en cuanto a Servicio e lenguaje Python 3.0 y el framework Flask 2.1.2

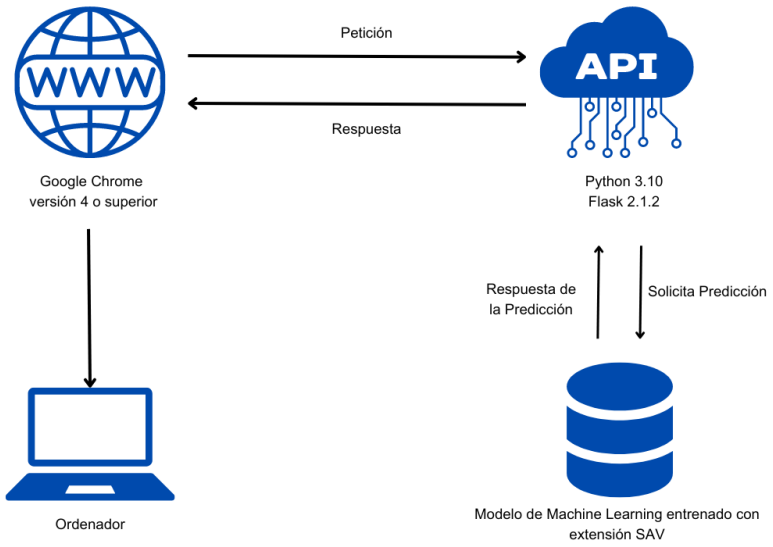
Arquitectura física.

La Figura 3 muestra la arquitectura física que se usara para desarrollar la extensión de Google Chrome llamada " CyberSafeGuard".

Al navegar por internet, cuando el usuario haga clic en la extensión, se enviará automáticamente la URL del sitio web actual a la API. La API se encargará de extraer las características de dicha URL y del sitio web correspondiente. El modelo analizará la información y determinará si el sitio web es legítimo o si representa un intento de phishing. Luego, la API enviará la respuesta al resultado del análisis de la extensión, informando al usuario sobre la naturaleza del sitio web que está visitando. Además, en caso de ser un sitio malicioso se notificará al usuario sobre el tipo de anomalía (característica) que presenta dicho sitio web y se procederá al bloqueo y cierre automático del sitio.

Figura 3

Figura de la arquitectura física del sistema



Nota. La figura muestra la arquitectura física del sistema en donde el usuario realizara la petición usando Google Chrome de versión 4 o superior a través de un ordenador, laptop o computadora de escritorio, la API recibe esta petición y solicita al dataset de Machine Learning ya entrenado una respuesta para enviarla al usuario de internet.

Hardware

Para la ejecución y desarrollo del proyecto en cada uno de los Sprint fue un procesador Intel Core i7-11375H con una disponibilidad de memoria RAM de 16.0 GB y sistema operativo Windows 10 Home.

Implementación de algoritmos y modelos de Machine Learning para sitios web Phishing

La planificación de cada Sprint en Scrum es el proceso mediante el cual el Equipo Scrum selecciona las Historias de Usuario que se abordarán durante ese periodo de tiempo. El Sprint es una iteración fija y corta en la que se desarrolla, prueba y entrega un incremento de producto potencialmente utilizable (Schwaber & Sutherland, 2017).

Sprint 01: Selección del mejor modelo de Machine Learning

Historias de usuario detalladas. La Historia de Usuario H.U. 01, que se refiere a la selección del modelo y/o algoritmo de Machine Learning para el sistema de prevención de phishing (CyberSafeGuard), se define resultado el Sprint para considerarlo como valido.

Tabla 9

Historia de usuario para la selección del modelo y/o algoritmo de Machine Learning

Historias de Usuario	
Número: H.U. 01	**Usuario:** Usuario de internet
Nombre historia: Definición y selección del modelo para prevención de sitios web con phishing**.**	
Prioridad de negocio: Alta	**Riesgo en desarrollo:** Media
Puntos estimados (días): 20	**Interacción asignada:** 1
Programadores responsables: Geraldyn Semblantes	
Descripción: • Como usuario quiero que la extensión utilice el mejor algoritmo y/o modelo de Machine Learning para la prevención de phishing en sitios web.	
Validación (Criterios de aceptación): • Se llevarán a cabo pruebas individuales para cada modelo seleccionado, y se registrarán los resultados obtenidos para cada uno de ellos. • Se seleccionará solo un modelo para aplicarse en el sistema, el que presente mejor precisión.	

Nota. La tabla muestra los detalles de la Historia de Usuario 01 con información relevante como la prioridad, el riesgo de desarrollo, los días estimados para desarrollarse, la interacción asignara, el responsable y así mismo una descripción y criterios de aceptación para la Historio de Usuario.

Sprint Backlog. El Sprint Backlog 01 detalla las actividades realizadas durante el sprint, la persona responsable de su ejecución, los datos de planificación para la ejecución del sprint, las estimaciones de tiempo en horas para cada tarea y el estado actual de cada tarea.

Tabla 10

Sprint Backlog 01

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	1	02/03/2023	8 horas	29/03/2023	02/03/2023	03/03/2023	06/03/2023	07/03/2023	08/03/2023	09/03/2023	10/03/2023	13/03/2023	14/03/2023	15/03/2023	16/03/2023	17/03/2023	20/03/2023	21/03/2023	22/03/2023	23/03/2023	24/03/2023	27/03/2023	28/03/2023	29/03/2023	
	Tareas Pendientes				8	8	7	7	6	6	5	4	4	3	3	3	3	2	2	2	2	1	1	0
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0

Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 01	Selección de artículos	Revisión de literatura	Geraldyn Semblantes	Finalizado	16	8

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	1	02/03/2023	8 horas	29/03/2023	02/03/2023	03/03/2023	06/03/2023	07/03/2023	08/03/2023	09/03/2023	10/03/2023	13/03/2023	14/03/2023	15/03/2023	16/03/2023	17/03/2023	20/03/2023	21/03/2023	22/03/2023	23/03/2023	24/03/2023	27/03/2023	28/03/2023	29/03/2023	
	Tareas Pendientes				8	8	7	7	6	6	5	4	4	3	3	3	3	2	2	2	2	1	1	0
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0

Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 01	Extracción de modelos y/o algoritmos de Machine Learning	Revisión deliteratura	Geraldyn Semblantes	Finalizado	16	8
H.U. 01	Extracción de valores del accuracy respectivamente	Revisión de literatura	Geraldyn Semblantes	Finalizado	16	8

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	1	02/03/2023	8 horas	29/03/2023	02/03/2023	03/03/2023	06/03/2023	07/03/2023	08/03/2023	09/03/2023	10/03/2023	13/03/2023	14/03/2023	15/03/2023	16/03/2023	17/03/2023	20/03/2023	21/03/2023	22/03/2023	23/03/2023	24/03/2023	27/03/2023	28/03/2023	29/03/2023	
	Tareas Pendientes				8	8	7	7	6	6	5	4	4	3	3	3	3	2	2	2	2	1	1	0
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0

Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 01	Documentación de la Frecuencia de los modelos y/o algoritmos de Machine Learning	Documentación	Geraldyn Semblantes	Finalizado	8	4

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	1	02/03/2023	8 horas	29/03/2023	02/03/2023	03/03/2023	06/03/2023	07/03/2023	08/03/2023	09/03/2023	10/03/2023	13/03/2023	14/03/2023	15/03/2023	16/03/2023	17/03/2023	20/03/2023	21/03/2023	22/03/2023	23/03/2023	24/03/2023	27/03/2023	28/03/2023	29/03/2023	
	Tareas Pendientes				8	8	7	7	6	6	5	4	4	3	3	3	3	2	2	2	2	1	1	0
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0

Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 01	Selección de Modelos y/o algoritmos de Machine Learning para realización de pruebas	Documentación	Geraldyn Semblantes	Finalizado	16	6

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	1	02/03/2023	8 horas	29/03/2023	02/03/2023	03/03/2023	06/03/2023	07/03/2023	08/03/2023	09/03/2023	10/03/2023	13/03/2023	14/03/2023	15/03/2023	16/03/2023	17/03/2023	20/03/2023	21/03/2023	22/03/2023	23/03/2023	24/03/2023	27/03/2023	28/03/2023	29/03/2023	
	Tareas Pendientes				8	8	7	7	6	6	5	4	4	3	3	3	3	2	2	2	2	1	1	0
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0

Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 01	Implementación de Modelos y/o algoritmos de Machine Learning seleccionados	Codificación	Geraldyn Semblantes	Finalizado	32	4

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	1	02/03/2023	8 horas	29/03/2023	02/03/2023	03/03/2023	06/03/2023	07/03/2023	08/03/2023	09/03/2023	10/03/2023	13/03/2023	14/03/2023	15/03/2023	16/03/2023	17/03/2023	20/03/2023	21/03/2023	22/03/2023	23/03/2023	24/03/2023	27/03/2023	28/03/2023	29/03/2023	
	Tareas Pendientes				8	8	7	7	6	6	5	4	4	3	3	3	3	2	2	2	2	1	1	0
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0

Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 01	Ejecución de pruebas	Pruebas	Geraldyn Semblantes	Finalizado	32	8
H.U. 01	Selección de Modelos y/o algoritmos de Machine Learning con mejor valor de accuracy	Pruebas	Geraldyn Semblantes	Finalizado	16	4

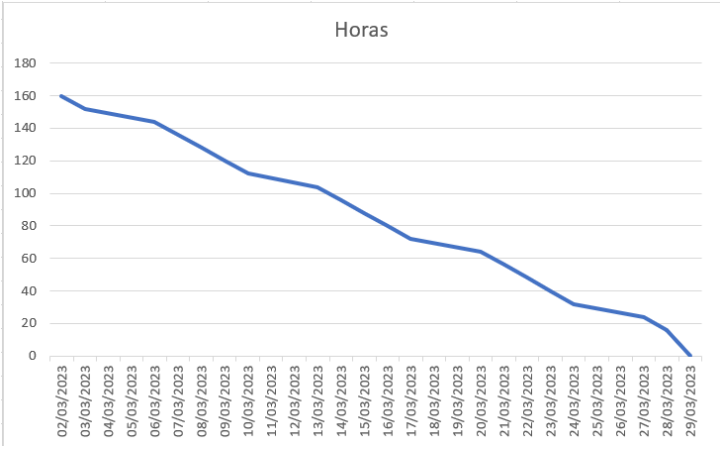
Nota. La tabla muestra las actividades que se realizó durarte el Sprint 01, su responsable, horas ocupadas y esfuerzo.

Burndown chart. Esta grafica muestra el descenso de carga de trabajo al pasar de los días de la siguiente forma: la cantidad de trabajo pendiente está en el eje vertical (eje y) y el tiempo transcurrido en el eje horizontal (eje x) (Schwaber & Sutherland, 2020).

La Figura 4 presenta el Burndown chart del Sprint 01, donde se visualiza el progreso realizado a lo largo del tiempo estimado para el desarrollo de este sprint. El gráfico muestra en su eje X las fechas correspondientes a los días del intervalo de tiempo, que va desde el 03 de marzo de 2023 hasta el 29 de abril de 2023, como se especifica en la Tabla 10. El valor máximo en el eje y se obtiene multiplicando el número total de días estimado al inicio del sprint (en este caso, 20 días) por las horas trabajadas al día (8 horas al día). estimado (en este caso, 20 días) por las horas trabajadas al día (8 horas al día). Esta multiplicación nos da un valor de 160 horas, que representa el máximo valor en el eje Y del gráfico, entonces a medida que transcurren los días, el valor de horas en el gráfico debe ir disminuyendo progresivamente hasta llegar a cero, lo que indica que el Sprint ha sido completado exitosamente.

Figura 4

Burndown Chart - Sprint 01



Nota. La figura muestra el decrecimiento de las tareas pendientes con relación al número de horas (eje x) y al día (eje y).

Resultados del Sprint. Se las métricas de evaluación de los 9 algoritmos mencionados en Capítulo II. Para esto se hizo una búsqueda exhaustiva en artículos referentes a los algoritmos. Se determino la frecuencia que presenta cada algoritmo y/o modelo Learning y se seleccionaron los que presentaban una mayor frecuencia, con esto resulto que solo se hará uso de 8 modelo y/o algoritmo de Machine. Debido a que el algoritmo K-means no muestra que es apto para los sistemas de predicción de phishing.

