UPN
UNIVERSIDAD PRIVADA DEL NORTE

FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

“DESARROLLO DE APLICATIVO MÓVIL PARA LA DETECCIÓN DE PHISHING EN MENSAJES DE TEXTO (SMS) DE DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID”

Tesis para optar el título profesional de:

Ingeniero de Sistemas Computacionales

Autor:

Pablo Fernando Flores Barrios

Asesor:

Mg. Jorge Alfredo Guevara Jiménez
https://orcid.org/0000-0002-8459-9342

Lima - Perú

2022

JURADO EVALUADOR

Jurado 1 Presidente(a)	**JORGE ALFREDO BOJORQUEZ SEGURA**	**10318709**
	Nombre y Apellidos	Nº DNI

Jurado 2	**CARLOS RAMOS GONZALES**	**25771858**
	Nombre y Apellidos	Nº DNI

Jurado 3	**JORGE ROSVIN NARVÁEZ VILLACORTA**	**41455569**
	Nombre y Apellidos	Nº DNI

DEDICATORIA

Esta investigación está dedicada a mi familia que, sin su apoyo, no podría contar con la tranquilidad para el desarrollo de esta investigación.

AGRADECIMIENTO

Agradecimiento a la familia, amigos, compañeros y a todas las personas que me apoyaron con su opinión, recursos y su valioso tiempo para aportar en la realización de esta investigación. Asimismo, agradezco a Dios por la vida, la libertad y la salud que complementan la voluntad para cumplir los sueños.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación tuvo como objetivo desarrollar un aplicativo móvil que mejore la detección de Phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android. La investigación fue de tipo explicativa, relaciona causa efecto entre las variables, y es cuasi experimental por tener intervención pero con una muestra no aleatoria adaptada a las necesidades. Según el enfoque es de tipo cuantitativa y según el propósito fue de tipo aplicada tecnológica por ser práctica e intentar resolver un problema real de la sociedad a través de una solución concreta. Asimismo, se consideró dos variables que fueron medidas en la matriz de operacionalización: aplicativo móvil como variable indirecta y detección de Phishing como variable directa. Finalmente, con respecto a la muestra del estudio, se contó con una muestra para un objetivo específico de la investigación la cual fue representada por 20 mensajes SMS recibidos de un dispositivo con sistema operativo Android infectados con phishing o mensajes de texto sospechosos. Asimismo, se realizó una muestra de 5 profesionales en TIC que cumplan con un perfil determinado para la realización de los requerimientos del aplicativo. En los objetivos específicos, primero se obtuvo el cumplimiento de requerimientos, resolviendo el objetivo específico 1. Asimismo, se obtuvo los dos entregables de eficiencia que solucionan el objetivo específico 2 y 3 que sumados al anterior cumplen el objetivo principal de la investigación. Los requerimientos obtenidos en la recolección de datos de las entrevistas tuvieron como base las buenas prácticas del ISO 25000 y el aplicativo se realizó a través del método del desarrollo incremental, plasmando sus resultados en las conformidades de cada incremento y las fichas de registro correspondientes. Las pruebas para medir la eficiencia y cumplimiento de los objetivos específicos 2 y 3, presentaron óptimos resultados en sus dimensiones propuestas, asimismo, se obtuvo una mejora de un 55% en cada uno de los indicadores. Los valores obtenidos en los Post test (medidos con el aplicativo propuesto)

obtuvieron un 90% de TPR. La efectividad lograda con el aplicativo móvil propuesto, colabora para futuras integraciones e investigaciones relacionadas a soluciones antimalware.

PALABRAS CLAVES: Detección de Phishing, Phishing en SMS, Aplicativo antiphishing, Aplicativo antimalware, Phishing en Android, smishing.

CAPÍTULO I: INTRODUCCIÓN

1.1. Realidad problemática

En la actualidad, el uso de dispositivos móviles ha aumentado masivamente a nivel mundial. Según los datos estadísticos del banco mundial publicados en su portal web, desde el año 2000 hasta el 2020, se ha incrementado en una proporción de once a uno (Banco Mundial, 2020). Los dispositivos móviles se han convertido en parte de lo cotidiano en la sociedad. La importancia de esta tecnología en todos los ámbitos se ve reflejada naturalmente "Beyond digital platforms for the transfer of money, goods and services, smartphones are an enabler of education, information, work, health, social participation and more sustainable solutions." Kjaer (2014). Las diversas funcionalidades de estos dispositivos, se ha convertido en una necesidad para las personas y las organizaciones, pero por el mal uso de los propios usuarios, puede conllevar a diversas vulnerabilidades "…la protección de la seguridad de la información, a través de sus políticas, se llevaría a cabo solo a través de una perspectiva tecnológica… es necesario tener una visión amplia a través de un enfoque interdisciplinario, donde el principal factor, el humano, juega un papel fundamental." (Altamirano & Ballona, 2017, p. 113). La agilidad en el avance de la tecnología en el mundo evoca una necesidad de actualizar constantemente las medidas y soluciones de seguridad para estos dispositivos que van en aumento de producción y con ello, el alto riesgo ante la ciberdelincuencia. Wibowo & Ali (2016) alertan en su publicación al respecto "Mobile malware is certainly a growing and evolving threat, and individuals and organizations which utilize mobile technology must be educated on what mobile malware is and how to protect oneself from it." (p. 121).

En países con menor desarrollo tecnológico y menor difusión de medidas preventivas en seguridad de los móviles, existe un mayor riesgo de infección, esto ligado a que la mayor parte de usuarios en el mundo cuentan con un dispositivo celular, la mayoría de veces sin contar

con un antivirus o contando con uno gratuito de demostración que no garantiza la robustez y adecuado aseguramiento de la información. Desde muy temprana edad, los usuarios de teléfonos móviles cuentan con todos los accesos a sus funcionalidades, libre navegación y descarga, acceso a cualquier enlace, disponibilidad total del uso de las aplicaciones, y otras utilidades potencialmente riesgosas. Hilt (2019) investiga sobre esta población y profundiza en la dependencia de este recurso móvil "El celular (móvil) ha llegado a formar parte de la vida cotidiana de los jóvenes y su uso continúa en expansión, siendo utilizado cada vez a una menor edad." (p. 103).

En la actualidad, es más frecuente que la información sensible, sea institucional o personal, se encuentre almacenada en los mismos dispositivos móviles, por ello, es de suma importancia el aseguramiento de la integridad, accesibilidad y la disponibilidad de su información. Los ataques por malware son cada vez más sofisticados, a veces basta con solo pulsar un botón, archivo o enlace para ser infectado, evadiendo antivirus básicos y tradicionales. Wirth (2017) advierte el aumento del riesgo y recomienda cambios "With the increasing number of computer viruses and sophistication of attacks we now see, the changes required were much more profound than just adding more signatures to the virus definition" (p. 269). Dentro de los malwares más conocidos, existe la suplantación de identidad o Phishing, el cual, es generado utilizando la inteligencia social para el engaño a los usuarios. Básicamente, el mecanismo de infección se realiza a través de hipervínculos o enlaces hacia páginas web falsas que son enviados a través de mensajería de texto SMS o correos electrónicos. La principal consecuencia de no protegerse ante este ataque informático es el robo de cuentas bancarias, billeteras digitales y la vulneración de información personal y/o sensible.

Es importante aclarar que los dispositivos móviles no solo cuentan con funcionalidades orientadas a la comunicación, poseen también la capacidad del procesamiento y

almacenamiento, aunque limitada en comparación con las computadoras portátiles o de escritorio. Es por ello que es muy importante la eficiencia en los procesos de las herramientas que contiene. Esta responsabilidad cae directamente sobre los aplicativos móviles, los cuales, generan solidez y masificación en el uso de los dispositivos móviles.

Aplicativo móvil

Serna & Pardo (2017) definen al aplicativo móvil "Un aplicativo móvil es un pequeño paquete de software que sirve para resolver una o varias tareas en específico" (p. 20).

El aplicativo móvil es un programa específico para un dispositivo móvil y tiene una función específica. Barquero (2016) señala en su publicación "Están pensadas para satisfacer una necesidad concreta del usuario relacionada con la información, compra, entretenimiento, comunicación, educación, productividad, artísticas y creativas, etc." (p. 18).