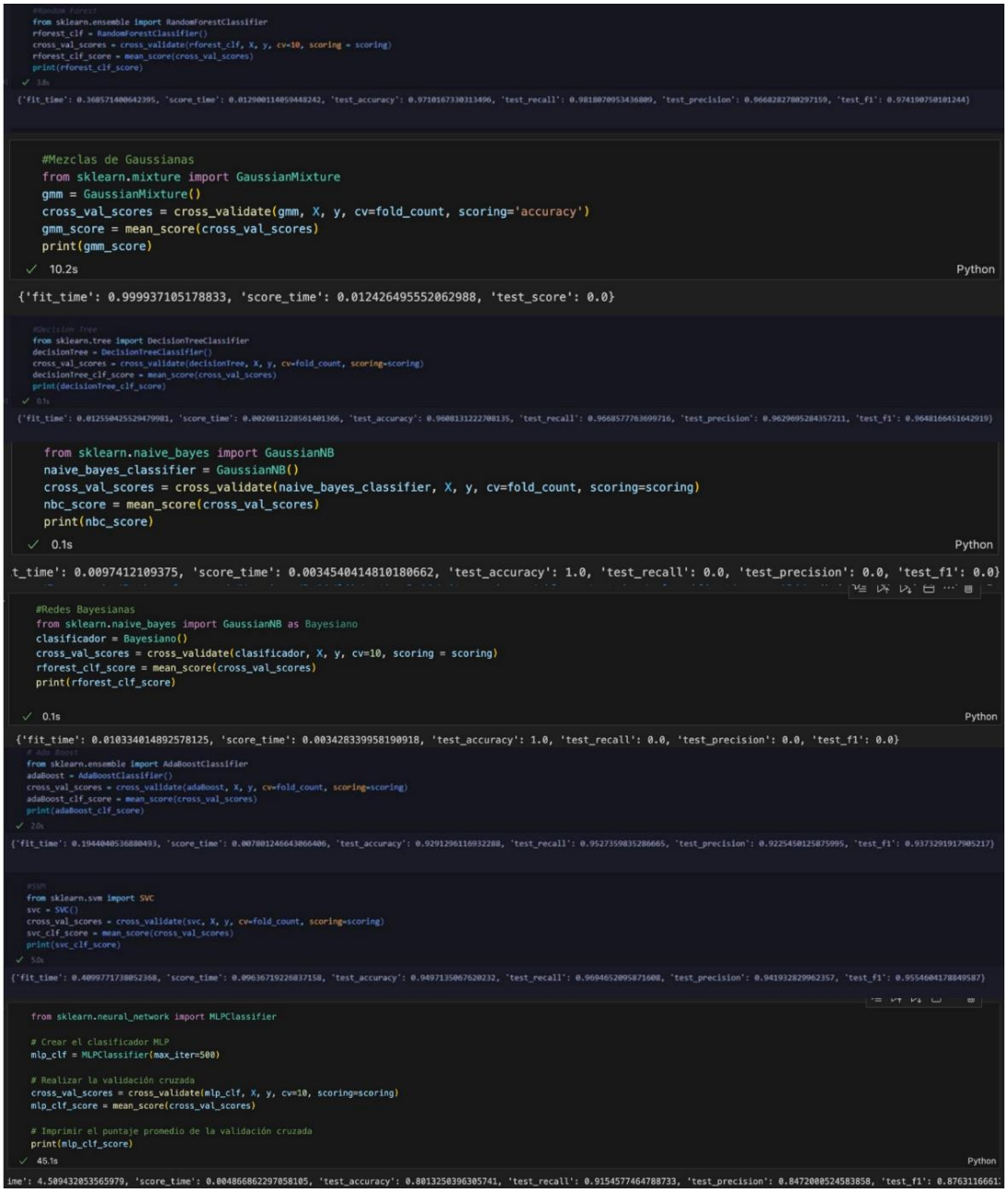
> K-means es un algoritmo de agrupación utilizado para dividir un conjunto de datos en grupos o clusters basados en la similitud de las características de los datos. No está diseñado para clasificar o predecir clases, como la predicción de phishing (Aung & Min, 2018).

Por lo tanto, K-means es óptimo para la creación de datasets y no es óptimo para el desarrollo del sistema de prevención de intrusos.

Con los 8 modelos de Machine Learning o los algoritmos potencialmente con los mejores valores de precisión en la prevención de phishing en sitios, se llevaron a cabo y se probaron utilizando el conjunto de datos utilizado en la revisión pasada, además de nuevo conjunto de datos realizado, al que se dará sentido exhaustivo en la Sprint 02. Estos dos conjuntos de datos tienen URLs que presentan los 30 presentados en la Tabla 1, esta implementación se muestra en la Figura 5 y sus resultados en la Tabla 11.

Figura 5

Implementación de modelos y/o algoritmos Machine Learning



Nota. La figura muestra una captura de pantalla de la implementación de los algoritmos y-o modelos Machine Learning puestos a prueba y sus resultados de accuracy, precisión y recall correspondientes.

Tabla 11

Resultados pruebas modelos y/o algoritmos de Machine Learning implementados

Características	Algoritmos/Modelos	Accuracy	Precision	Recall
30 características	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

Nota. La tabla muestra los resultados obtenidos de accuracy, precisión y recall de los 8 modelos y-o algoritmos Machine Learning seleccionados y probados.

Con los resultados de la Tabla 11 podemos resaltar algunos puntos relevantes. El primero es que el algoritmo de Mezclas Gaussianas no es apto para su implementación debido a que el resultado de accurary es demasiado bajo en comparación de la media del resto, entonces no es necesario calcular la precisión ni el recall, ya que este queda totalmente descartado. Otro dato a resaltar es que los algoritmos de Naive Bayes y Redes Bayesianas presentan un alto nivel de accuracy de 1,00, esto hace referencia a la cantidad de elementos correctamente clasificados entre positivos y negativos, sin embargo, en cuanto a las métricas de precisión y recall presenta un valor de 0, por lo tanto, no es seleccionado.

Al final del sprint se eligió el algoritmo Radom Forest con un 97,10 %. de precisión al prevenir phishing.

Sprint 02: Creación del dataset

Historias de usuario detallada. En esta historia de usuario se especifican los detalles del proceso para generar el conjunto de datos que será utilizado en el sistema, en donde se encuentran los encargados del desarrollo y los criterios de aceptación para la creación del dataset que contendrá las características seleccionadas para la implementación del sistema propuesto. Esto se detalla en la Tabla 12

Tabla 12

Historia de usuario para la creación de un dataset

Historias de Usuario	
Número: H.U. 02	**Usuario:** Usuario de internet
Nombre historia: Creación de dataset	
Prioridad de negocio: Alta	**Riesgo en desarrollo:** Media
Puntos estimados (días): 20	**Interacción asignada:** 1
Programadores responsables: Geraldyn Semblantes	
Descripción: • Como usuario quiero un dataset con características que faciliten la identificación de sitios web legítimos y aquellos con phishing, en busca de un mayor nivel de seguridad para el usuario.	
Validación (Criterios de aceptación): • Se utilizará como base el conjunto de datos de características del estudio anterior el cual incluye 30 características clave organizadas en orden descendente según su frecuencia. • Se hará la creación de un nuevo dataset, que incluya nuevas URLs tanto legítimas como ilegítimas.	

Historias de Usuario	
Número: H.U. 02	**Usuario:** Usuario de internet
Nombre historia: Creación de dataset	
Prioridad de negocio: Alta	**Riesgo en desarrollo:** Media
Puntos estimados (días): 20	**Interacción asignada:** 1
Programadores responsables: Geraldyn Semblantes	
Validación (Criterios de aceptación): • Se crearán diferentes escenarios de pruebas para los modelos y/o algoritmos de Machine Learning. Estos escenarios serán de acuerdo a la clasificación de las características.	

Nota. La tabla muestra los detalles de la Historia de Usuario 02 con información relevante como la prioridad, el riesgo de desarrollo, los días estimados para desarrollarse, la interacción asignara, el responsable y así mismo una descripción y criterios de aceptación para la Historio de Usuario.

Sprint Backlog. El Sprint Backlog 02 detalla las actividades realizadas durante el sprint, la persona responsable de su ejecución, los datos de planificación para la ejecución del sprint, las estimaciones de tiempo en horas para cada tarea y el estado actual de cada tarea.

Tabla 13

Sprint Backlog 02

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	2	30/03/2023	8 horas	26/04/2023	30/03/2023	31/03/2023	03/04/2023	04/04/2023	05/04/2023	06/04/2023	07/04/2023	10/04/2023	11/04/2023	12/04/2023	13/04/2023	14/04/2023	17/04/2023	18/04/2023	19/04/2023	20/04/2023	21/04/2023	24/04/2023	25/04/2023	26/04/2023	
	Tareas Pendientes				5	5	4	4	3	3	3	3	3	2	2	2	2	2	1	1	1	0	0	
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0

Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 02	Revisión y entendimiento de características de estudio anterior	Revisión de literatura	Geraldyn Semblantes	Finalizado	16	4

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	2	30/03/2023	8 horas	26/04/2023	30/03/2023	31/03/2023	03/04/2023	04/04/2023	05/04/2023	06/04/2023	07/04/2023	10/04/2023	11/04/2023	12/04/2023	13/04/2023	14/04/2023	17/04/2023	18/04/2023	19/04/2023	20/04/2023	21/04/2023	24/04/2023	25/04/2023	26/04/2023	
	Tareas Pendientes				5	5	4	4	3	3	3	3	3	2	2	2	2	2	1	1	1	0	0	
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0

Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 02	Selección de nuevo dataset	Implementación	Geraldyn Semblantes	Finalizado	16	4
H.U. 02	Limpieza y unión de datasets seleccionados	Codificación	Geraldyn Semblantes	Finalizado	40	6

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	2	30/03/2023	8 horas	26/04/2023	30/03/2023	31/03/2023	03/04/2023	04/04/2023	05/04/2023	06/04/2023	07/04/2023	10/04/2023	11/04/2023	12/04/2023	13/04/2023	14/04/2023	17/04/2023	18/04/2023	19/04/2023	20/04/2023	21/04/2023	24/04/2023	25/04/2023	26/04/2023	
	Tareas Pendientes				5	5	4	4	3	3	3	3	3	2	2	2	2	2	1	1	1	0	0	
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0

Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 02	Entrenamiento para la extracción de característica de una URL	Codificación	Geraldyn Semblantes	Finalizado	40	8

Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
2	30/03/2023	8 horas	26/04/2023	30/03/2023	31/03/2023	03/04/2023	04/04/2023	05/04/2023	06/04/2023	07/04/2023	10/04/2023	11/04/2023	12/04/2023	13/04/2023	14/04/2023	17/04/2023	18/04/2023	19/04/2023	20/04/2023	21/04/2023	24/04/2023	25/04/2023	26/04/2023
Tareas Pendientes				5	5	4	4	3	3	3	3	3	2	2	2	2	2	1	1	1	1	0	0
Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0

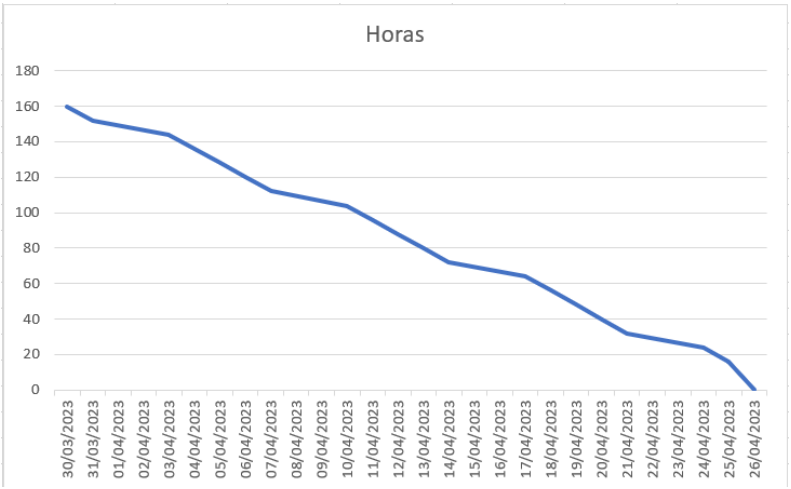
Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 02	Pruebas de presión con uso de herramientas	Pruebas	Geraldyn Semblantes	Finalizado	32	6

Nota. La tabla muestra las actividades que se realizó durarte el Sprint 02, su responsable, horas ocupadas y esfuerzo.

Burndown chart. Se realizo de igual manera Burndown Chart del Sprint 02, donde se visualiza el progreso realizado a lo largo del tiempo estimado para el desarrollo de este sprint. El gráfico muestra en su eje X desde el 30 de marzo de 2023 hasta el 26 de abril de 2023, y el eje Y las horas de trabajo, obtenidos multiplicando el número total de días estimado (20 días) por las horas de trabajo por día (8 horas diarias), que nos da un valor de 160 horas, que representa el máximo valor en el eje Y del gráfico, entonces a medida que transcurren los días, el valor de horas en el gráfico debe ir disminuyendo progresivamente hasta llegar a cero, lo que indica que el Sprint ha sido completado exitosamente.

Figura 6

Burndown Chart - Sprint 02



Nota. La figura muestra el decrecimiento de las tareas pendientes con relación al número de horas (eje x) y al día (eje y).

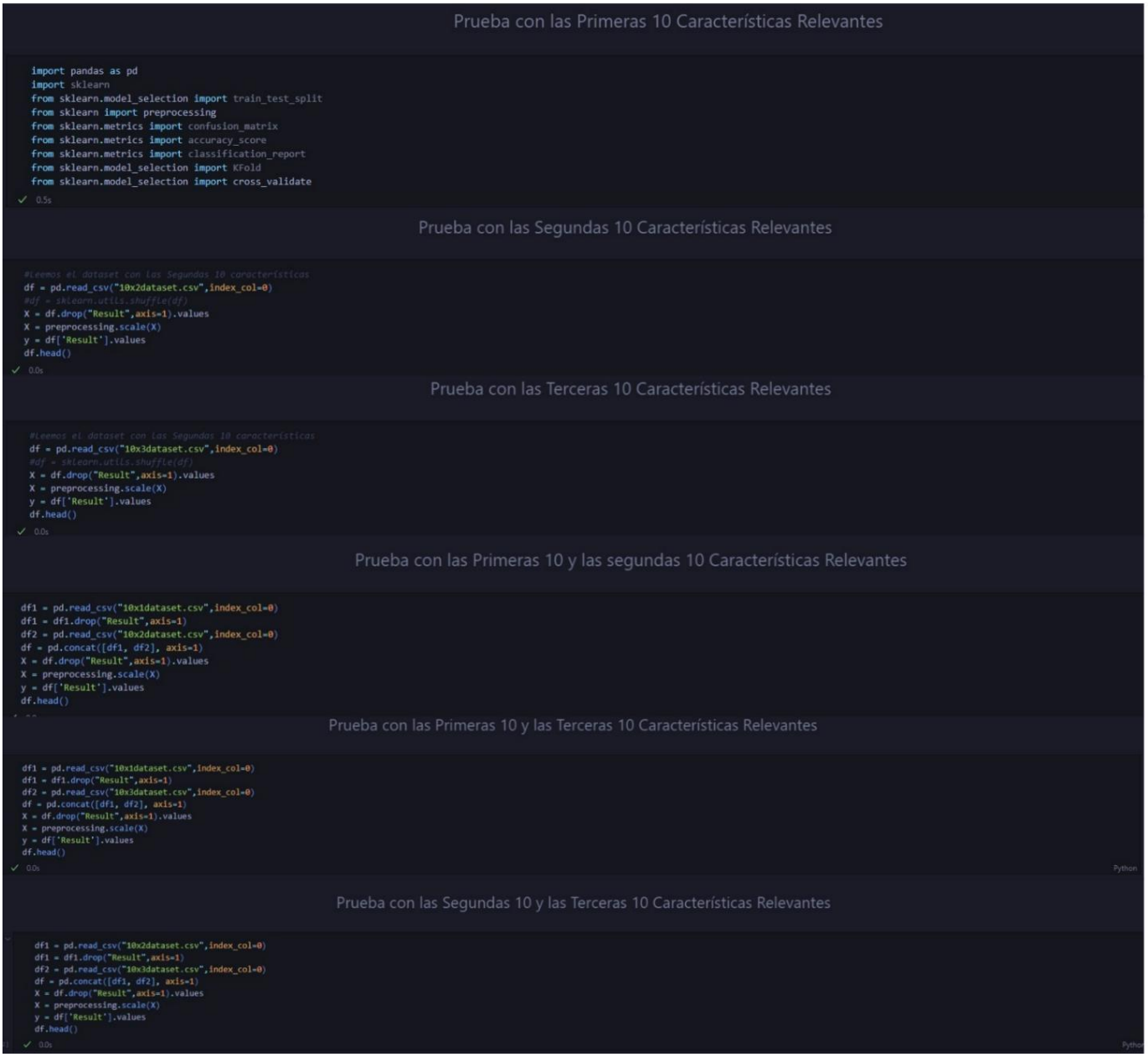
Resultados del Sprint. Se obtuvo un nuevo dataset con URLs tanto legítimas como ilegítimas, en el Anexo 3 se muestra el dataset seleccionado del repositorio KAGGLE.

En este Sprint, también se llevó a cabo la implementación del código para probar diferentes escenarios de validación. Para ello, se crearon grupos de 10 características (recursos de comprobación) en cada escenario. Se han creado tres escenarios con el propósito de evaluar el impacto de las

características más relevantes, menos relevantes y aquellas que se encuentran en el medio. Además, se busca examinar la contribución de la combinación de estos grupos de características. El objetivo principal es determinar cuáles de ellas son más significativas para la detección de phishing en sitios web. Para lograrlo, se llevaron a cabo pruebas individuales de los modelos, así como pruebas combinadas entre ellos, de la siguiente manera: se realizó una prueba inicial utilizando las primeras diez características. Posteriormente, se llevaron a cabo pruebas adicionales con las siguientes diez características y luego con las diez restantes. También se realizaron pruebas combinando las primeras diez características con las segundas diez, así como con las diez primeras y las diez terceras características. Finalmente, se evaluó la combinación de las segundas diez y las diez terceras características, como se muestra en la Figura 7: Pruebas de características con diferentes escenarios. Las pruebas fueron realizadas utilizando los modelos y/o algoritmos de Machine Learning detallados en la Tabla 14.

Figura 7

Diferentes escenarios para pruebas de características



Nota. La figura muestra como se clasificaron las características, siendo así 6 escenarios de prueba.

Tabla 14

Resultados de pruebas con los diferentes escenarios.

Ord.	Características	Algoritmos / modelos	Accuracy	Precision	Recall
1	Primeras 10 Características	Random Forest	0,9290	0,9170	0,9592
		Mezclas Gaussianas	0,9272	0,9144	0,9591
		Decision Tree	0,9293	0,9190	0,9574
		Naïve Bayes	0,9200	0,9133	0,9460
		Redes Bayesianas	0,9271	0,9132	0,9603
		SVM	0,9266	0,9127	0,9600
		ANN	0,9200	0,9133	0,9460
		Deep Learning	0,9200	0,9127	0,9464
2	Segundas 10 Características	Random Forest	0,6940	0,7040	0,7774
		Mezclas Gaussianas	0,6918	0,7057	0,7647
		Decision Tree	0,6937	0,7049	0,7733
		Naïve Bayes	0,6604	0,6719	0,7603
		Redes Bayesianas	0,6934	0,7013	0,7821
		SVM	0,6910	0,7024	0,7710
		ANN	0,6604	0,6719	0,7603
		Deep Learning	0,6896	0,7025	0,7671

Ord.	Características	Algoritmos / modelos	Accuracy	Precision	Recall
3	Terceras 10 Características	Random Forest	0,7934	0,7963	0,8517
		Mezclas Gaussianas	0,7754	0,7834	0,8311
		Decision Tree	0,7910	0,6961	0,8464
		Naïve Bayes	0,7532	0,7634	0,8205
		Redes Bayesianas	0,7947	0,7966	0,8545
		SVM	0,7770	0,7790	0,8457
		ANN	0,7532	0,7634	0,8205
		Deep Learning	0,7761	0,7797	0,8421
4	Primeras 10 y Segundas 10 Características	Random Forest	0,9513	0,9487	0,9648
		Mezclas Gaussianas	0,9475	0,9435	0,9633
		Decision Tree	0,9477	0,9465	0,9604
		Naïve Bayes	0,9260	0,9144	0,9566
		Redes Bayesianas	0,9494	0,9449	0,9654
		SVM	0,9397	0,9276	0,9672
		ANN	0,9260	0,9144	0,9566
		Deep Learning	0,9412	0,9306	0,9665

Ord.	Características	Algoritmos / modelos	Accuracy	Precision	Recall
5	Primeras 10 y Terceras 10 Características	Random Forest	0,9622	0,9608	0,9719
		Mezclas Gaussianas	0,9575	0,9600	0,9640
		Decision Tree	0,9558	0,9608	0,9599
		Naïve Bayes	0,9266	0,9227	0,9479
		Redes Bayesianas	0,9615	0,9621	0,9691
		SVM	0,9441	0,9378	0,9638
		ANN	0,9266	0,9227	0,9479
		Deep Learning	0,9448	0,9406	0,9618
6	Segundas 10 y Terceras 10 Características	Random Forest	0,8576	0,8590	0,8952
		Mezclas Gaussianas	0,8333	0,8397	0,8720
		Decision Tree	0,8455	0,8525	0,8785
		Naïve Bayes	0,7611	0,7772	0,8142
		Redes Bayesianas	0,8486	0,8526	0,8863
		SVM	0,8304	0,8318	0,8803
		ANN	0,7611	0,7772	0,8142
		Deep Learning	0,8286	0,8375	0,8673

Nota. La tabla muestra los resultados de accuray, presión y recall obtenidos en los diferentes escenarios de clasificación de características de los 8 algoritmos y/o modelos Machine Learning seleccionados.

La Tabla 15 presenta los modelos y/o algoritmos de Machine Learning que obtuvieron la calificación más alta en cada métrica evaluada para cada escenario.

Tabla 15

Ganador de cada escenario

ORD.	ESCENARIO / MÉTRICA	ACCURACY	PRECISION	RECALL
1	Primer Escenario (Primeras 10 Características)	ANN (93,00%)	Decision-Tree (91,90%)	ANN (96,03%)
2	Segundo Escenario (Segundas 10 Características)	Decision- Tree (69,37%)	Mezclas Gaussianas (70,57%)	Redes Bayesianas (78,21%)
3	Tercer Escenario (Terceras 10 Características)	Redes Bayesianas (79,47%)	Redes Bayesianas (79,66%)	Redes Bayesianas (85,45%)
4	Primer y Segundo Escenario (Primeras 10 y Segundas 10 Características)	Random Forest (95,13%)	Random Forest (94,87%)	SVM (96,72%)
5	Primer y Tercer Escenario (Primeras 10 y Terceras 10 Características)	Random Forest (96,22%)	Redes Bayesianas (96,21%)	Random Forest (97,19%)

ORD.	ESCENARIO / MÉTRICA	ACCURACY	PRECISION	RECALL
6	Segundo y Tercer Escenario (Segundas 10 y las Terceras 10 Características)	Random Forest (85,76%)	Random Forest (85,90%)	Random Forest (89,52%)
7	Primer, Segundo y Tercer Escenario (30 Características)	Random Forest (97,10%)	Random Forest (96,68%)	Random Forest (98,18%)

Nota. La tabla muestra los algoritmos y/o modelos como mejor accuracy, precisión y recall para cada escenario de características.

Creación del dataset

Para cumplir con la H.U. 02 y crear el dataset requerido, se llevó a cabo la implementación del código necesario para extraer las 30 características seleccionadas a partir de una URL. Este proceso es esencial para la generación exitosa del dataset. Cada una de las características seleccionadas fue implementada como un método dentro de una clase, donde cada método devuelve un valor numérico que representa la clasificación de la URL. Específicamente, el valor "1" indica que la URL es legítima, "0" denota que es sospechosa, y "-1" señala que es un sitio web con phishing.

Se obtuvo un dataset con 32.040 URLs de sitios web, en dónde 25.151 URLs contenían phishing y 6.889 URLs eran sitios web legítimos, al mezclar de dataset del estudio previo y el nuevo daset obtenido el repositorio de KAGGLE " Url Detection" (ANKIT, 2018), dicho repositorio se encuentra una lista de sitios web tanto legítimos como ilegítimos.

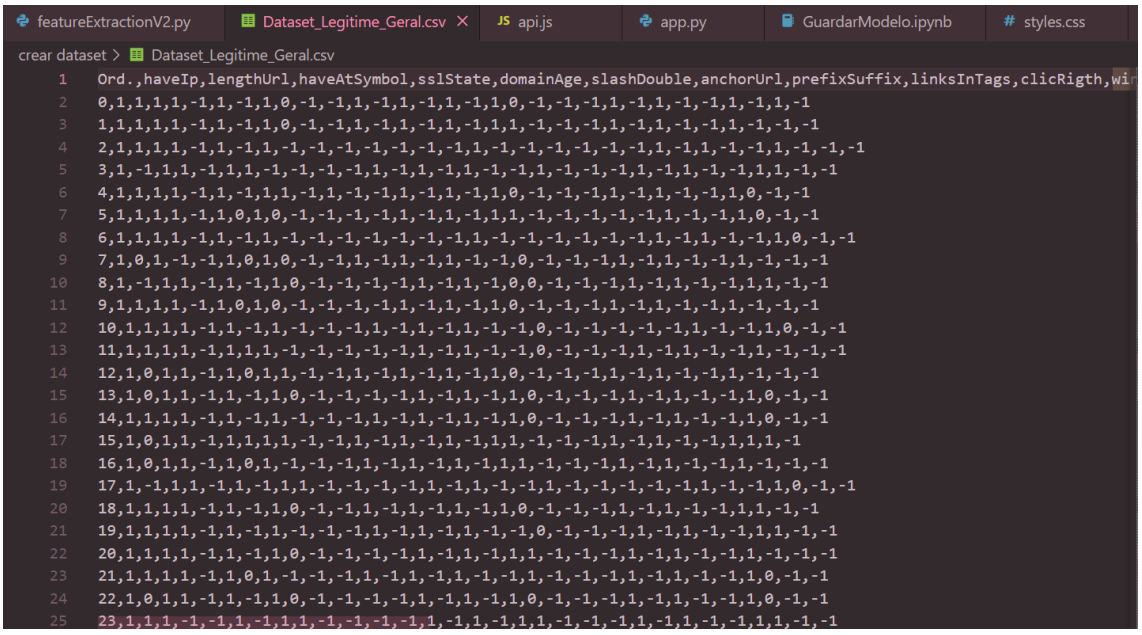
Se implementó un código para llevar a cabo la "limpieza" del dataset mencionado, el cual consiste en leer el dataset y enviar cada URL a través de un servicio GET con un límite de tiempo de 5 segundos.

Posteriormente, basándose en el resultado obtenido de cada URL, se procedió a filtrar las mismas y seleccionar únicamente aquellas que retornaron una respuesta equivalente a 200. Las respuestas con otros valores fueron descartadas, siendo una respuesta 200 indicativo de que la solicitud realizada tuvo éxito.

La Figura 8 muestra una captura de pantalla de una parte del dataset creado durante este sprint. El dataset contiene las características extraídas de cada URL ordenadas, junto con su correspondiente resultado, que puede ser etiquetado como sitio web legítimo (1) o sitio web con phishing (-1).

Figura 8

Dataset creado



Nota. La figura muestra una parte del dataset creado.

Desarrollo de la extensión para Google Chrome.