Para el desarrollo de las aplicaciones móviles, es necesario planificar en base a los requerimientos de los clientes u objetivos de la institución. En ese contexto, Cárdenas et al. (2021) indica "Es primordial para los desarrolladores establecer exactamente la finalidad de la pieza de software, identificando cual tendencia se acopla de mejor manera a su funcionamiento, estas tendencias indican hacia donde se apuntan las nuevas tecnologías y el interés general". (p. 142). Asimismo, para seleccionar el entorno de desarrollo integrado (IDE) adecuado, se debe conocer para que sistema operativo se desarrollará la aplicación móvil, el lenguaje a utilizar y el tipo de aplicación a desarrollar. De una encuesta a 20 expertos realizada por Moreyra & Pusdá (2018), el IDE Eclipse obtuvo mayor puntuación en cuanto a las características de manera general y como segundo IDE más utilizado fue Android Studio (p.216).

Para la calidad en el diseño y desarrollo de aplicaciones móviles, se han utilizado buenas prácticas y estándares de referencia. Moreyra & Pusdá (2018) utilizan el estándar ISO 9126 “El estándar ISO 9126 brinda parámetros que se utiliza como guía para la evaluación y medición de la calidad de un producto de software, las mismas sirven de base durante el ciclo de vida del software” (p. 220).

Los aplicativos móviles pueden clasificarse de diversas formas según la tecnología, funcionalidad, comercialización, soporte, diseño, etc. Según la tecnología, mayormente pueden ser dos formas, aplicaciones Android o aplicaciones IOS, las principales plataformas en donde se exponen para su descarga son Play Store en Android y App Store en IOS. Según el tipo de uso, se puede decir que la funcionalidad es variada, los usuarios pueden utilizar un aplicativo con fines de diversión, lucro, ocio, educación, productividad, comunicación, protección, etc. Por otro lado, según la comercialización, las aplicaciones pueden tener un costo o ser gratuitas. Según el soporte en donde se ejecuta, pueden ser aplicaciones web, aplicaciones para celular, aplicaciones para tv Smart, aplicaciones para smartwatch, etc. Por último, por tipo de diseño pueden ser genéricas o web, hibridas y nativas. Asimismo, existen diversos modelos para el diseño de los aplicativos móviles, pero uno de los más utilizados por su fácil mantenimiento, escalabilidad y control; es el modelo cliente – servidor.

Se debe considerar algunas limitaciones generales en el desarrollo de las aplicaciones móviles en dispositivos celulares. No disponer aún de un hardware con tanta capacidad de procesamiento en la mayoría de dispositivos móviles, tal como sí sucede en los computadores fijos. El acceso a internet es vital para el óptimo funcionamiento, especialmente en las aplicaciones móviles de tipo cliente –servidor. Asimismo, se debe indicar que, para una buena experiencia de usuario, se debe comprender la importancia de las pantallas táctiles, su tamaño y la integración con el diseño del aplicativo.

Existen diversos modelos de proceso para explicar el enfoque en el desarrollo del software. Dentro de las más conocidas son el modelo en cascada, desarrollo incremental y la ingeniería de software orientada a la reutilización (Sommerville, 2011).

Las etapas que se desarrollarán en esta investigación son las siguientes:

a) Requerimientos del software.
b) Diseño e implementación del software
c) Validación del Software

Para esta investigación se utilizó la metodología del desarrollo incremental. La selección de esta metodología tuvo el fin de cumplir desde un inicio con los requerimientos esenciales de la aplicación para después ir completando de forma prioritaria con las demás funcionalidades cumpliendo así de forma ordenada con los objetivos de la investigación. La flexibilidad de esta metodología permite realizar de forma práctica y ágil un aplicativo móvil con una base de datos local para la simulación del proceso de registro y detección de Phishing.

Para el presente diseño y desarrollo, se utilizó el lenguaje unificado de modelado (UML) como referencia para la presentación de los diagramas estructurales que plasman el desarrollo del aplicativo objetivo.

Con respecto a los casos de uso, Rumbaugh et al. (2006) definen “El propósito de un caso de uso es definir un cierto comportamiento de un clasificador (incluyendo un subsistema o todo el sistema) sin revelar la estructura interna del clasificador.” (p. 56).

Un diagrama de clases, representa la relación y la descripción de las clases del proyecto. Rumbaugh et al. (2006) profundiza estos conceptos de la vista estática del software “Una clase es la descripción de un concepto del dominio de la aplicación o de la solución de la aplicación” (p. 22).

Detección de Phishing

Una de las funcionalidades en todo dispositivo móvil, es la seguridad de la información. En ese aspecto existen diversas aplicaciones que contribuyen a este fin, protegiendo la información del usuario ante ataques cibernéticos o comúnmente llamados malware, los cuales, tienen una clasificación muy amplia como ransomware, phishing, virus, troyano, spyware, adware, entre otros; siendo el más acorde con nuestra investigación los ataques por ingeniería social, pero de tipo Phishing.

Por su parte, el phishing, o pesca de incautos, ha sido definido como el mecanismo criminal que emplea tanto ingeniería social, como subterfugios técnicos para robar los datos de identidad personales de los consumidores y los de sus tarjetas de crédito o cuentas bancarias. (Miró, 2013, p. 7).

El término Phishing proviene del vocablo inglés “fishing” que significa pesca, una metáfora que asemeja captar víctimas de ciberdelincuencia, personas naturales o compañías, como si fuera una pesca, capturándolas a través de dominios falsos, enlaces a páginas fraudulentas enviados a través correo electrónico, llamadas telefónicas o por mensajes de texto SMS, con el objetivo de extraer información personal y sensible para acceder y retirar el dinero de las cuentas bancarias.

Otro autor afirma lo siguiente:

> El atacante se pone en contacto con la víctima (generalmente, un correo electrónico) haciéndose pasar por una empresa con la que tenga alguna relación (su banco, su empresa de telefonía, etc.). En el contenido del mensaje intenta convencerle para que pulse un enlace que le llevará a una (falsa) web de la empresa. En esa web le solicitarán

su identificación habitual y desde ese momento el atacante podrá utilizarla" (Roa, 2013, p. 19).

Oxman (2013) también investigó al respecto "El Phishing y el Pharming son dos tipos de fraudes informáticos cuya finalidad común es la de apoderarse de información personal de un usuario de internet…" (p. 215). Asimismo, profundizó en la técnica utilizada. La imitación es el arma principal de ataque, se duplica webs o formularios de entidades financieras logrando obtener la información del cliente. De esa forma, poder tener el acceso a las cuentas del cliente y poder concebir la extracción del dinero mediante el retiro, transferencia u compras online. (Oxman, 2013, p. 217).

Asimismo, se describía en otras publicaciones:

Es uno de los ataques cibernéticos más comunes en todo el mundo, consistente en ganarse la confianza del internauta mediante una identidad falsa y obtener así información secreta como contraseñas, números de seguridad social o de tarjetas de crédito. La suplantación de identidad no es solo uno de los crímenes online más comunes sino también uno de los que más está creciendo, y en su último Informe de Inteligencia en Seguridad Microsoft halló que, en abril de 2019, de una muestra aleatoria de correos electrónicos analizados, un 0,7 % contenían "phishing". Aunque a primera vista esta cifra pueda parecer menor, esto significa que aproximadamente 1 de cada 150 e-mails analizados fue un intento de conseguir acceso ilegal a datos mediante la suplantación de identidad. El 0,7 % es, además, significativamente superior al 0,49 % detectado un año antes, en abril de 2018, y cinco veces más que el 0,14 % de enero de 2018. (EFE News Services, Inc.,2019).

En la actualidad, los antivirus basados en firmas, siguen siendo la solución comúnmente utilizada. Las soluciones estáticas tienen diversos inconvenientes, pero el más importante a mencionar es el retraso en la detección de malware (Nissim et al., 2016, p.798).

La forma de detectar phishing se realiza a través de un motor de detección. “ Analiza los paquetes en base a reglas definidas para detectar los ataques”(Gómez, 2009, p. 22).

Para esta investigación se realizó la medición en base a tasas de verdaderos positivos (TPR), utilizada para la detección de malwares. Nissim, et al. (2016) utiliza la misma métrica en su investigación “For evaluation purposes, we measured the true-positive rate (TPR) measure [13,15] which is the percentage of positive instances classified correctly.” (p. 809).

Causas de Phishing

Los escenarios más frecuentes luego de un ataque de phishing son el robo de credenciales, robo o secuestro de información, paralización de procesos y sobre todo pérdidas económicas. El phishing es causado por diversos motivos, pero la principal es por el error humano.