Sprint 03: Desarrollo de la extensión de Google Chrome

Durante el desarrollo de este Sprint, se consideró la Historia de Usuario H.U. 03, que se encuentra detallada en la Tabla 4. Para el desarrollo de la extensión dedicada a prevenir a los usuarios de sitios web con phishing, se utilizó como punto de partida la estructura del estudio previo (Castillo Veloz &

Chuquitarco Velasco, 2023), el cual se desarrolló una extensión para Google Chrome diseñada específicamente para la detección de phishing en sitios web. A partir de esta estructura base, se procedió a desarrollar las nuevas funcionalidades utilizando CSS3 para el diseño y JavaScript para la implementación de los tres sistemas de prevención con los cuales contara el aplicativo.

Historias de usuario detalladas. La Tabla 16 muestra la Historia de Usuario H.U. 04 del sistema de prevención de phishing (CyberSafeGuard) para el desarrollo de la extensión de Google Chrome. En esta tabla, se detallan los responsables del desarrollo y los criterios de aceptación que se utilizarán para la creación exitosa de la extensión de Google Chrome.

Tabla 16

Historia de usuario para el desarrollo de la extensión de Google Chrome

Historias de Usuario	
Número: H.U. 03	**Usuario:** Usuario de internet
Nombre historia: Desarrollo de la extensión Google Chrome	
Prioridad de negocio: Alta	**Riesgo en desarrollo:** Media
Puntos estimados (días): 20	**Interacción asignada:** 1
Programadores responsables: Geraldyn Semblantes	
Descripción: • Como usuario quiero contar con una extensión para el navegador Google Chrome que sea capaz de prevenirme de acceder a sitios web que contengan phishing.	
Validación (Criterios de aceptación): • La extensión debe funcionar en Google Chrome versión 4.0 o mayor. • La extensión debe prevenir al usuario cuando se encuentre en un sitio web phishing. • La extensión mostrará un mensaje al usuario indicando si el sitio web es legítimo o contiene phishing.	

Historias de Usuario	
Número: H.U. 03	**Usuario:** Usuario de internet
Nombre historia: Desarrollo de la extensión Google Chrome	
Prioridad de negocio: Alta	**Riesgo en desarrollo:** Media
Puntos estimados (días): 20	**Interacción asignada:** 1
Programadores responsables: Geraldyn Semblantes	

Validación (Criterios de aceptación):

- La extensión mostrará un mensaje al usuario sobre que factor de compromiso tiene el sitio web, en caso de ser ilegítimo.
- La extensión deberá bloquear el sitio web ilegítimo.
- La extensión cerrará el sitio web ilegítimo, de manera automática.

Nota. La tabla muestra los detalles de la Historia de Usuario 03 con información relevante como la prioridad, el riesgo de desarrollo, los días estimados para desarrollarse, la interacción asignara, el responsable y así mismo una descripción y criterios de aceptación para la Historio de Usuario.

Sprint Backlog. En la Tabla 16: Sprint Backlog 03, se detallan las actividades realizadas durante el sprint, el responsable de su ejecución, las fechas de planificación para la ejecución del sprint, las estimaciones de tiempo en horas para cada tarea, el esfuerzo real en horas trabajadas cada día y el estado actual de cada tarea. Es importante destacar que el sprint backlog que se presenta ya se encuentra completado.

Tabla 17

Sprint Backlog 03

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	3	27/04/2023	8 horas	24/05/2023	27/04/2023	28/04/2023	01/05/2023	02/05/2023	03/05/2023	04/05/2023	05/05/2023	08/05/2023	09/05/2023	10/05/2023	11/05/2023	12/05/2023	15/05/2023	16/05/2023	17/05/2023	18/05/2023	19/05/2023	22/05/2023	23/05/2023	24/05/2023
	Tareas Pendientes				9	9	8	7	6	6	5	5	5	4	4	3	3	3	3	2	1	1	1	0
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0

Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 03	Investigación de técnicas para prevención de ataques phishing	Revisión de literatura	Geraldyn Semblantes	Finalizado	16	6

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	3	27/04/2023	8 horas	24/05/2023	27/04/2023	28/04/2023	01/05/2023	02/05/2023	03/05/2023	04/05/2023	05/05/2023	08/05/2023	09/05/2023	10/05/2023	11/05/2023	12/05/2023	15/05/2023	16/05/2023	17/05/2023	18/05/2023	19/05/2023	22/05/2023	23/05/2023	24/05/2023	
	Tareas Pendientes				9	9	8	7	6	6	5	5	5	4	4	3	3	3	3	2	1	1	1	0	
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0	

Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 03	Creación de Mockups	Documentación	Geraldyn Semblantes	Finalizado	8	4
H.U. 03	Instalación de aplicativo anterior	Instalación	Geraldyn Semblantes	Finalizado	8	4

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	3	27/04/2023	8 horas	24/05/2023	27/04/2023	28/04/2023	01/05/2023	02/05/2023	03/05/2023	04/05/2023	05/05/2023	08/05/2023	09/05/2023	10/05/2023	11/05/2023	12/05/2023	15/05/2023	16/05/2023	17/05/2023	18/05/2023	19/05/2023	22/05/2023	23/05/2023	24/05/2023	
	Tareas Pendientes				9	9	8	7	6	6	5	5	5	4	4	3	3	3	3	2	1	1	1	0	
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0	

Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 03	Desarrollo de notificación sobre ataque phishing	Codificación	Geraldyn Semblantes	Finalizado	16	6
H.U. 03	Desarrollo de notificación sobre factor de compromiso	Codificación	Geraldyn Semblantes	Finalizado	24	8

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	3	27/04/2023	8 horas	24/05/2023	27/04/2023	28/04/2023	01/05/2023	02/05/2023	03/05/2023	04/05/2023	05/05/2023	08/05/2023	09/05/2023	10/05/2023	11/05/2023	12/05/2023	15/05/2023	16/05/2023	17/05/2023	18/05/2023	19/05/2023	22/05/2023	23/05/2023	24/05/2023	
	Tareas Pendientes				9	9	8	7	6	6	5	5	5	4	4	3	3	3	3	2	1	1	1	0	
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0	

Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 03	Aplicación de diseño a notificaciones	Codificación	Geraldyn Semblantes	Finalizado	16	6
H.U. 03	Desarrollo de bloqueo de sitio web compromiso	Codificación	Geraldyn Semblantes	Finalizado	32	8

	Sprint	Inicio	Jornada	Fin	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X	J	V	L	M	X
	3	27/04/2023	8 horas	24/05/2023	27/04/2023	28/04/2023	01/05/2023	02/05/2023	03/05/2023	04/05/2023	05/05/2023	08/05/2023	09/05/2023	10/05/2023	11/05/2023	12/05/2023	15/05/2023	16/05/2023	17/05/2023	18/05/2023	19/05/2023	22/05/2023	23/05/2023	24/05/2023	
	Tareas Pendientes				9	9	8	7	6	6	5	5	5	4	4	3	3	3	3	2	1	1	1	0	
	Horas Pendientes				160	152	144	136	128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	0	

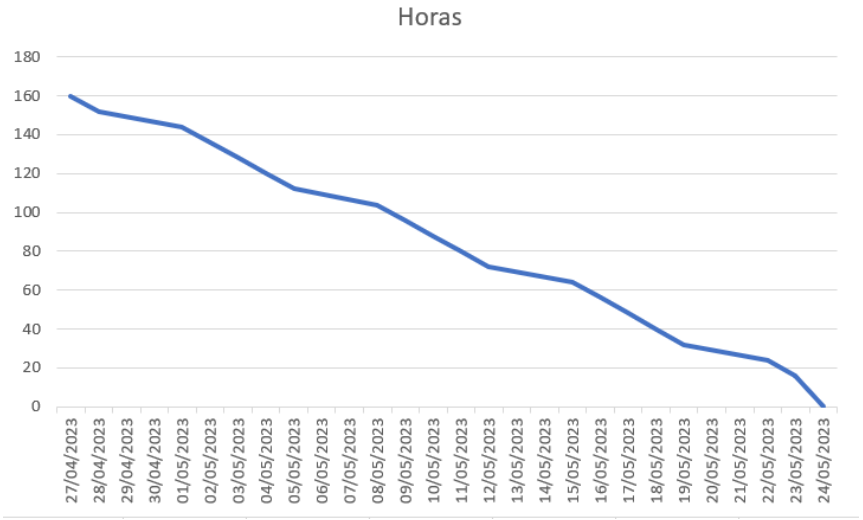
Backlog	Tarea	Categoría	Responsable	Estado	Estimación (Horas)	Esfuerzo
H.U. 03	Aplicación de diseño a página de bloqueo	Codificación	Geraldyn Semblantes	Finalizado	8	6
H.U. 03	Desarrollo de cierre automático de sitio web	Codificación	Geraldyn Semblantes	Finalizado	24	8

Nota. La tabla muestra las actividades que se realizó durarte el Sprint 03, su responsable, horas ocupadas y esfuerzo.

Burndown Chart. La Figura 9 presenta el Burndown Chart del Sprint 03, donde se visualiza el progreso realizado a lo largo del tiempo estimado para el desarrollo de este sprint. El gráfico muestra en su eje X las fechas correspondientes a los días del intervalo de tiempo, que va desde el 27 de abril de 2023 hasta el 24 de mayo de 2023, como se especifica en la Tabla 17. Por otro lado, el eje Y representa el número total de horas estimadas al inicio del sprint, el valor máximo en el eje Y se obtiene multiplicando el número total de días estimado (que en este caso son 20 días) por las horas de trabajo por día (que son 8 horas diarias). Esta multiplicación nos da un valor de 160 horas, que representa el máximo valor en el eje Y del gráfico, entonces a medida que transcurren los días, el valor de horas en el gráfico debe ir disminuyendo progresivamente hasta llegar a cero, lo que indica que el Sprint ha sido completado exitosamente.

Figura 9

Burndown Chart - Sprint 03



Nota. La figura muestra el decrecimiento de las tareas pendientes con relación al número de horas (eje x) y al día (eje y).

Resultados del Sprint. Con la realización de este Sprint inicialmente, se recopilaron artículos científicos relevantes que abordaban métodos y técnicas empleadas en la prevención de intrusiones

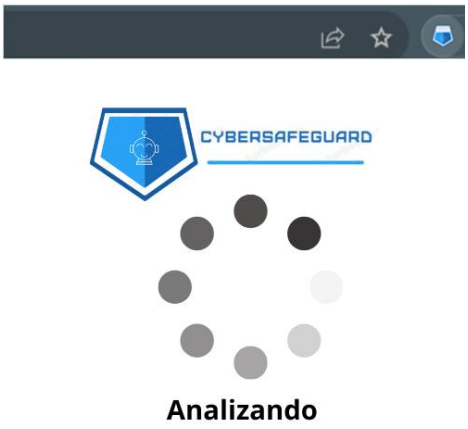
relacionadas con el phishing. A partir de esta revisión, se definieron tres funcionalidades clave, tal como se mencionó en el Capítulo II. Estas funcionalidades consisten en: i) Notificación de sitios web ilegítimos, ii) Notificación de factores de compromiso, iii) Bloqueo de sitios web y iv) Cierre automático de sitios web.

Una vez establecidas estas funcionalidades, se procedió a crear los mockups. Los mockups son representaciones visuales estáticas de un diseño o interfaz de usuario. Son utilizados para mostrar cómo se verá y funcionará una aplicación o sitio web antes de su implementación (O'Sullivan, 2016). Estos mockups se presentan en las Figuras 10,11,12,13 y 14, a continuación.

Mockup 1: La Figura 10: Mockup analizando sitio web, sucede al dar clic en la extensión, esta empezará a analizar la legitimidad del sitio web.

Figura 10

Mockup analizando sitio web

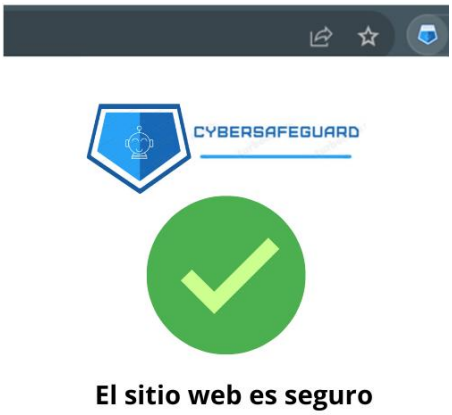


Nota. La figura muestra cómo será visualmente el sistema para el usuario cuando se esté analizando el sitio web.

Mockup 2: La Figura 11: Mockup sitio web legítimo, aparecerá cuando el sitio web sea legítimo.

Figura 11

Mockup sitio web legítimo



Nota. La figura muestra cómo será visualmente el sistema para el usuario cuando el sitio web sea legítimo.

Mockup 3: La Figura 12: Mockup sitio web phishing, aparecerá cuando el sitio web ilegítimo es decir sea un sitio web con phishing.

Figura 12

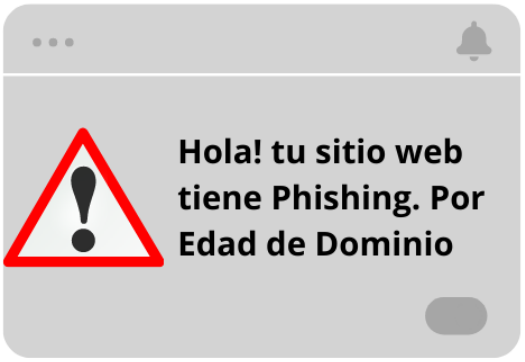
Mockup sitio web phishing

Nota. La figura muestra cómo será visualmente el sistema para el usuario cuando el sitio web sea ilegítimo.

Mockup 4: La Figura 13: Mockup alerta, aparecerá cuando el sitio web sea ilegítimo, informando por qué tiene phishing.

Figura 13

Mockup alerta

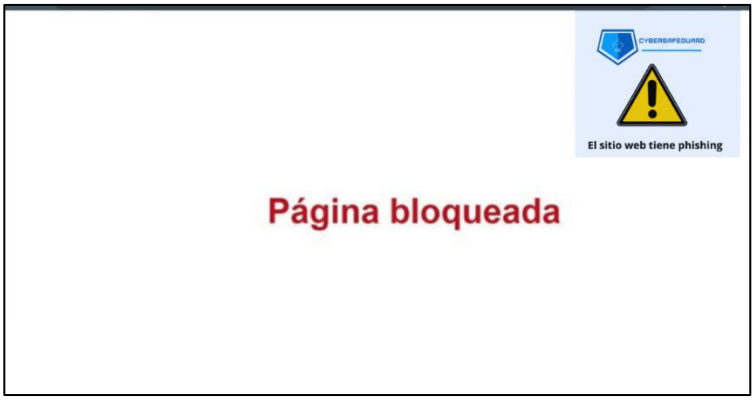


Nota. La figura muestra cómo será visualmente la notificación de Google Chrome para el usuario informando el factor de compromiso que presenta el sitio web.

Mockup 5: La Figura 14: Mockup bloqueo de sitio web, aparecerá cuando el sitio web sea ilegítimo, bloqueando la página.

Figura 14

Mockup bloqueo de sitio web



Nota. La figura muestra cómo será visualmente como será la pantalla de bloqueo del sitio web.

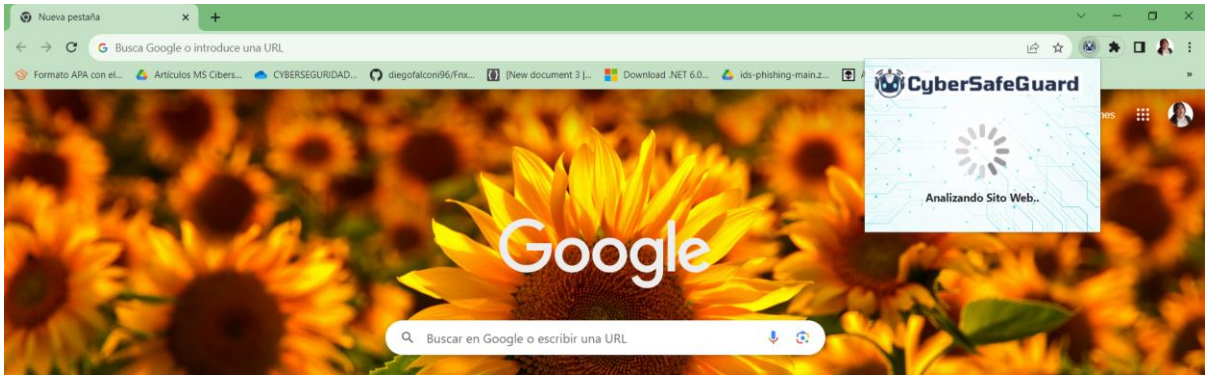
Una vez que el sistema a desarrollar quedo diseñado, el siguiente paso fue implementar el sistema del estudio previo (Castillo Veloz & Chuquitarco Velasco, 2023). Para llevar a cabo esta tarea, se organizó una reunión de trabajo a través de la plataforma Meet con los autores Mishell Castillo y Kevin Chuquitarco. En esta reunión se realizó la entrega de las credenciales de API necesarias para la instalación del sistema. La API toma las peticiones de la extensión de Google Chrome y realiza predicciones de sitios web utilizando su URL con el modelo Machine Learning Random Forest.

Las nuevas funcionalidades de la extensión para la prevención de sitios web con phishing fueron tres principales: la notificación al usuario cuando se encuentra en un sitio web con phishing y el nivel de riesgo que presenta dicho sitio, el bloqueo del sitio web y, por último, el cierre automático del sitio web. Estas funcionalidades se programaron dentro del archivo "manifest.json" y se crearon los scripts correspondientes para cada una de ellas. A continuación, se aplicaron los estilos basados en los mockups presentados en las Figuras 4, 5, 6, 7 y 8.

Las Figuras 15, 16 y 17 muestra el resultado final de este Sprint, con la extensión de Google Chrome completamente desarrollada.

Figura 15

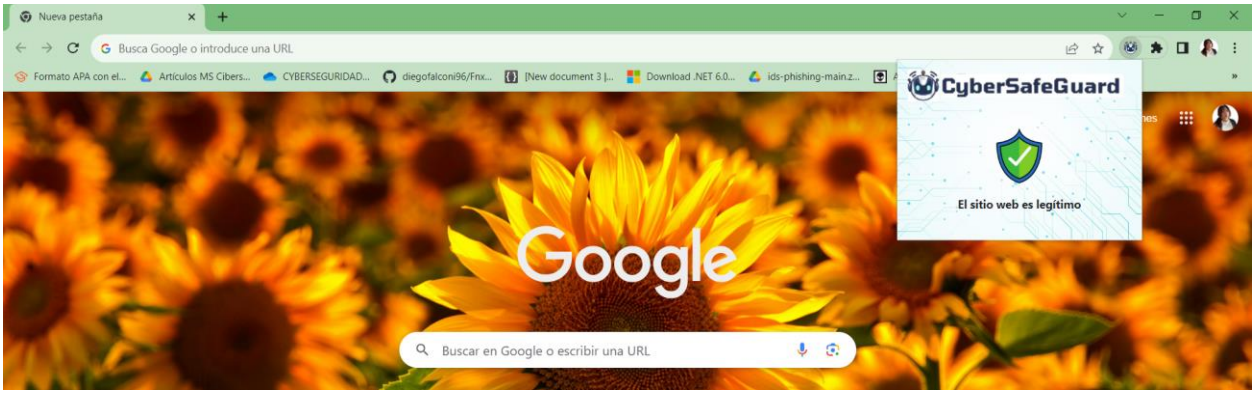
Extensión de Google Chrome desarrollada analizando el sitio web



Nota. La figura muestra la ejecución de la extensión (parte superior derecha), la cual está consumiendo el servicio web previamente desarrollado.

Figura 16

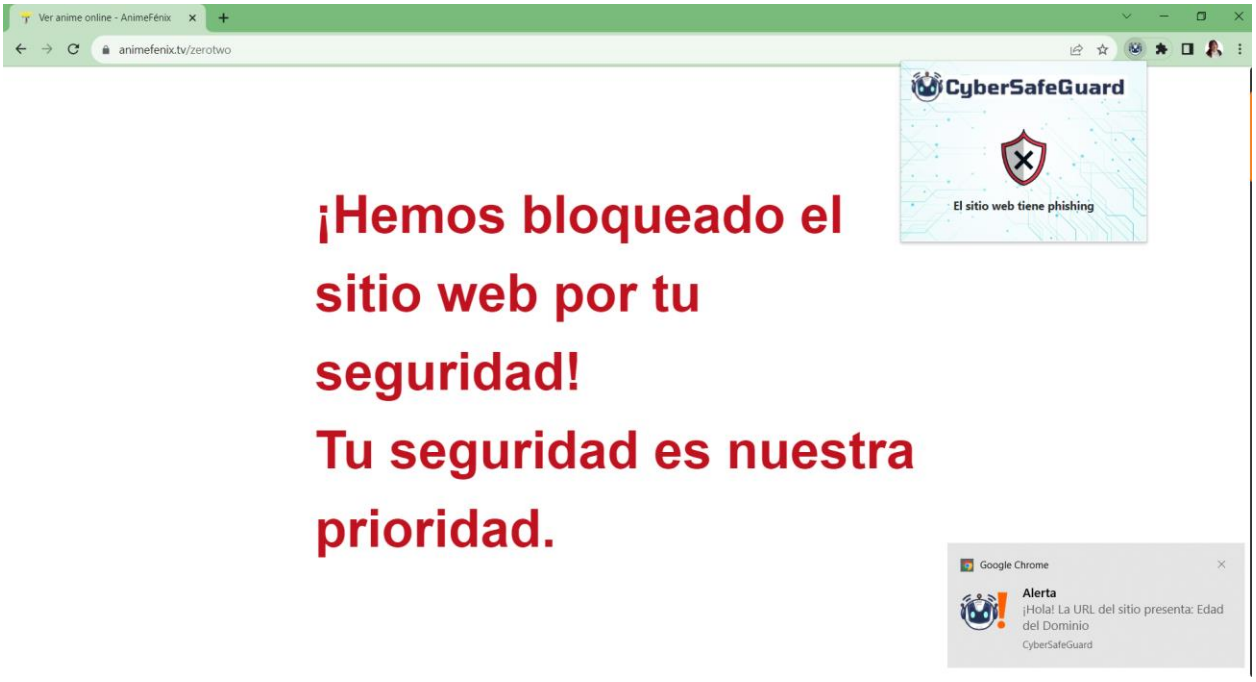
Extensión de Google Chrome desarrollada sitio web legítimo



Nota. La figura muestra la notificación de la extensión (parte superior derecha), cuando el sitio web sea legítimo.

Figura 17

Extensión de Google Chrome desarrollada sitio web ilegítimo



Nota. Se muestra el sitio con phishing bloqueado, la notificación de la extensión (parte superior derecha) cuando el sitio web sea legítimo. Y la notificación de Google Chrome (parte inferior izquierda), con el mensaje del sitio web con phishing y el factor de compromiso que presento el sitio web.

Capítulo IV

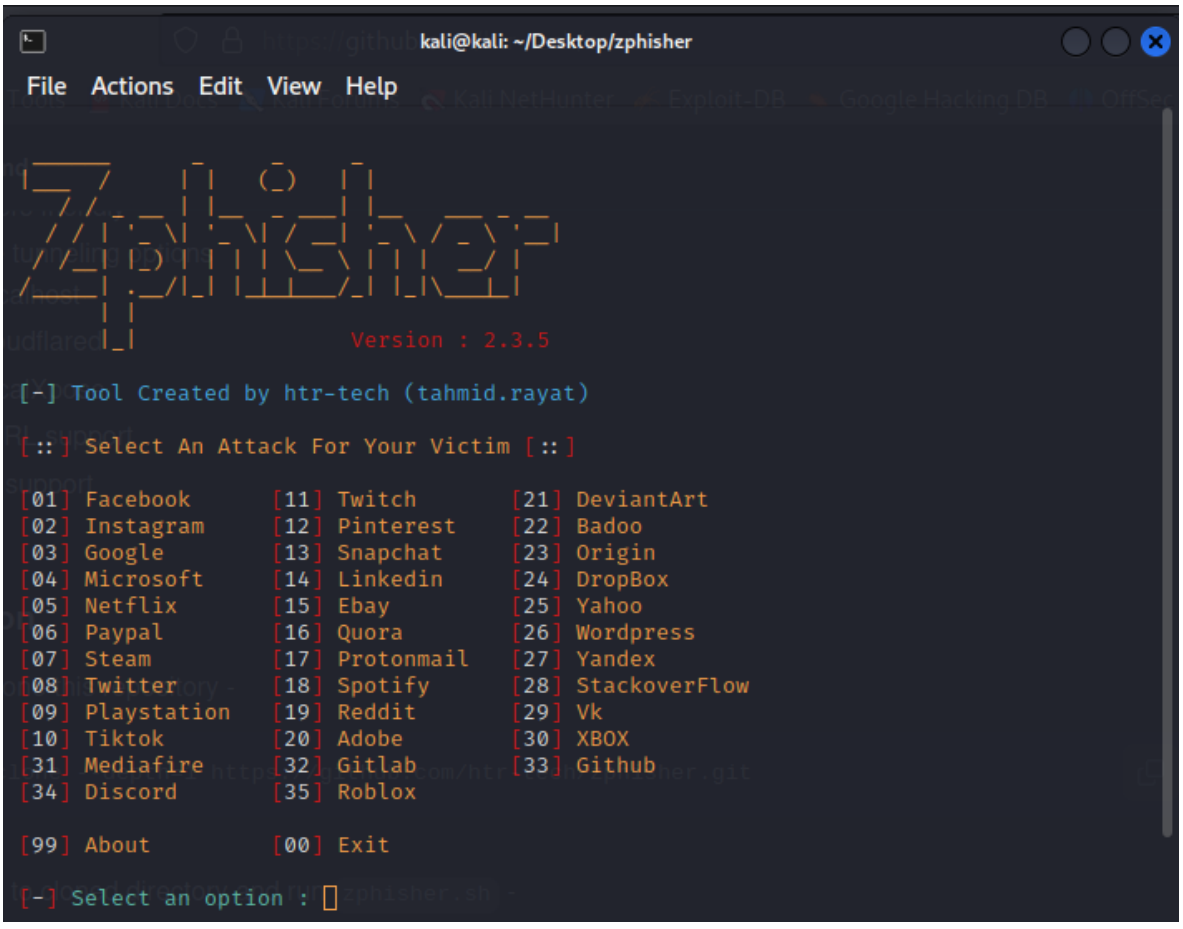
Validación Del Sistema

En este capítulo se hace uso de las herramientas Zphisher y PyPhisher, las cuales se encuentran disponibles en el sistema operativo Kali Linux, con el fin de probar la extensión CyberSafeGuard.