La comunidad de investigadores de seguridad, han reconocido que el comportamiento humano tiene un papel crucial en muchos fallos de seguridad, en la literatura sobre seguridad de la información, a los humanos se les suele llamar el eslabón más débil de la cadena de seguridad. (Altamirano & Ballona, 2017, pp 115)

Otra causa por el cual el phishing sigue teniendo relevancia dentro de los tipos de ataques, es por su constante sofisticación de ataques. “ Los atacantes se han vuelto más expertos en la suplantación de identidad y en aprovechar nuestras ocupadas vidas laborales” (Avast, 2021).

La facilidad de realizar el ataque, es otra causa por la cual este ataque es tan popular. “ Los ataques de phishing se conciben como ataques de bajo riesgo que ofrecen grandes ganancias con poco esfuerzo” (Coronado et al., 2020).

Se debe mencionar que el Phishing se ha incrementado a razón de la Pandemia y las medidas que trajo con ello como es lo del trabajo remoto y el trabajo con dispositivos personales. " A raíz de la implementación del trabajo remoto, 70% de las organizaciones en la región han permitido que su fuerza laboral trabaje con sus dispositivos personales, con lo que la exposición a algún tipo de incidente cibernético aumentó considerablemente…" (Microsoft, 2021).

Antecedentes

Existen diversas investigaciones destinadas a proporcionar soluciones para la detección de malwares, las cuales, colaboran en definir estrategias y nuevas alternativas de mejora para este fin. La mayoría de soluciones están basadas en Machine Learning utilizan base de datos y arquitecturas como cliente-servidor, pero todas con el fin de lograr la efectividad en la detección de malware y tratando de no utilizar tantos recursos de hardware que es su principal desafío.

En el caso de aplicaciones con IA, Cárdenas et al. (2021) concluye "La inteligencia artificial en aplicaciones móviles representa actualmente un medio poco viable para su uso comercial, debido a su poca integración con características de las aplicaciones móviles, altos niveles de consumo de recursos de hardware". (p. 142)

Nissim, et al. (2016) presentaron una publicación cuasiexperimental sobre un sistema actualizador antimalware llamado Aldroid, aplicaron una muestra de 800 aplicaciones en donde 72 eran malware para el entrenamiento. La muestra para las pruebas fue de 50, 100 y 245 aplicaciones nuevas por día de un tota de 2670 aplicaciones. El instrumento utilizado fue las fichas, graficos y tablas. Esta solución alcanza a detectar más del doble de la cantidad de nuevos

malwares y 6,5 veces más malwares por el algoritmo de análisis supervisado del SVM utilizado para esa investigación en comparación de motores heurísticos de antivirus convencionales.

Siguiendo con soluciones de tipo Machine Learning, Firdaus, et al. (2018) realizaron una investigación aplicada de una solución llamada Bio Analyzer, pero a través de redes neuronales artificiales (ANN) que funciona con bajos recursos. La metodología fue la recolección de datos a través de ingeniería inversa, asimismo, se utilizó fichas, cuadros y gráficos como instrumentos de la investigación. La muestra para el entrenamiento fue de 5551 aplicaciones benignas. La investigación analiza desde varios algoritmos para encontrar la mejor forma de detección de malware analizando los permisos de aplicativo, telefonía y la ruta de directorio, se utilizó varios clasificadores pero el de mejor resultado fue el perceptrón multicapa (MLP), que utiliza el algoritmo de backpropagation o retroalimentación en errores, en donde se observa que la mejor respuesta con respecto a su parámetro de rango de aprendizaje de un total de 0.1 – 1, fue en el rango 0.1 presentando un 90% de exactitud, 87% de rango de verdaderos positivos, 7.2% de rango de falsos positivos, 92.3% de precisión, 87% de recuperación y 89.6% de media armónica de la precisión, concluyendo que a menor rango, mayor tasa de aprendizaje.

Otra solución, pero ya utilizando técnicas híbridas, Mejía (2019) realizó una investigación aplicativa, que se enfocó a la detección de malware en base a los permisos. Se utilizó la técnica del método científico para el desarrollo. La solución se llamó: Behavior Detector (BD), el cual, cambia estática o dinámicamente los permisos solicitados según lo detectado en el App como riesgoso, es decir aquello que puede afectar a la privacidad y el funcionamiento del dispositivo, la solución administra los permisos según su motor de base de datos encontrados en las aplicaciones Nativas (de fábrica) o descargadas desde el Play Store, este aplicativo fue trabajado en Android Studio.

En otra investigación, Jang et al. (2016), proponen una investigación aplicada sobre la detección fue en base a perfiles, a través de su solución: Andro Profiler. La muestra utilizada fue de 8840 apps benignas y 643 malwares. Utilizaron la técnica de la observación del método científico, ordenando los resultados en tablas. Andro Profiler detecta malware a través de un modelo cliente servidor, analizando preventivamente antes de la instalación, el comportamiento del malware para luego alertar al cliente del riesgo del mismo con una efectividad en la detección y clasificación de malware superior al 98%.

Con respecto a soluciones realizadas en emuladores[1], Demertzis & Iliadis (2017) realizan una solución llamada: ClantiMF, la cual, utiliza redes neuronales para la clasificación de malware con un mínimo de consumos de recursos de hardware. La investigación es de tipo aplicada, utiliza la técnica de la observación y plasma los resultados en tablas. La muestra del de aprendizaje fue 37,120 benignas y 36,342 malwares. La solución está basada en el algoritmo OSELM, el cual detecta y previene contra actividades cifradas de la dark web y ataques Botnets, analizando el tráfico de transmisión web con resultados mínimos del 94,2 mínimo de precisión en la clasificación o detección de malware.

Asimismo, Wang et al. (2015) realizan una investigación aplicativa, utilizando la técnica de la observación con el instrumento de tablas, gráficos. La muestra utilizada son 6000 apps benignos y 5560 malwares. La solución para esta investigación fue el emulador CuckooDroid del sistema Cuckoo Sandbox, el cual, fue enfocado para la implementación en la nube. El trabajo combina el análisis estático y dinámico para la detección de malware, el motor de detección es muy efectiva para detectar ataques de día cero, el algoritmo detecto una alta

[1] El emulador es un software que permite la reproducción del funcionamiento de algoritmos y funcionalidades del sistema operativo Android.

tasa de detección positiva, presentando un 98.84% de TPR, 1.16% de falsos negativos y 1.3% de falsos positivos.

Con respecto a soluciones exclusivas para la detección de tipo phishing, Coronado et al. (2020) realizaron una investigación cuasiexperimental, utilizando una muestra de 64,635 muestras benignas y de igual modo para malware para el entrenamiento del algoritmo utilizado, la muestra final de URL fue de 68,729. El instrumento utilizado fueron fichas y plasmados por la técnica de la observación. El sistema de detección fue híbrido, este realizó la combinación entre listas negras y aprendizaje automático para poder llegar a una mayor detección de páginas infectadas, primero analizó la dirección de la web en las listas negras, luego extrajo hasta 39 características de la web y se compararon con el modelo que ha sido entrenado. La detección alcanzada con este método con el mejor de sus algoritmos empleados, alcanzó un 90.6% de TPR, 2.35% de falsos positivos y una precisión de 95.5%. Se debe recordar que esta investigación utilizó el repositorio Phistank, que también es una herramienta de ayuda para nuestro estudio.

Por otro lado, en Cuba, Hernandez & Baluja (2021), realizaron una investigación descriptiva, en donde nos hablan de mecanismos para detectar el phishing con respecto a los SMS, los métodos de aprendizaje automático (Bosques aleatorios, árboles de decisión y máquina de soporte vectorial) resaltan por su frecuencia y efectividad, los cuales llegaron hasta un 99.1% de detección en el mejor de los casos y 96.4% especialemnte en phishing en SMS a través de la herramienta SmiDCA.

En el ámbito local, Jancachagua (2021) presenta el modelo de herramienta en contra del phishing de código abierto Gophish implementado en una entidad financiera. La investigación fue de corte cuasiexperimental, se utilizó la técnica de la observación e instrumentos como fichas y tablas, asimismo, se usó una muestra de 450 correos con phishing.

El objetivo era reducir la infección de phishing enviados a través de correos electrónicos. La investigación logró reducir este tipo de ataques en un 54.83%.