La herramienta con Zphisher, se crea URLS de sitios web falsos que imiten sitios web legítimos (Alshabib *et al*., 2022) mostrados en la Figura 18. Por otra parte, Pyphisher es una herramienta de phishing en Python que incluye sitios web populares como Facebook, Twitter, Instagram, Gmail y muchos otros, incluye 65 sitios web (Kothamasu *et al*., 2023) mostrado en la Figura 19.

Figura 18

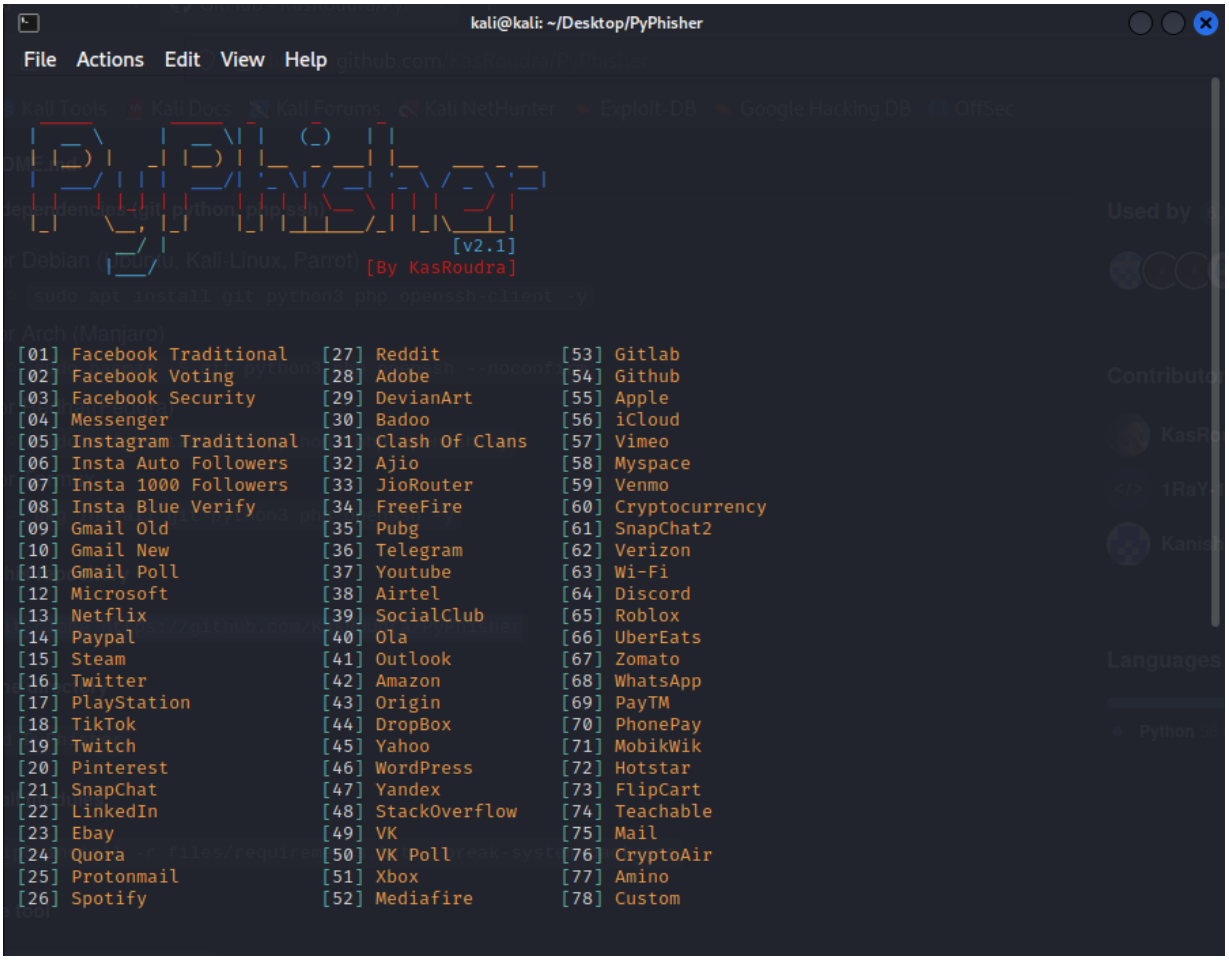
Ataques disponibles Zphisher



Nota. La figura muestra la herramienta Zphisher con sus opciones de sitio web.

Figura 19

Ataques disponibles Pyphisher



Nota. La figura muestra la herramienta Pyphisher con sus opciones de sitio web.

Para las pruebas se hizo uso de dos equipos: el primero con Kali Linux en una máquina virtual, con el que se generó los ataques de phishing. Y en el segundo equipo se encontraba instalada la extensión de Google Chrome (CyberSafeGuard), que se utilizó para evaluar la prevención de sitios web con phishing. Después de que el ataque es lanzado desde el primer equipo, se accede al sitio web desde el segundo equipo con el fin de examinar su contenido y registrar el resultado obtenido. Se muestra gráficamente el proceso de pruebas en la Figura 20.

Figura 20

Proceso de ejecución de pruebas

Nota. La figura muestra el proceso de ejecución de cómo se realizó las pruebas usando dos computadores, uno con Kali Linux (PC1) y otro con Windows (PC2) y se iba documentando los resultados.

Definición y aplicación de métricas de pruebas

Aplicación de las pruebas

Para llevar a cabo la evaluación de métricas, se inició con la ejecución de pruebas de la extensión CyberSafeGuard utilizando el primer modelo de Machine Learning entrenado. Estas pruebas se realizaron mediante las herramientas Zphisher y Pyphisher, y los resultados obtenidos se presentan detalladamente en la Tabla 20: Resultados de las pruebas de CyberSafeGuard con el primer modelo de Machine Learning. En esta tabla se presentan los resultados de las evaluaciones al sistema CyberSafeGuard. Para estas evaluaciones, se utilizaron 86 sitios web ilegítimos, creados a través del uso de ZPhisher (43 sitios web) y Pyphisher (43 sitios web) y 43 sitios web legítimos pertenecientes a la misma sección del sitio web.

El “Login Page", que es la primera interfaz que un usuario visualiza y donde ingresa sus datos privados en un sistema web fue tomada con mayor consideración en los sitios web puestos a prueba, debido a que la mayoría de sitios cuenta con esta. No obstante, para alcanzar el total de 86 sitios web

mencionados, se optó por seleccionar múltiples secciones de diversos sitios web, en su mayoría enfocadas en áreas que demandan la introducción de datos por parte del usuario, todas ellas susceptibles de ser generadas por Zphisher y Pyphisher.

Tabla 18

Resultados pruebas de CyberSafeGuard con primer modelo de Machine Learning

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Facebook	1	Tradicional Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
	2	Advanced Voting Poll Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
	3	Fake Security Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
	4	Facebook Messenger Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Instagram	5	Traditional Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
	6	Auto Followers Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
	7	1000 Followers Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
	8	Blue Badge Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
Google	9	Gmail Old Login Page	Phishing	Phishing	Legítimo	Legítimo	Legítimo
	10	Gamil New Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
	11	Advanced Voting Poll	Phishing	Phishing	Phishing	Legítimo	Legítimo

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Microsoft	12	Microsoft Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
Netflix	13	Netflix Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
PayPal	14	PayPal Login Page	Phishing	Phishing	Legítimo	Legítimo	Legítimo
Steam	15	Steam Login Page	Phishing	Phishing	Legítimo	Legítimo	Legítimo
Twitter	16	Twitter Login Page	Phishing	Phishing	Phishing	Legítimo	Phishing
PlayStation	17	PlayStation Login Page	Phishing	Phishing	Phishing	Legítimo	Phishing
Tiktok	18	Tiktok Login Page	Phishing	Phishing	Legítimo	Legítimo	Legítimo

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Twitch	19	Twitch Login Page	Phishing	Phishing	Legítimo	Legítimo	Legítimo
Pinterest	20	Pinterest Login Page	Phishing	Phishing	Legítimo	Legítimo	Phishing
Snapchat	21	Snapchat Login Page	Phishing	Phishing	Legítimo	Legítimo	Legítimo
Linkedin	22	Linkedin Login Page	Phishing	Phishing	Legítimo	Legítimo	Legítimo
Ebay	23	Ebay Login Page	Phishing	Phishing	Legítimo	Legítimo	Legítimo
Quora	24	Quora Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
Protonmail	25	Protonmail Login Page	Phishing	Phishing	Legítimo	Legítimo	Legítimo

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Spotify	26	Spotify Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Reddit	27	Reddit Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Adobe	28	Adobe Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
DeviantArt	29	DeviantArt Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Badoo	30	Badoo Login Page	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**	**Legítimo**
Origin	31	Origin Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
DropBox	32	DropBox Login Page	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**	**Legítimo**

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Yahoo	33	Yahoo Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
Wordpress	34	Wordpress Login Page	Phishing	Phishing	Legítimo	Legítimo	Phishing
Yandex	35	Yandex Login Page	Phishing	Phishing	Phishing	Legítimo	Phishing
StackoverFlow	36	StackoverFlow Login Page	Phishing	Phishing	Legítimo	Legítimo	Legítimo
VK	37	Traditional Login Page	Phishing	Phishing	Legítimo	Legítimo	Phishing
	38	Advanced Voting Poll Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
XBOX	39	XBOX Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Mediafire	40	Mediafire Login Page	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**	**Legítimo**
Gitlab	41	Gitlab Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Phishing**
Github	42	Github Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Discord	43	Discord Login Page	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**	**Legítimo**
SITIOS WEB BIEN CLASIFICADOS					26		37
SITIOS WEB MAL CLASIFICADOS					17		6

Nota. La tabla muestra los resultados esperados y los resultados obtenidos de las pruebas realizadas al sistema en un total de 46 sitios web.

Se creo la matriz de confusión usando los resultados anteriores.

Tabla 19

Matriz de confusión del primer modelo Machine Learning

	POSITIVOS	**NEGATIVOS**
POSITIVOS	**26 (VP)**	**6 (FP)**
NEGATIVOS	**17 (FN)**	**37 (VN)**

Nota. La tabla muestra los datos obtenidos de la Tabla 18 para la matriz de confusión

Se empleo las fórmulas indicadas en la Tabla 4 para calcular las métricas de precisión, recall y accuracy, cuyos resultados son presentados en la Tabla 20: Resultados de las métricas de evaluación calculadas.

Tabla 20

Métricas de evaluación calculadas

MÉTRICA DE EVALUACIÓN	**RESULTADO**
Accuracy	0,73 (73%)
Precision	0,81 (81%)
Recall	0,60 (60%)

Nota. La tabla muestra el accuracy, precisión y recall obtenidos aplicando las métricas de evaluación.

Se obtuvo que la clasificación correcta (accuracy) de los sitios web es de 73%. Los sitios web phishing determinados como tal (precisión) es de 81% y los sitios bien clasificados y mal clasificados (recall) es 60%.

Identificación de errores

Tras la aplicación de las métricas de evaluación al primer modelo, se lograron identificar los siguientes errores:

- Las métricas de evolución presentan un valor relativamente bueno, pero no perfecto.
- No se identificas a los sitios ilegítimos con presencia de phishing.
- Los sitios legítimos son clasificados como sitios con phishing.

Corrección de errores y ajuste de modelos

Corrección y primer ajuste del modelo

Se planteó una solución que implicaba la ampliación del conjunto de datos de entrenamiento con sitios web adicionales, tanto de phishing como legítimos. El propósito detrás de esta medida era mejorar los niveles de precisión del modelo. Esta acción resultó en una mejora notable en las métricas de evaluación. La tasa de precisión (Accuracy) aumentó en un 1,65%, la precisión (Precision) mejoró en un 0,41% y el alcance (Recall) experimentó un incremento de 0,03% en comparación con los valores obtenidos en el primer modelo entrenado en el capítulo 3: Implementación del Sistema. Para respaldar la afirmación de que los porcentajes de precisión no son tan bajos, se tomó la decisión de ampliar el conjunto de datos en un modesto 3.06%. Esta expansión consistió en la incorporación de 339 URLs adicionales de sitios web legítimos, con el propósito de fortalecer el nivel de precisión. Estas URLs fueron derivadas del análisis detallado realizado en el estudio de (Kothamasu et al., 2023). Con la inclusión de este nuevo conjunto de datos, se procedió a llevar a cabo un nuevo proceso de entrenamiento del modelo de Machine Learning (Random Forest). Cabe recordar que este modelo fue previamente elegido y aplicado en el capítulo 3: Implementación del Sistema.

Después de completar el entrenamiento del modelo, se procedió a aplicar las métricas de evaluación correspondientes, obteniendo los siguientes resultados: un Accuracy de 98,75% %, una

Precision de 97,09% y un Recall de 98,21%. En la Tabla 21, se aprecia una notoria mejora en las métricas de evaluación.

Tabla 21

Comparación de modelos sin ajustar y ajustado

	Accuracy	**Precision**	**Recall**
Modelo Sin Ajustar	97,10%%	96,68%	98,18%
Modelo Ajustado	98,75%	97,09%	98,21%
% Incremento	1,65%	0,41%	0,03%

Nota. La tabla muestra el accuracy, precisión y recall obtenidos aplicando las métricas de evaluación en el modelo sin ajustar y en el modelo ajustado. Además del incremento que representa.