Asimismo, Castañeda (2013), realiza una investigación experimental basada exclusivamente a la detección en SMS de mensaje no deseados, el cual a través de un algoritmo de aprendizaje supervisado (SVM) hace posible la clasificación de SMS con contenido de SPAM.La muestra total de 4,900,468 SMS, de los cuales 215 son spam. Para esta investigación se utilizó como instrumentos fichas y tablas.

Dimensiones

Para definir las dimensiones de la investigación se utilizó el estándar ISO/IEC 25000, también llamado SQUARE. Este estándar es la evolución de los ISO 9126 y el ISO 14598 y es utilizado convencionalmente para los procesos de evaluación de productos de software. Se debe indicar que el estándar fue necesario solo como referencia de buenas prácticas.

El modelo de calidad representa la piedra angular en torno a la cual se establece el sistema para la evaluación de la calidad del producto. En este modelo se determinan las características de calidad que se van a tener en cuenta a la hora de evaluar las propiedades de un producto software determinado.(ISO 25000, 2022).

Este estándar está subdividido en 5 partes:

ISO/IEC 2500n, División de gestión de la calidad.

ISO/IEC 2501n, División del modelo de la calidad.

ISO/IEC 2502n, División de mediciones de la calidad.

ISO/IEC 2503n, División de requisitos de la calidad.

ISO/IEC 2504n, División de evaluación de la calidad.

En esta investigación, se tomó en cuenta las divisiones del ISO y se tomó el modelo ISO/IEC 25010, División del modelo de calidad, para recurrir a sus dimensiones y definir la calidad del aplicativo y como soporte para las dimensiones de las variables de la investigación. Las dimensiones elegidas para la variable independiente fueron la adecuación funcional, a través de sus subcaracterísticas de completitud funcional, corrección funcional y pertinencia funcional. Por otro lado, para la variable dependiente se seleccionó la eficiencia de desempeño, con sus subcaracterísticas de utilización de recursos y capacidad.

a) Adecuacion funcional

"Representa la capacidad del producto software para proporcionar funciones que satisfacen las necesidades declaradas e implícitas, cuando el producto se usa en las condiciones especificadas"(ISO/IEC 25010, 2022).

La adecuación funcional se forma a su vez de las siguientes sub características, las cuales fueron incluidas como dimensiones para la variable independiente de esta investigación.

Completitud funcional

"Grado en el cual el conjunto de funcionalidades cubre todas las tareas y los objetivos especificados por el usuario". (Marulanda, 2014, p.126)

Este indicador se convierte en un requisito para iniciar en el cumplimiento de los requerimientos del aplicativo móvil cmo parte del desarrollo del OE1. Para ello, se realizó entrevistas a 05 profesionales de TIC con un perfil definido y conveniente para obtener un listado de requerimientos del aplicativo móvil.

Corrección funcional

"Capacidad del producto o sistema para proveer resultados correctos con el nivel de precisión requerido"(ISO 25000, 2022).

Este indicador es validado con una ficha de registro al final del cumplimiento de los requerimientos, en donde se presenta un check list final de las funcionalidades necesarias para cumplir con la precisión requerida en los objetivos específicos propuestos.

Pertinencia funcional

"Capacidad del producto software para proporcionar un conjunto apropiado de funciones para tareas y objetivos de usuario especificados"(ISO 25000, 2022).

Este indicador es validado con una ficha de registro al final del cumplimiento de los requerimientos, en donde se presenta un check list de funcionalidades que aporten en el trabajo automático y práctico para el usuario.

b) Eficiencia de desempeño

"Esta característica representa el desempeño relativo a la cantidad de recursos utilizados bajo determinadas condiciones" (ISO/IEC 25010, 2022).

En esta segunda dimensión, se toma en cuenta las siguientes sub características para tomarlas como dimensiones de la variable dependiente en esta investigación:

Utilización de recursos

"Las cantidades y tipos de recursos utilizados cuando el software lleva a cabo su función bajo condiciones determinadas" (ISO/IEC 25000, 2022).

Capacidad

"Grado en que los límites máximos de un parámetro de un producto o sistema software cumplen con los requisitos "(ISO/IEC 25000, 2022).

Justificación

Este trabajo de investigación desarrolla un aplicativo móvil llamado SMS Seguro, el cual funciona en el sistema operativo Android, analiza el contenido y detecta dominios web sospechosos o reportados como Phishing que fueron enviados a través de mensajería de texto SMS. Asimismo, el aplicativo avisa a través de una alerta a los usuarios para que no accedan a dicho mensaje infectado advirtiendo de la amenaza recibida y envía recomendaciones según sea el tipo de incidencia analizada. Para el diseño del mismo, se seleccionó la arquitectura cliente – servidor, por ser la más frecuente en el tipo de desarrollos en donde se necesite realizar las consultas de varios clientes hacia una misma base de datos. Los beneficios de contar con este aplicativo es la automatización en la detección de phishing de manera preventiva, no será necesario el ingreso al mensaje SMS por parte del usuario para comprobar que existe malware en él, asimismo, su uso es práctico e intuitivo para el usuario y cuenta con una zona educativa de recomendaciones ante el evento malicioso para la constante educación del usuario en el tema y así colaborar en la cultura de prevención ante la ciberdelincuencia. El aplicativo detectará a través de algoritmos de búsqueda y repositorios de otras investigaciones oficiales para cumplir con el objetivo propuesto. La detección de phishing, generación de alertas y el envío de las predicciones o recomendaciones, será de forma constante en el caso de direcciones sospechosas o sin certificado SSL, pero en el caso de validar con la base de datos de malware, el dispositivo deberá conectarse localmente para trabajar de forma completa. La importancia de contar con este aplicativo radica en lo práctico del uso, lo ágil y automático en la detección y prevención contra las infecciones de malware y lo eficiente en consumo de memoria y almacenamiento para el dispositivo móvil. Asimismo, esta investigación pretende generar un desarrollo que colabore en futuras investigaciones aplicadas en las que se necesite una herramienta práctica

para la detección de phishing en los mensajes de texto SMS de los dispositivos móviles con sistema operativo Android o también para futuras integraciones con otra solución antimalware.

1.2 Formulación del problema

a) Pregunta General

¿Cómo desarrollar un aplicativo móvil que mejore la detección de Phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android?

b) Preguntas Específicas

- ¿Cómo desarrollar los requerimientos de un aplicativo móvil que mejore la detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android?
- ¿Cómo desarrollar un aplicativo móvil que mejore la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android?
- ¿Cómo desarrollar un aplicativo móvil que genere alertas de Phishing en cada mensaje de texto (SMS) recibido en dispositivos con sistema operativo Android?

1.3 Objetivos

a) Objetivo general

Desarrollar un aplicativo móvil que mejore la detección de Phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

b) Objetivos específicos

- OE1: Desarrollar los requerimientos de un aplicativo móvil que mejore la detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

- OE2: Desarrollar un aplicativo móvil que permita la mejora en la tasa de verdaderos positivos (TPR) en la detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.
- OE3: Desarrollar un aplicativo móvil que permita la generación de alertas de Phishing en cada mensaje de texto (SMS) recibido en dispositivos con sistema operativo Android.

1.4 Hipótesis

a) Hipótesis general

El desarrollo de un aplicativo móvil permitirá mejorar la detección de Phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

b) Hipótesis específicas

- HE1: El desarrollo de los requerimientos de un aplicativo móvil permitirá que mejore la detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.
- HE2: El desarrollo de un aplicativo móvil permitirá el aumento de la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.
- HE3: El desarrollo de un aplicativo móvil permitirá la generación de alertas de Phishing en cada mensaje de texto (SMS) recibido en dispositivos con sistema operativo Android.

CAPÍTULO II: METODOLOGÍA

2.1 Tipo de investigación

La investigación es de tipo explicativa, por tratar realizar la causa efecto entre las variables independiente y dependiente. Asimismo, es de tipo cuasi experimental por contar con una muestra predefinida y tener intervención a través de un aporte para la solución de la problemática. Según el enfoque es de tipo cuantitativa y según el propósito fue de tipo aplicada tecnológica por ser práctica e intentar resolver un problema real de la sociedad. La población de la investigación son todos los mensajes SMS recibidos en un dispositivo móvil con sistema operativo Android en un mes en la ciudad de Lima. Asimismo, para la encuesta la población fue profesionales en TIC. La muestra son 20 mensajes SMS recibidos de un dispositivo con sistema operativo Android infectados con phishing o mensajes de texto sospechosos. Asimismo, para validar el indicador de Cobertura funcional, se contó con una muestra para la entrevista de 5 profesionales con experiencia en el área de TIC, los cuales posteriormente sirvieron para completar los 02 indicadores de test de validación. Se considera dos variables para las mediciones correspondientes en el cuadro matriz de operacionalización de las variables y son: Aplicativo móvil y detección de Phishing, el cual se presenta en la Tabla 1. Asimismo, en el Apéndice A, se presenta la matriz de consistencia, la cual demuestra a manera de resumen el trabajo de investigación.

Tabla 1

Matriz de operacionalización de las variables

Variables	Definición conceptual	Dimensiones	Definición operacional /Indicadores	Instrumentos

Aplicativo Móvil	Programa específico para un dispositivo móvil. Están pensadas para satisfacer una necesidad concreta del usuario relacionada con la información, compra, entretenimiento, comunicación, educación, productividad, artísticas y creativas, etc. Todas responden a un criterio común: su funcionalidad (Barquero, 2016).	Completitud Funcional	Cobertura funcional	Entrevista
		Corrección Funcional	Test de validación	Ficha de registro
		Pertinencia Funcional	Test de validación	Ficha de registro
Detección de Phishing	Phishing es un tipo de fraude informático cuya finalidad es apoderarse de la información personal de un usuario de internet (Oxman, 2013).	Utilización de recursos.	Tasa de verdaderos positivos (TPR) de detección de phishing de una muestra de 20 mensajes de texto SMS. Representación por porcentaje.	Fichas de registro.
		Capacidad.	Tasa de verdaderos positivos (TPR) de generación de alertas o recomendaciones en los mensajes de texto SMS recibidos. Representación por porcentaje.	Fichas de registro.

2.2 Población y muestra de la investigación

Población

La población seleccionada para la entrevista fueron profesionales de TIC. Asimismo, la población seleccionada para las pruebas fue el tráfico de mensajes de texto (SMS) recibidos en un semestre en un dispositivo celular, ubicado en la ciudad de Lima.

La población de los mensajes de texto (SMS) es tomada como referencia de un estudio realizado por OSIPTEL, en donde se indica que el promedio de mensajes de texto (SMS) mensual en un dispositivo celular en la ciudad de Lima, es 40.8 (Bendezú & Chahuara, 2012, p.6)

Muestra:

Con respecto a la muestra de la entrevista, se realizó en base a un perfil dedicado para obtener la información más precisa y necesaria para realizar el objetivo principal de la investigación. El detalle del perfil de la muestra se encuentra descrito en la Tabla 2.

Con respecto a la muestra de mensajes de texto (SMS), según una publicación de Fortinet, Perú ha recibido en promedio 11 mil millones de ciberataques en el 2021, lo que hace un total de 916,7 millones de ataques al mes en promedio. Por otro lado, según OSIPTEL, actualmente contamos con aproximadamente 42 millones de equipos celulares. Con esto, se puede definir que como máximo cada equipo ha recibido al mes una media de 21,8 cibertaques. Según lo analizado, se seleccionó una muestra conveniente de mensajes de texto (SMS) con contenido de phishing o sospechoso recibidos al mes, para lo cual, se tomó 20 de los 21 posibles con la intención de obtener una muestra par máxima que se aproxime a lo informado por FORTINET y OSIPTEL. De esa forma, la muestra pudo ser dividida en 2 partes, 10 mensajes de texto (SMS) infectados con malware tipo phishing de la base Phistank y 10 mensajes, de propia autoría, con direcciones web sospechosas.

Muestreo:

El tipo de muestreo fue no probabilístico de conveniencia, se utiliza la opinión de los involucrados en la investigación. “Este método es una técnica de muestreo que no realiza procedimientos de selección al azar, sino que se basan en el juicio personal del investigador para realizar la selección de los elementos que pertenecerán a la muestra.” (Parra & Vásquez, 2017, p. 9).

El método a utilizar será de tipo por conveniencia debido a que se tomó una muestra en primer lugar de 5 profesionales reconocidos pero elegidos por disponibilidad y con respecto a la segunda muestra, se debe aclarar que en la realidad no todos los mensajes recibidos son infectados con Phishing, pero esta muestra se tuvo que seleccionar por ser la más adecuada y necesaria para la investigación. Asimismo, nos interesa realizar algunos de propia autoría por considerar importante las diferentes casuísticas locales de intentos de infección por mensajes de texto (SMS).

Este tipo de muestreo tiene como particularidad obtener muestras de relevancia mediante la inclusión en la muestra de grupos supuestamente significativos o regulares. (Navarro,2018).

2.3 Materiales, técnicas e instrumentos de investigación

2.3.1 Materiales

Los materiales que se emplearon para la investigación fueron los siguientes:

- Computadora portátil. Empleada para el desarrollo de la investigación.
- Dos Dispositivos móviles con sistema operativo Android
- Software Android Studio
- Software Excel

- Software Word
- Software SPSS
- Herramienta Online Lucid Chart
- Herramienta Bizagi Modeler

2.3.2 Técnicas de investigación

a) Observación:

La observación basada en el método científico, fue utilizada en la recolección de datos. Asimismo, esta técnica fue plasmada en fichas de registro con el fin de presentar de una forma ordenada y clara para cumplir los objetivos propuestos.

b) Entrevista:

Para esta investigación se utilizó esta técnica la cual consiste en obtener información detallada de forma estructurada por parte de personal involucrado en la especialidad y tema a investigar. Esta técnica fue valiosa para poder recopilar información importante sobre los requerimientos, calidad y uso del aplicativo móvil.

c) Indicadores

Cobertura funcional

La cobertura funcional indica el porcentaje de utilización de las capacidades de algún bloque en específico o de todo el circuito, con los reportes generados se conoce si algún bloque del circuito precisa de más pruebas específicas para verificar toda su funcionalidad.(Ortega et al, 2012, pp 3)

La cobertura funcional está basada en el cumplimiento de todos los requerimientos a través de lo indicado por el resultado de la suma de las conformidades de los incrementos

desarrollados. Esto se valida a través del listado de requerimientos y el cumplimiento, el cual debe estar completo en un 100%.

Test de validación

Es un formato elaborado de autoría propia como complemento a la cobertura funcional, los cuales, evaluan el cumplimiento de dimensiones de adecuación funcional como corrección funcional y pertinencia funcional. Son tablas de check list, las cuales validan funcionalidades del aplicativo con respecto al cumplimiento de objetivos y al uso en que debe enfocarse.

Tasa de verdaderos positivos (TPR) en detección de phishing:

"For evaluation purposes, we measured the true-positive rate (TPR) measure which is the percentage of positive instances classified correctly." (Nissim, et al., 2016).

Este indicador se define como el porcentaje positivo de detección de la muestra. La muestra de esta investigación consta de 20 mensajes SMS infectados con phishing o contenido sospechoso, comprobados según el repositorio phishtank y mensajes con contenido de direcciones web sin certificado de seguridad SSL (Secure Socket Layer).

Tasa de verdaderos positivos (TPR) en generación de alertas:

Este indicador se define como la cantidad total de alertas o recomendaciones de la muestra generadas por el aplicativo móvil cada vez que se recibe un mensaje de texto (SMS) en el dispositivo de prueba con sistema operativo Android. La alerta y recomendación del aplicativo deberá generarse así sea positiva o negativa en la detección de phishing respectiva. La muestra empleada para este indicador será la misma que se utiliza para el TPR de detección de phishing.

2.3.3 Instrumentos de la investigación

- Cuadros y gráficos

La presentación y análisis de los datos recabados, se realizó en gráficos, cuadros y tablas estadísticas elaboradas a través del software Excel, los cuales, sirven para observar con mayor detalle, los resultados obtenidos. La documentación fue redactada a través del software Word apoyado con gráficos a través de la herramienta online Lucid Chart y Bizagi Modeler.

- Fórmulas matemáticas

Se realizó cálculos matemáticos y fórmulas como apoyo para el análisis y presentación de las estadísticas en las fichas. Los cálculos fueron resueltos en hojas de Excel, asimismo, se presentó gráficos según fueron el caso, para una mayor comprensión del análisis.