Aplicación de métricas de evaluación del modelo ajustado

Se llevaron a cabo una vez más las pruebas idénticas a la extensión CyberSafeGuard, esta vez utilizando el modelo de Machine Learning ajustado. Se llevaron a cabo las mismas pruebas tal como se detalla en la sección 4.1.2, donde se aplicaron las métricas de evaluación utilizando las herramientas Zphisher y Pyphisher. Los resultados de estas pruebas se presentan en la Tabla 22: Resultados de las pruebas de CyberSafeGuard con el modelo de Machine Learning ajustado.

Tabla 22

Resultados pruebas de CyberSafeGuard con modelo de ML ajustado

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Facebook	1	Tradicional Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
	2	Advanced Voting Poll Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
	3	Fake Security Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
	4	Facebook Messenger Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Instagram	5	Traditional Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
	6	Auto Followers Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
	7	1000 Followers Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
	8	Blue Badge Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
Google	9	Gmail Old Login Page	Phishing	Phishing	Legítimo	Legítimo	Legítimo
	10	Gamil New Login Page	Phishing	Phishing	Phishing	Legítimo	Legítimo
	11	Advanced Voting Poll	Phishing	Phishing	Phishing	Legítimo	Legítimo

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Microsoft	12	Microsoft Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Netflix	13	Netflix Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
PayPal	14	PayPal Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Steam	15	Steam Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Twitter	16	Twitter Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Phishing**
PlayStation	17	PlayStation Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Tiktok	18	Tiktok Login Page	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**	**Legítimo**

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Twitch	19	Twitch Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Pinterest	20	Pinterest Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Snapchat	21	Snapchat Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Linkedin	22	Linkedin Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Ebay	23	Ebay Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Quora	24	Quora Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Protonmail	25	Protonmail Login Page	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**	**Legítimo**

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
Protonmail	25	Protonmail Login Page	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**	**Legítimo**
Spotify	26	Spotify Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Reddit	27	Reddit Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Adobe	28	Adobe Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
DeviantArt	29	DeviantArt Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Badoo	30	Badoo Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Origin	31	Origin Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
DropBox	32	DropBox Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Yahoo	33	Yahoo Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Wordpress	34	Wordpress Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Yandex	35	Yandex Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
StackoverFlow	36	StackoverFlow Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
VK	37	Traditional Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Phishing**
	38	Advanced Voting Poll Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**

SITIO WEB	ORD.	SECCIÓN DEL SITIO WEB	PRUEBAS SITIOS WEB PHISHING			PRUEBAS SITIOS WEB LEGÍTIMOS	
			RESULTADO ESPERADO ZPHISHER	RESULTADO ESPERADO PYPHISHER	PREDICCIÓN	RESULTADO ESPERADO	PREDICCIÓN
XBOX	39	XBOX Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Mediafire	40	Mediafire Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Gitlab	41	Gitlab Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Github	42	Github Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
Discord	43	Discord Login Page	**Phishing**	**Phishing**	**Phishing**	**Legítimo**	**Legítimo**
SITIOS WEB BIEN CLASIFICADOS					40		41
SITIOS WEB MAL CLASIFICADOS					3		2

Nota. La tabla muestra los resultados esperados y los resultados obtenidos de las pruebas realizadas al sistema en un total de 46 sitios web.

Se hizo la matriz de confusión con los resultados

Tabla 23

Matriz de confusión modelo ajustado

	POSITIVOS	NEGATIVOS
POSITIVOS	**40 (VP)**	**2 (FP)**
NEGATIVOS	**3 (FN)**	**41 (VN)**

Nota. La tabla muestra los datos obtenidos de la Tabla 22 para la matriz de confusión

Luego, se emplean las fórmulas indicadas en la Tabla 4, lo que nos lleva a obtener los resultados presentes en la Tabla 24: Métricas de evaluación calculadas para el modelo ajustado.

Tabla 24

Métricas de evaluación calculadas modelo ajustado

MÉTRICA DE EVALUACIÓN	RESULTADO
Accuracy	0,9419 (94,19%)
Precision	0,9524 (95,24%)
Recall	0,9302 (93,02%)

Nota. La tabla muestra el accuracy, precisión y recall obtenidos aplicando las métricas de evaluación.

Análisis de resultados

En la fase de entrenamiento del sistema de las métricas de evaluación fueron: accuracy con un 97,10%, precisión con un 96,68% y recall con un 98,18%.

Para evaluar la eficacia de la aplicación, se sometió a pruebas en entornos simulados y reales, con un conjunto total de 129 sitios web de prueba. En el escenario simulado (ambiente controlado), se

utilizaron 83 sitios web generados mediante las herramientas Zphisher y Pyphisher. Por otro lado, en el escenario real (ambiente no controlado), se emplearon los mismos 43 sitios web legítimos (originales).

Una vez puesto esté en funcionamiento en un entorno real/controlado nos dio como resultado un accuracy 73%, para precisión 81% y para recall 60%. Esto puede suceder por diferentes razones una de ellas es que la naturaleza del phishing es dinámica y está en constante evolución, lo que dificulta la creación de un modelo único y estático capaz de capturar todas las variantes de ataque (Yang *et al*., 2019).

Como se determinó que los niveles de aceptación eran muy bajos para el sistema se procedió a realizar un ajuste del modelo y se puso una vez más a prueba, a partir del cual se obtuvieron las medias de cada métrica de evaluación, dando como resultado los siguientes valores: 94,19% de precisión, 95,24% de precisión y 93,02% de recall.

Tabla 25

Comparación de modelos sin ajustar y primer ajuste – métricas de evaluación del modelo

	Etapa de entrenamiento			**Campo simulado/real**		
	Accuracy	**Precision**	**Recall**	**Accuracy**	**Precision**	**Recall**
Modelo	97,10%	96,68%	98,18%	73%	81%	60%
Modelo primer ajuste	98,75%	97,09%	98,21%	94,19%	95,24%	93,02%

Nota. La tabla muestra el accuracy, precisión y recall obtenidos en la etapa del entrenamiento (columna izquierda) y en la etapa de pruebas (columna derecha) tanto como del modelo inicial como del modelo con el primer ajuste.

Los resultados presentados confirman la existencia de una diferencia significativa entre el modelo entrenado y el modelo sometido a pruebas en un entorno simulado/real. Como se observa en la Tabla 20, se presentaban errores en la clasificación de ciertos sitios web como legítimos cuando en

realidad eran phishing, y viceversa, algunos sitios web legítimos fueron clasificados erróneamente como phishing: es por ello que se procedió a realizar ajustes en el modelo.

A diferencia de estudios previos, este análisis no demandó ajustes significativos para alcanzar niveles de accuracy aceptables sido el más bajo 97,10% y el más alto 98,75%, estos valores están dentro del rango previo en el caul se obtuvo un Accuracy mas alto del 93,02%. Esto se debe a que el modelo se entrenó desde el inicio con un conjunto de datos más amplio y se sometió a pruebas exhaustivas utilizando dos herramientas para verificar su eficacia de manera más sólida.

Capítulo V

Conclusiones y Recomendaciones

Conclusiones

A continuación, se presentan las conclusiones derivadas del desarrollo de esta investigación:

- Los resultados obtenidos, se encontró que no todos los modelos de Machine Learning y, además, los algoritmos, no se pueden utilizar en la ejecución de sistemas de interrupción dirigidas a la prevención de phishing. En esta circunstancia específica, el cálculo de K-Means integra información en un conjunto de datos en vista de los elementos presentes en el conjunto de datos, lo que provoca resultados poco notables y poco fiables. La utilización de cálculos de agrupación es un paso intermedio, ya que funcionan de forma indirecta. Por otra parte, Navie Bayes es un cálculo rápido y básico, pero puede no ser lo suficientemente delicado para identificar las intrincadas conexiones fundamentales de los ataques de phishing. Por otro lado, las Redes bayesianas pueden experimentar problemas a la hora de demostrar información compleja.
- Para la creación de la aplicación IPS, denominada CyberSafeGuard, se llevó a cabo el proceso de entrenamiento utilizando un conjunto de datos que incluye tanto sitios web legítimos como ilegítimos, con un total de 32.040 sitios web y usando los recursos de comprobación del estudio anterior, un total de 30 características. Durante este proceso, se exploraron y evaluaron seis modelos y/o técnicas distintas de Machine Learning. Como este análisis, se llegó a la conclusión de que el modelo Random Forest presenta un desempeño mayor en términos de accuracy, precision y recall. Estos resultados cumplen con el primer objetivo del estudio, conocer el estado del arte sobre métodos y técnicas de Machine Learning enfocados a IPS de phishing.
- Con el propósito de alcanzar el segundo objetivo específico, se procedió a desarrollar la extensión CyberSafeGuard para el navegador Google Chrome, en la cual se implementa la

tecnología de Machine Learning con el fin de prevenir la interacción de los usuarios con sitios web potencialmente ilegítimos, asegurando así la seguridad de los mismos.

- Para validar la eficacia del sistema, se llevaron a cabo pruebas en ambientes tanto controlados como reales, haciendo uso de herramientas como Zphisher y Pyphisher. Con el fin de verificar la efectividad del sistema CyberSafeGuard y, en caso necesario, realizar ajustes al modelo. Con fin el fin de cumplir con el tercer objetivo específico del estudio: Validar los resultados, analizar los errores y ajustar los modelos del sistema de prevención de intrusos
- Scrum ha demostrado ser una metodología eficaz para la ejecución de este proyecto, permitiendo una gestión ágil y una adaptación continua a los requisitos cambiantes. Su enfoque iterativo y su énfasis en la retroalimentación constante han sido fundamentales para lograr los objetivos planteados de manera exitosa.
- La extensión de Google Chrome desarrollado (CyberSafeGuard) demuestra su viabilidad en un entorno real, pero es importante destacar la necesidad de un entrenamiento periódico para mantenerse al día con las nuevas formas de phishing que puedan surgir.

Recomendaciones

- Se sugiere realizar una revisión literaria previa al estudio para obtener un mejor entendimiento de los conceptos, métricas y tecnologías que se utilizarán en el desarrollo posterior.
- Es aconsejable utilizar bases de datos indexadas como SCOPUS e IEEE para extraer estudios que se alineen con el tema de investigación, garantizando así fuentes confiables y comparativas relevantes.
- En relación al desarrollo de la aplicación, se recomienda emplear conjuntos de entrenamiento más amplios que contengan una mayor cantidad de datos (URLs) para mejorar aún más la precisión de las predicciones.
- El uso de herramientas para realizar pruebas en entornos controlados y reales es altamente recomendado, ya que proporciona datos concretos sobre la efectividad de la aplicación en situaciones reales.
- Se recomienda aumentar la variedad de recursos de verificación (características) para enriquecer el proceso de entrenamiento de la aplicación y, por ende, mejorar su capacidad predictiva.

Bibliografía

Adil, M., Khan, R., & Nawaz Ul Ghani, M. A. (2020). Preventive techniques of phishing attacks in networks. *2020 3rd International Conference on Advancements in Computational Sciences (ICACS)*.

Al, R. (2005). *Ingenieria en Software*.

Alshabib, O., Jabeur R. A., & Alserhani, F. M. (2022). Digital Forensic Analytics in Social Media Environment Using DNN Approach. *Journal of Theoretical and Applied Information Technology*, *100*(19).

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

ANKIT. (2018). url detection [Data set]. En *KAGGLE*. https://www.kaggle.com/datasets/aktank/url-detection

Anupam, S., & Kar, A. K. (2020). Phishing website detection using support vector machines and nature-inspired optimization algorithms. *Telecommunication Systems*. https://doi.org/10.1007/s11235-020-00739-w

Aung, Y. Y., & Min, M. M. (2018). An analysis of K-means algorithm based network intrusion detection system. *Advances in Science Technology and Engineering Systems Journal*, *3*(1), 496–501. https://doi.org/10.25046/aj030160

AWS. (2023). *¿Qué es el aprendizaje automático?* AWS AMAZON. https://aws.amazon.com/es/what-is/machine-learning/

Balamurugan, V., & Saravanan, R. (2019). Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation. *Cluster Computing*, *22*(S6), 13027–13039. https://doi.org/10.1007/s10586-017-1187-7

Bass, L., Clements, P., & Kazman, R. (2022). *Software architecture in practice* (4a ed.). Addison Wesley.

Beazley, D. (2009). *Python Essential Reference*. Addison-Wesley Professional.

Bishop, C. M. (2006). *Pattern recognition and machine learning*. Springer.

Breiman, L. (2001). Random forests. *Machine learning*, *45*, 5-32.

Breiman, L., Friedman, J. H., Olshen, R. A., & Stone, C. J. (2017). *Classification And Regression Trees*. Routledge.

Bruce S. (2020). *Click here to kill everybody*. Mao Tou Ying.

Bubukayr, M., & Frikha, M. (2023). Effective Techniques for Protecting the Privacy of Web Users. *Applied Sciences.*, *13*(5), 3191.

Butnaru, A., Mylonas, A., & Pitropakis, N. (2021). Towards lightweight URL-based phishing detection. *Future Internet*, *13*(6), 154. https://doi.org/10.3390/fi13060154

Cárdenas, A. J. (2017, mayo 4). *Google revela ataques de 'phishing' a usuarios de Docs*. Expansión. https://expansion.mx/tecnologia/2017/05/03/google-revela-ataques-de-pishing-a-usuarios-de-docs

Carvalho, J., Ponti, M., & Veiga, L. (2017). Anomaly detection in network traffic using machine learning techniques. *In International Conference on Availability, Reliability, and Security*, 323-337.

Castillo Veloz, M. E., & Chuquitarco Velasco, K. J. (2023). *Sistema de detección de intrusos en sitios web, usando modelos y/o algoritmos de Machine Learning: caso práctico Phishing Google Chrome*. Universidad de las Fuerzas Armadas ESPE.

Castro Moreno, J. W. (2022). *Domain Spoofing Attack*.

Chakraborty, N. (2013). Intrusion detection system and intrusion prevention system: A comparative study. *International Journal of Computing and Business Research (IJCBR)*, *4*(2), 1-8.

Chawla, A. (2022). Phishing website analysis and detection using Machine Learning. *International Journal of Intelligent Systems and Applications in Engineering*, *10*(1), 10–16. https://doi.org/10.18201/ijisae.2022.262

Chen, S., Zhou, L., & Li, Y. (2020). A Study on Security of Website Closing. *IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE)*, 117-120.

Chiew, K. L., Choo, J. S.-F., Sze, S. N., & Yong, K. S. C. (2018). Leverage website favicon to detect phishing websites. *Security and communication networks*, *2018*, 1–11. https://doi.org/10.1155/2018/7251750

Chong, H., & Shim, J. (2019). Predictive Machine Learning Models for Phishing Detection and Prevention. *International Conference on New Technologies, Mobility and Security*, *10*, 1–5.

Chrome Extensions getting started guides. (s/f). Chrome Developers. Recuperado el 15 de agosto de 2023, de https://developer.chrome.com/docs/extensions/mv3/getstarted/

Ciberseguridad. (2021, abril 7). *Ciberataques. Guía para la gestión y notificación de ataques informáticos*. Ciberseguridad. https://ciberseguridad.com/ciberataques/

Cohn, M. (2004). *User stories applied: For agile software development*. Addison-Wesley Professional.

Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine Learning*, *20*(3), 273–297. https://doi.org/10.1007/bf00994018

CSS tutorial. (2023). W3schools.com. https://www.w3schools.com/css/

Deshpande, A., Pedamkar, O., Chaudhary, N., & Borde, S. (2021). . Detection of phishing websites using Machine Learning. *International Journal of Engineering Research & Technology (IJERT)*, *10*(05).

Fernandes, E., Laskov, P., & Kirda, E. (2016). Detecting credential spearphishing attacks in enterprise settings. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1475–1487.

Fortinet. (2023). *¿Qué es un IPS (Sistema de Prevención de Intrusiones)?* Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/what-is-an-ips

Gao, J., Zhang, Y., Li, B., Zhao, Q., Li L., & Zhang, X. (2019). A deep learning approach to network traffic classification for intrusion detection systems. *IEEE Access.*

Gokhale, M., Frigo, J., Mccabe, K., Theiler, J., Wolinski, C., & Lavenier, D. (2003). Experience with a hybrid processor: K-means clustering. *The Journal of Supercomputing,* 131-148.

Grinberg, M. (2018). *Flask web development: Developing web applications with python* (2a ed.). O'Reilly Media.

Gunnarsson, P., Jakobsson, A., & Carlsson, N. (2022). On the impact of internal webpage selection when evaluating ad blocker performance. *2022 30th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*.

Hastie, T., Tibshirani, R., & Friedman, J. (2017). *The elements of statistical learning: Data mining, inference, and prediction, second edition* (2a ed.). Springer.

Hernández Báez, I. (2016). *Clasificador bayesiano ingenuo en RapidMiner*. Universidad Autónoma de Puebla.

Hr, M. G., Mv, A., Prasad, G., & Vinay. (2020). Development of anti-phishing browser based on random forest and rule of extraction framework. *Cybersecurity*, *3*(1). https://doi.org/10.1186/s42400-020-00059-1

Huang, R., Wang, B., X., Z., Chen, J., & Wang, X. (s/f). Detecting application-layer DoS attacks with machine learning. *IEEE Transactions on Network and Service Management*, 1499-1512.

Iglesias, P. F. (2017, julio 25). *Al hilo de los certificados SSL: seguridad no implica legitimidad*. PabloYglesias | seguridad + privacidad + tecnología; PabloYglesias. https://www.pabloyglesias.com/ssl-campanas-phishing/

Iqbal, R., Khan, N., Khan, A., & Raza, M. (2020). An Empirical Study on Impact of Web Browser Extensions on User Experience. *Journal of Software Evolution and Process*, 32.

IT Digital Media Group. (2018). *Del Phishing al smishing | Reportajes | IT Digital Security*. https://www.itdigitalsecurity.es/reportajes/2018/03/del-phishing-al-smishing

Jones, D. (2021, agosto 17). *How much does phishing really cost the enterprise?* Cybersecurity Dive. https://www.cybersecuritydive.com/news/phishing-cost-enterprise/605110/

Kamalam, G. K., Suresh, P., Nivash, R., Ramya, A., & Raviprasath, G. (2022). Detection of phishing websites using machine learning. *2022 International Conference on Computer Communication and Informatics (ICCCI)*.

Kaur, S., & Singh, R. (2020). A Comprehensive Study of Web Security Threats and its Countermeasures. *10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 329–334.

Khonji, M., Iraqi Y., & Jones, A. (2013). Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials*, *15*(4), 2091-2121.

Kolosnjaji, B., Zarras, A., Webster, G., & Eckert, C. (2016). Deep learning for classification of malware system call sequences. En *AI 2016: Advances in Artificial Intelligence* (pp. 137–149). Springer International Publishing.

Kothamasu, G. A., Venkata, S. K. A., Pemmasani, Y., & Mathi, S. (2023). An Investigation on Vulnerability Analysis of Phishing Attacks and Countermeasures. *International Journal of Safety and Security Engineering*, *13*(2), 333–340.

Koziol, J. (2003). *Intrusion detection with snort*. Sams Publishing.

Kumar, D., Goel, M., & Rani, A. (2020). Browser Extensions for Phishing Detection: A Comparative Study. *International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, 448–452.

Labbe, K. G., Rowe, N. C., & Fulp, J. D. (2006). A methodology for evaluation of host-based intrusion prevention systems and its application. *2006 IEEE Information Assurance Workshop*.

Li, X., Geng, G., Yan, Z., Chen, Y., & Lee, X. (2016). Phishing detection based on newly registered domains. *2016 IEEE International Conference on Big Data (Big Data)*.

Liao, H., & Hsieh, C. (2016). The research of phishing prevention and management mechanism. *Information Technology Journal*, 241–248.

Lutz, M. (2014). *Python pocket reference: Python in your pocket* (5a ed.). O'Reilly Media.

Ma, X., Li, Y., Wang, J., Wang, X., & Luo, Z. (2016). Intrusion detection based on one-class support vector machine ensemble learning. *Future Generation Computer Systems*, 92–102.

MacKay, J. (2018, julio 2). 5 formas de identificar un sitio web de phishing. *MetaCompliance*. https://www.metacompliance.com/es/blog/phishing-and-ransomware/5-ways-to-identify-a-phishing-website

MacKay, J. (2019, enero 14). Qué es el spear phishing y técnicas antiphishing para evitarlo. *MetaCompliance*. https://www.metacompliance.com/es/blog/cyber-security-awareness/what-is-spear-phishing-and-anti-phishing-techniques-to-prevent-it

MacQueen, J. (1967). Some methods for classification and analysis of multivariate observations. *Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability,* 281-297.

Mahajan, R., & Siddavatam, I. (2018). Phishing website detection using machine learning algorithms. *International journal of computer applications*, *181*(23), 45–47. https://doi.org/10.5120/ijca2018918026

Malik, H., & Siew, H. (2009). Review of agile methodologies in software. *International Journal of Research and Reviews in Applied Sciences*, 2076–7366.

Mat Rani, L., Universiti Tun Hussein Onn Malaysia, Mohd Foozy, C. F., Mustafa, S. N. B., Universiti Tun Hussein Onn Malaysia, & Book Hack Enterprise. (2023). Feature selection toEnhance phishing website detection based on URL using machine learning techniques. *Journal of Soft Computing and Data Mining*, *4*(1). https://doi.org/10.30880/jscdm.2023.04.01.003

Mcgrath, D. K., & Gupta, M. (2008). Behind Phishing: An Examination of Phisher Modi Operandi. *LEET*, *8*, 4.

Mehta, P. (2016). Creating google chrome extensions. *Apress*.

Mitchell, T. M. (1997). *Machine Learning*. McGraw-Hill.

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2012). An assessment of features related to phishing websites using an automated technique. *In 2012 international conference for internet technology and secured transactions*, 492–497.

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Phishing websites features. *School of Computing and Engineering. School of Computing and Engineering, University of Huddersfield.*

Moramarco, S. (2016, abril 27). *Phishing definition and history*. Infosecinstitute.com. https://resources.infosecinstitute.com/topics/phishing/phishing-attacks-examples-in-history/

Muhammad, A., Junaid, B., Fareed, Z., & Zhang, J. (2020). Effective features for phishing website detection using supervised learning. *Concurrency and Computation: Practice and Experience*.

Nagaraj, K., Bhattacharjee, B., Sridhar, A., & Gs, S. (2018). Detection of phishing websites using a novel twofold ensemble model. *Journal of Systems and Information Technology*, *20*(3), 321–357. https://doi.org/10.1108/jsit-09-2017-0074

Ollmann, G. (2004). *The phishing guide*. Next Generation Security Software Limited.

O'reilly Media, N. (s/f). *Head First C#: A Learner's Guide to Real-World Programming with C#, XAML, and*.

Patil, V., Thakkar, P., Shah, C., Bhat, T., & Godse, S. P. (2018). Detection and prevention of phishing websites using machine learning approach. *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*.

Pressman, R., & Maxim, B. (2019). *Software Engineering: A Practitioner's Approach* (9a ed.). McGraw-Hill Education.

Pressman, R. S. (2002). *Ingenieria del Software - Un Enfoque Practico 5b: Edicion*. McGraw-Hill Companies.

¿Qué es un sistema de detección de intrusos (IDS)? (2022, julio 15). Check Point Software ES. https://www.checkpoint.com/es/cyber-hub/what-is-an-intrusion-detection-system-ids/

Rigatti, S. J. (2017). Random forest. *Journal of Insurance Medicine*, *4*(1), 31-39.

Rodrigues de Oliveira, E., Cabral Ribeiro, P., Picinini Méxas, M., & Oliveira, S. (2023). Scrum method assessment in Federal Universities in Brazil: multiple case studies. *Brazilian Journal of Operations and Production Management*, *20*.

Schwaber, K., & Sutherland, J. (2023). *La Guía de Scrum*.

Scrum method assessment in Federal Universities in Brazil: multiple case studies. (s/f).

Shirazi, H., Haefner, K., & Ray, I. (2017). Fresh-phish: A framework for auto-detection of phishing websites. *2017 IEEE International Conference on Information Reuse and Integration (IRI)*.

Singh, C., & Meenu. (2020). Phishing website detection based on machine learning: A survey. *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*.

Sotnikov, D. (2016). *Web development with clojure: Build bulletproof web apps with less code* (2a ed.). Pragmatic Bookshelf.

Srinivasa Rao, R., & Pais, A. R. (2017). Detecting phishing websites using automation of human behavior. *In Proceedings of the 3rd ACM workshop on cyber-physical system security* , 33–42.

Sucar, L. E., & Tonantzintla, M. (2006). *Redes bayesianas. Aprendizaje Automático: conceptos básicos y avanzados*. 77-100.

Symantec. (2021). Internet Security Threat Report. *Internet Security Threat Report*, *24*.

Tedyyana, A., & Ghazali, O. (2021). Teler real-time HTTP intrusion detection at website with Nginx web server. *JOIV International Journal on Informatics Visualization*, *5*(3), 327. https://doi.org/10.30630/joiv.5.3.510

Torres, J. (2018). *DEEP LEARNING Introduccion*.

Tyagi, I., Shad, J., Sharma, S., Gaur, S., & Kaur, G. (2018). A novel machine learning approach to detect phishing websites. *2018 5th International Conference on Signal Processing and Integrated Networks (SPIN)*.

Urrutia, D. (2020, enero 28). *Qué es el JavaScript - Definición, significado y ejemplos*. Arimetrics. https://www.arimetrics.com/glosario-digital/javascript

Vargas, A. E. M. (2020). Comparación de técnicas de machine learning para detección de sitios web de phishing. *Interfases*, *(013)*, 77-103.

Vayansky I., & Kumar, S. (2018). Phishing–challenges and solutions. *Computer Fraud & Security, 2018*, *1*, 15–20.

Vira Yudha, G., & Wisnu Wardhani, R. (2021). Design of a snort-based IDS on the raspberry pi 3 model B+ applying TaZmen sniffer protocol and log alert integrity assurance with SHA-3. *2021 9th International Conference on Information and Communication Technology (ICoICT)*.

Wang, G., Xu, K., Zhang, Z., & Yao, D. (2019). Web Browser Extension Based Anti-Phishing Techniques. *International Symposium on Network Computing and Applications (NCA)*, 1-8.

Wang, Z., & Li, X. (2013). Intrusion prevention system design. *In Proceedings of the International Conference on Information Engineering and Applications (IEA) 2012*, *3*, 375–382.

Watson, D., Holz, T., & Mueller, S. (2005). Know your Enemy: Phishing. *The Honeynet Project & Research Alliance*.

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE access: practical innovations, open solutions*, *6*, 35365–35381. https://doi.org/10.1109/access.2018.2836950

Yang, P., Zhao, G., & Zeng, P. (2019). Phishing website detection based on multidimensional features driven by deep learning. *IEEE access*, *7*, 15196-15209.

Zabihimayvan, M., & Doran, D. (2019). Fuzzy rough set feature selection to enhance phishing attack detection. *2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*.

Anexos