Instrumentos de recolección de datos

- Guía de entrevista:

Este instrumento, tuvo como objetivo obtener la información adecuada y precisa de profesionales especializados que cumplan con el perfil de la Tabla 2. La guía de entrevista consta de un cuestionario de 10 preguntas para obtener contenido técnico sobre el desarrollo de aplicaciones móviles, las preguntas del cuestionario fueron realizadas en base a los objetivos de la investigación, lo cual, ayudó con información esencial para la determinación de requerimientos del aplicativo móvil desarrollado y cumplir con el indicador 1: Completitud Funcional que posteriormente sirve de base para el cumplimiento de los indicadores 2 y 3 de la variable independiente y con ello el cumplimiento del OE1. La guía de entrevista y el cuestionario de preguntas, está presentado en la Tabla 3 y las respuestas al mismo, fueron detalladas en la Tabla 4 de la presente investigación.

Tabla 2

Objetivo de la guía de entrevista y perfil de los entrevistados

Objetivos de la guía de entrevista	Nacionalidad	Cargo	Experiencia	Tipo de Entidad donde labora	Edad
La búsqueda de información técnica y relevante para el desarrollo de aplicaciones móviles que colaboren en la determinación de los requerimientos de la solución propuesta en la investigación.	Latino americano	Desarrollador, Especialista o Experto en soluciones de seguridad de la información, Telecomunicaciones o Software licenciado.	Mínimo 5 años de experiencia en el sector de TI, Telecomunicaciones o Seguridad.	Pública o Privada	Entre 30 y 60 años

Tabla 3

Cuestionario de la guía de entrevista

Numeración de pregunta	Pregunta
1	¿Qué tipos de desarrollo existen en la actualidad de aplicativos móviles para los dispositivos móviles Smart?
2	¿Qué tipo de desarrollo de aplicación móvil recomienda en caso que la temática sea de seguridad en SMS para dispositivos Android?
3	¿Qué tipo de Framework o IDE recomienda para este tipo de desarrollo?
4	¿Qué lenguaje de programación utiliza para el desarrollo de aplicativos móviles en Android?
5	¿Qué requisitos técnicos considera necesario para el desarrollo de aplicativos móviles en Android?
6	¿Qué normas de calidad aplica para el desarrollo de un aplicativo móvil?
7	¿Qué herramientas o gestores recomienda para la creación y administración de base de datos para aplicativos móviles?
8	¿Qué recomendaciones técnicas brindaría para que se pueda realizar la constante comparativa de la base de datos con los mensajes SMS entrantes al dispositivo móvil en tiempo real?

9	Teniendo la información de la base de datos en un archivo de formato Excel, ¿Qué recomendaciones realizaría para poder administrarlo desde un sistema de base de datos e integrarlo con el aplicativo móvil?
10	¿Qué recomendaría en el caso que se necesite implementar funciones con machine learning en aplicaciones móviles para Android?

Tabla 4

Respuestas de las entrevistas

Pregunta	**Respuestas**				
	Experto 1	**Experto 2**	**Experto 3**	**Experto 4**	**Experto 5**
1	Las nativas, las híbridas y las aplicaciones web progresivas o llamadas PWA.	Se clasifican en aplicaciones web, nativas e hibridas.	Las más frecuentes son las nativas, híbridas, PWA y las aplicaciones web.	Nativo y Multiplata forma.	Aplicaciones nativas, hibridas, Multiplatafor ma, Progresiva, web app responsive.
2	Por la necesidad de reconocer funcionalidades y hardware del dispositivo móvil como el chip del operador, recomendaría que sea Nativa.	Pienso que debe ser nativa, por la agilidad que se necesita y por requerirla para el sistema operativo Android.	Como es de seguridad, tal vez puede ser Nativa.	Nativo	Nativas
3	En el caso de las nativas, uno de los que yo recomendaría sería React Native, ya que es un framework ligero y muy práctico para	Recomiendo el IDE Android Studio, es el más eficiente para trabajar con Android.	Recomiendo Flutter por tener gran cantidad de diseños y por lo práctico. La otra opción sería Android Studio por ser la más popular y segura	Android: Android studio IOS: Xcode Flutter: Visual studio code	Android studio

	trabajar tanto en Android y IOS.		para apps nativas en Android.		
4	A mi criterio son Java y Kotlin. Es importante elegir ello antes de empezar a planificar el diseño.	Java es el más utilizado.	Java y Kotlin, aunque también se utiliza JavaScript, pero más que todo en aplicaciones web.	Dart Java	Java o Kotlin
5	Una Pc con un mínimo de 1 Giga de Ram y conocimientos en lenguaje de programación Java o Kotlin	Recomiendo Android Studio, ese IDE sería el ideal, pero con una PC con 4 gigas de RAM, mínimo.	Recomiendo el Android Studio.	Conocer un lenguaje de programación para móviles o en su defecto uno general como Java.	Con respecto al sistema operativo sugiero de Android 5 o superior, con respecto al equipo que tenga mínimo 1 Giga de RAM o superior.
6	En nuestro caso nos guiamos del ISO 25000 y utilizamos diagramas UML para los diagramas.	En la entidad nos guiamos del ISO 25000.	En la empresa se utiliza el ISO 25000 como referencia. Además, se utiliza el método de ingeniería clásico para el desarrollo.	No utilizamos un ISO en especial.	ISO25000 - SQuaRE (System and Software Quality Requirements and Evaluation) ISO27001 - Seguridad de datos.
7	Recomiendo back4app para crear Appi, es una base de datos práctica y no se necesita programar, funciona muy bien con React Native.	Puedo recomendar SQL Server, pero si no se necesita algo tan robusto, podría ser con SQLite es pequeño y solvente para su trabajo con poco	Me parece que el más práctico es SQLite, aunque si se desea online recomiendo los gestores SQL Server o MYSQL. Otra opción es phpMyAdmin que es gratuito, práctico.	Cualquiera disponible mediante la Nube como Mysql o phpMyadmin.	Considerando que sería una base de datos relacional una buena opción libre de licenciamiento es PostGresql con la ide PgAdmin.

		procesamiento de hardware.			
8	Se puede cargar documentos CSV con facilidad en back4app. Luego desde ahí se podría administrar y actualizar rápidamente.	Si sólo es con una base de datos fija y no se necesita tanta frecuencia para actualizar, mejor sería integrar la aplicación con el SQLite sería más rápido.	Es mejor una base de datos en línea con un gestor, la herramienta phpMyAdmin es buena para las aplicaciones sencillas.	Cargarlo a la base de datos. El gestor phpMyAdmin es bien sencillo de usar.	Puedes usar Firebase, pero eso significa costo en licenciamiento o significa un punto a tener en cuenta. La otra forma de realizar aplicación en tiempo real con Postgres y no tener costo de licenciamiento es utilizando la librería SOCKET.IO.
9	Se puede cargar documentos CSV con facilidad en back4app. Luego desde ahí se podría administrar y actualizar rápidamente.	Primero, se debe analizar el archivo Excel para elegir la solución más adecuada, asimismo, evaluar la capacidad de soportar la misma por el aplicativo móvil y por el gestor de base de datos, la mayoría soportan ese formato.	Las bases de datos en Excel ya se pueden importar directamente a los gestores, pero normalmente deben estar en formato CSV.	Importar la base de Excel a la base de datos utilizada, para luego comparar directo desde esa base de datos.	Crear rutina de importación del archivo Excel a la base de datos. Carga de forma automática cada x tiempo. El Excel se puede dejar en un directorio de disco, ftp, o recibir por email y al llegar el archivo nuevo se inicia el proceso de importación.

					Importante conocer la volumetría.
10	Existen alternativas como los Kits de aprendizaje automático de google, que pueden reconocer rostros, textos, códigos de barra, idiomas, etc. Es interesante y sin tanta complejidad, aunque ello puede a consumir recursos de procesamiento del dispositivo para su óptimo funcionamiento.	No recomiendo el trabajo con Machine learning en este caso ya que se hará en base a una comparativa con una base Excel y no a patrones de análisis.	Recomiendo que utilices algoritmos de búsqueda para dar eficiencia, pero debes tener cuidado ya que ello conlleva a utilizar mayores recursos de procesamiento.	Nube de google o firebase para machine learning.	Un par de alternativas es API Google Cloud o Amazon Web Services (AWS) Machine Learning. Es importante entender cuál sería el objetivo de los modelos ML para la aplicación ya que en base a eso se puede orientar al aprovechamiento de modelos ya previamente entrenados.

- Fichas de registro:

Se elaboró fichas para el muestreo y recolección de datos con respecto al cumplimiento de indicadores. En total se realizaron 08 fichas, 02 fichas para el análisis de los resultados obtenidos en el desarrollo del aplicativo y cumplimiento del OE1 y 06 fichas para registrar los resultados de las observaciones en las pruebas con los SMS (Pre test, Re test y Post test) para el cumplimiento de los OE2 y OE3. Las fichas se presentan en las figuras del 1 al 8.

Figura 1.

Ficha de registro – Corrección funcional

TEST DE VALIDACION CORRECCION FUNCIONAL

ITEM	FUNCIONALIDAD DEL APLICATIVO	OBJETIVO AL QUE APORTA	ESTADO
1	SE CONECTA CON SERVIDOR LOCAL		
2	DETECTA PHISHING EN SMS		
3	VALIDA PHISHING CON BASE DE DATOS		
4	REGISTRA USUARIOS		
5	GENERA RECOMENDACIONES ANTIPHISHING		
6	LEE DE FORMA AUTOMATICA LOS SMS ENTRANTES		
7	PRESENTA EN PANTALLA DE FORMA AUTOMATICA EL RESULTADO DE LA VALIDACION DE PHISHING		
8	LAS ALERTAS SIEMPRE SON GENERADAS DE FORMA AUTOMATICA AL DETECTAR UN MENSAJE NUEVO		
9	GENERA ALERTAS DE DETECCION DE PHISHING		
10	GENERA ALERTAS DE NO CONEXIÓN CON LA BASE DE DATOS		
11	GENERA ALERTAS DE CONEXIÓN CON BASE DE DATOS		
12	PRESENTA EN PANTALLA DE FORMA AUTOMATICA EL MENSAJE Y NÚMERO ENVIADA POR EL EMISOR		

Figura 2.

Ficha de registro – Pertinencia funcional

TEST DE VALIDACION PERTINENCIA FUNCIONAL

ITEM	FUNCIONALIDAD DEL APLICATIVO	PERFIL DE USUARIO	ESTADO
1	EL APLICATIVO OCUPA POCO ALMACENAMIENTO	AUTOMÁTICO, ÁGIL Y PRÁCTICO	
2	EL APLICATIVO ES NATIVO PARA ANDROID		
3	EL APLICAIVO GENERA DE FORMA AUTOMÁTICA LAS ALERTAS		
4	EL APLICATIVO LEE DE FORMA AUTOMÁTICA LOS MENSAJES SMS		
5	EL APLICATIVO DETECTA DE FORMA AUTOMÁTICA EL PHISHING		
6	EL APLICATIVO PRESENTA DE FORMA AUTOMÁTICA LA VALIDACIÓN DE PHISHING		
7	EL APLICATIVO SOLO PIDE UN REGISTRO INICIAL AL USUARIO.		
8	EL APLICATIVO DEMORA MENOS DE 2 SEGUNDOS EL PROCESO DE VALIDACIÓN Y GENERACIÓN DE ALERTA DE PHISHING		
9	EL APLICATIVO MUESTRA EL MENSAJE Y NÚMERO DEL EMISOR DEL SMS DE FORMA AUTOMÁTICA.		
10	EL APLICATIVO TRABAJA EN SEGUNDO PLANO.		
11	EL APLICATIVO NO REQUIERE AUTENTICACIÓN.		

Figura 3.

Ficha de registro – Detección de Phishing Re test

FICHA DE REGISTRO - DETECCION DE PHISHING (RE-TEST)						
ENCARGADO	Pablo Flores Barrios					
OBJETIVO	Plasmar la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS).					
FECHA DE INICIO	15/05/2022					
FECHA DE FINAL	20/05/2022					
VARIABLE	INDICADOR			MEDIDA	FORMULA	
Detección de Phishing en mensajes de texto (SMS).	Tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS).			Cantidad	TPR [%]=CIEP*100/MT Donde: CIEP: Cantidad de items en estado positivo. CIEN: Cantidad de items en estado negativo. MT: Muestra total TPR: Tasa de verdaderos positivos en detección de	
ITEM	FECHA	MENSAJE	HORA DE ENVIO	HORA DE RECEPCION	ESTADO DE DETECCION	TPR
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

Figura 4.

Ficha de registro – Generación de alertas Re test

FICHA DE REGISTRO - GENERACION DE ALERTAS (RE- TEST)						
ENCARGADO	Pablo Flores Barrios					
OBJETIVO	Plasmar la tasa de verdaderos positivos (TPR) de generación de alertas y/o recomendaciones por cada item de la muestra.					
FECHA DE INICIO	15/05/2022					
FECHA DE FINAL	20/05/2022					
VARIABLE	INDICADOR			MEDIDA	FORMULA	
Detección de Phishing en mensajes de texto (SMS).	Tasa de verdaderos positivos (TPR) de generación de alertas en los mensajes de texto SMS recibidos.			Cantidad	TPR [%]=CIEP*100/MT Donde: CIEP: Cantidad de items en estado positivo. CIEN: Cantidad de items en estado negativo. MT: Muestra total TPR: Tasa de verdaderos positivos en generación de alertas.	
ITEM	FECHA	MENSAJE	HORA DE ENVIO	HORA DE RECEPCION	ESTADO DE GENERACION DE ALERTA	TPR
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

Figura 5.

Ficha de registro – Detección de Phishing Pre test

FICHA DE REGISTRO - DETECCION DE PHISHING (PRE-TEST)						
ENCARGADO	Pablo Flores Barrios					
OBJETIVO	Plasmar la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS).					
FECHA DE INICIO	15/05/2022					
FECHA DE FINAL	30/05/2022					
VARIABLE	INDICADOR			MEDIDA	FORMULA	
Detección de Phishing en mensajes de texto (SMS)	Tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS).			Cantidad	TPR (%)=CEP* 100/MT Donde: CEP: Cantidad de items en estado positivo MT: Muestra total TPR: Tasa de verdaderos positivos en detección de phishing	
ITEM	FECHA	MENSAJE	HORA DE ENVIO	HORA DE RECEPCION	ESTADO DE DETECCION	TPR
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

Figura 6.

Ficha de registro – Detección de Phishing Post test

FICHA DE REGISTRO - DETECCION DE PHISHING (POST-TEST)						
ENCARGADO	Pablo Flores Barrios					
OBJETIVO	Plasmar la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS).					
FECHA DE INICIO	15/05/2022					
FECHA DE FINAL	30/05/2022					
VARIABLE	INDICADOR			MEDIDA	FORMULA	
Detección de Phishing en mensajes de texto (SMS)	Tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS).			Cantidad	TPR (%)=CEP* 100/MT Donde: CEP: Cantidad de items en estado positivo. MT: Muestra total TPR: Tasa de verdaderos positivos en detección de phishing	
ITEM	FECHA	MENSAJE	HORA DE ENVIO	HORA DE RECEPCION	ESTADO DE DETECCION	TPR
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

Figura 7

Ficha de registro – Generación de alertas Pre test

FICHA DE REGISTRO - GENERACION DE ALERTAS (PRE TEST)						
ENCARGADO	Pablo Flores Barrios					
OBJETIVO	Plasmar la tasa de verdaderos positivos (TPR) de generación de alertas y/o recomendaciones por cada ítem de la muestra.					
FECHA DE INICIO	15/05/2022					
FECHA DE FINAL	30/05/2022					
VARIABLE	INDICADOR			MEDIDA	FORMULA	
Detección de Phishing en mensajes de texto (SMS).	Tasa de verdaderos positivos (TPR) de generación de alertas o recomendaciones en los mensajes de texto SMS recibidos.			Cantidad	TPR (%)=CIEP*100/MT Donde: CIEP: Cantidad de ítems en estado positivo. MT: Muestra total TPR: Tasa de verdaderos positivos en generación de alertas.	
ITEM	FECHA	MENSAJE	HORA DE ENVIO	HORA DE RECEPCION	ESTADO DE DETECCION	TPR
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

Figura 8

Ficha de registro – Generación de alertas Post test

FICHA DE REGISTRO - GENERACION DE ALERTAS (POST TEST)						
ENCARGADO	Pablo Flores Barrios					
OBJETIVO	Plasmar la tasa de verdaderos positivos (TPR) de generación de alertas y/o recomendaciones por cada ítem de la muestra.					
FECHA DE INICIO	15/05/2022					
FECHA DE FINAL	30/05/2022					
VARIABLE	INDICADOR			MEDIDA	FORMULA	
Detección de Phishing en mensajes de texto (SMS).	Tasa de verdaderos positivos (TPR) de generación de alertas o recomendaciones en los mensajes de texto SMS recibidos.			Cantidad	TPR (%)=CIEP*100/MT Donde: CIEP: Cantidad de ítems en estado positivo. MT: Muestra total TPR: Tasa de verdaderos positivos en generación de alertas.	
ITEM	FECHA	MENSAJE	HORA DE ENVIO	HORA DE RECEPCION	ESTADO DE DETECCION	TPR
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

2.3.4 Validez de instrumento

Para esta investigación se utilizó el juicio de expertos, el cual, consta en la revisión de la información recolectada por personal calificado para medir la validez y confiabilidad de la información recolectada, y de esa forma, poderla utilizar en la obtención de medidas adecuadas para la investigación.

Un autor afirma lo siguiente con respecto a este instrumento:

El juicio de expertos es un método de validación útil para cotejar la fiabilidad de una investigación … el juicio de expertos debe unir a la validez y la confiabilidad. La tarea principal del experto es percibir las ambigüedades que pueda haber y excluirlos; por otra parte, también tendrá el rol de recomendar los posibles ajustes necesarios para que sea válido y confiable el instrumento de recolección. (Almada, 2019, p.19).

Para realizar la validez del instrumento, se realizó un juicio de expertos conformado por 3 Ingenieros. Asimismo, se realizó tablas de evaluación para la validez del instrumento por cada experto. Las tablas creadas son cuatro, dos para el indicador de detección de Phishing en mensajes de texto (SMS) y dos para el indicador de generación de alertas en cada mensaje de texto (SMS) recibido. Para observar el antes y después se propuso las evaluaciones Pre test y Post test de cada indicador. Asimismo, para la validación de los indicadores de las dimensiones completitud funcional, corrección funcional y pertinencia funcional, se realizó en base al cumplimiento de la elaboración y desarrollo de todos los requerimientos, lo cual se valida con las pruebas y el funcionamiento del aplicativo. Se adjuntan los Apéndices AM y AN, en donde se presenta las fichas de cumplimiento de los indicadores corrección funcional y pertinencia funcional.

Los indicadores utilizados para las dimensiones de utilización de recursos y capacidad fueron: Tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS) y Tasa de verdaderos positivos (TPR) de generación de alertas o recomendaciones en los mensajes de texto (SMS) recibidos. Los mismos que, dan como resultado final de validez un promedio total de: 87.87%, por lo cual, se concluye que las muestras son válidas para la investigación. Asimismo, se adjuntan en los Apéndices AB, AC, AD, AE, AF, AG, AH, AI, AJ, AK, AL, ALL; donde se presentan las tablas de evaluación para los expertos. Asimismo, en la Tabla 5 se presenta el resumen del juicio de expertos.

Tabla 5

Resumen del juicio de expertos

Item	Nombre	Pre test Detección Phishing	Post test Detección Phishing	Pre test Generación de alarmas	Post test Generación de alarmas	Promedio por evaluador
Experto 1	James Bello Tacilla	84.1	84.8	84.7	84.9	84.8
Experto 2	Leoncio Roca Rojas	85.9	92.1	87	91.8	90.3
Experto 3	Luis Catalán Fonseca	88.5	88.5	88.5	88.5	88.5
Promedio		86.16666667	88.46666667	86.73333333	88.4	87.86666667

2.3.5 Confiabilidad de instrumento

Con respecto a la confiabilidad, se utilizó el método Test – Retest, con lo cual, se compara dos estados de la muestra en diferentes momentos. Para esta investigación se dividió

las pruebas en dos estados: Pre test y Re test. En los Apéndices S y Y; se presentan las fichas de Pre test, Re test y Post test respectivas de cada indicador.

"La confiabilidad puede ser entendida como una propiedad de las puntuaciones del test y en su versión más clásica denota la proporción de varianza verdadera y está vinculada al error de medición. Por ende, a mayor confiabilidad, menor error de medida." (Ventura-León, 2017, p. 1).

Asimismo, se presenta la correlación de Pearson para exponer la intensidad con que estas variables se asocian.

Tabla 6

Correlación de Pearson (Hernández et al., 2018)

Rango de valores rxy	Interpretación
0.00<= |rxy|< 0.10	Correlación nula
0.10<= |rxy|< 0.30	Correlación débil
0.30<= |rxy|< 0.50	Correlación moderada
0.50<= |rxy|< 1.00	Correlación fuerte

Se realizó el test de correlación de Pearson para cada indicador relacionando las etapas de pre test y re test respectivas.

- **Correlación de Pearson del estado pretest y re test de detección de phishing de una muestra de 20 mensajes de texto SMS:**

  La correlación encontrada según el programa SPSS para el análisis de correlación entre las variables: Estado Pre test de detección de Phishing y estado re test de detección de phishing, resultó en 0,892, lo cual, se considera una correlación fuerte positiva y nos brinda confianza con respecto a los datos recolectados.

  Figura 9

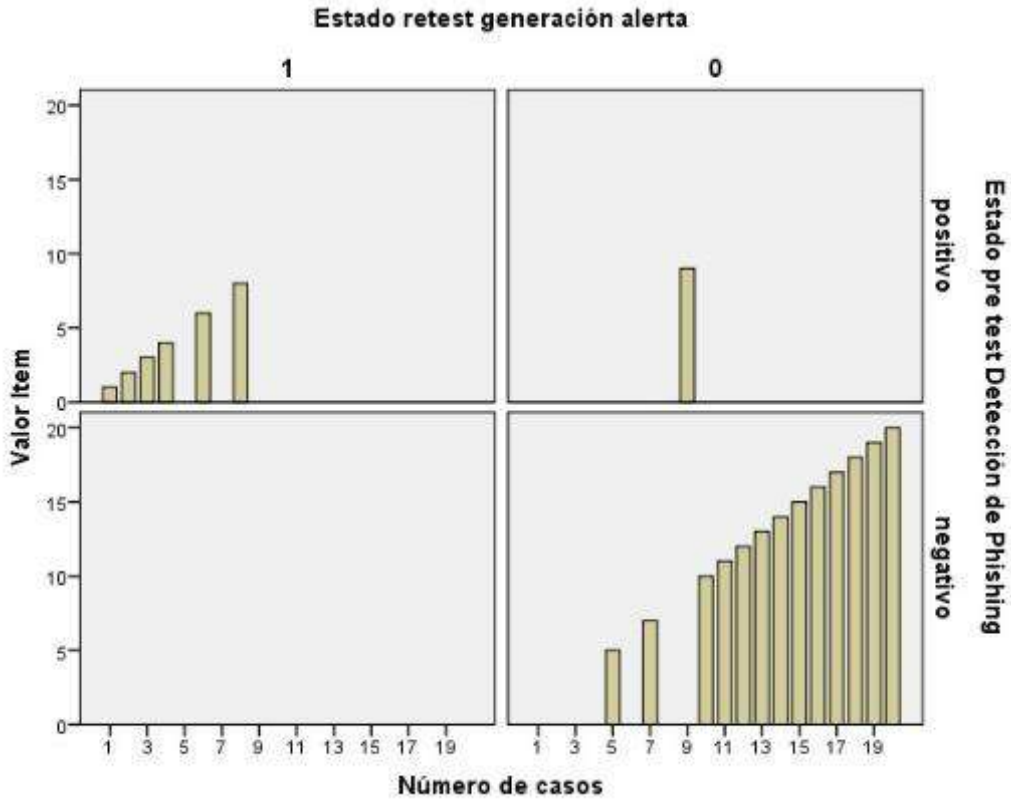
Correlación de Pearson – Detección phishing

Correlaciones

		Estado pre test Detección de Phishing	Estado retest Detección de phishing
Estado pre test Detección de Phishing	Correlación de Pearson	1	,892**
	Sig. (bilateral)		,000
	N	20	20
Estado retest Detección de phishing	Correlación de Pearson	,892**	1
	Sig. (bilateral)	,000	
	N	20	20

Figura 10

Gráfico de barras por ítem – Detección de phishing



- **Correlación de Pearson del estado pre test y retest de generación de alertas en los mensajes de texto SMS recibidos:**

La correlación encontrada en este indicador según el programa SPSS para el análisis de correlación entre las variables: Estado Pre test de generación de alerta y estado re test de generación de alerta, resultó en 0,892, lo cual, es similar a la antigua correlación. Por ello, también se le considera una correlación fuerte positiva y nos brinda confianza para el posterior análisis.

Figura 11

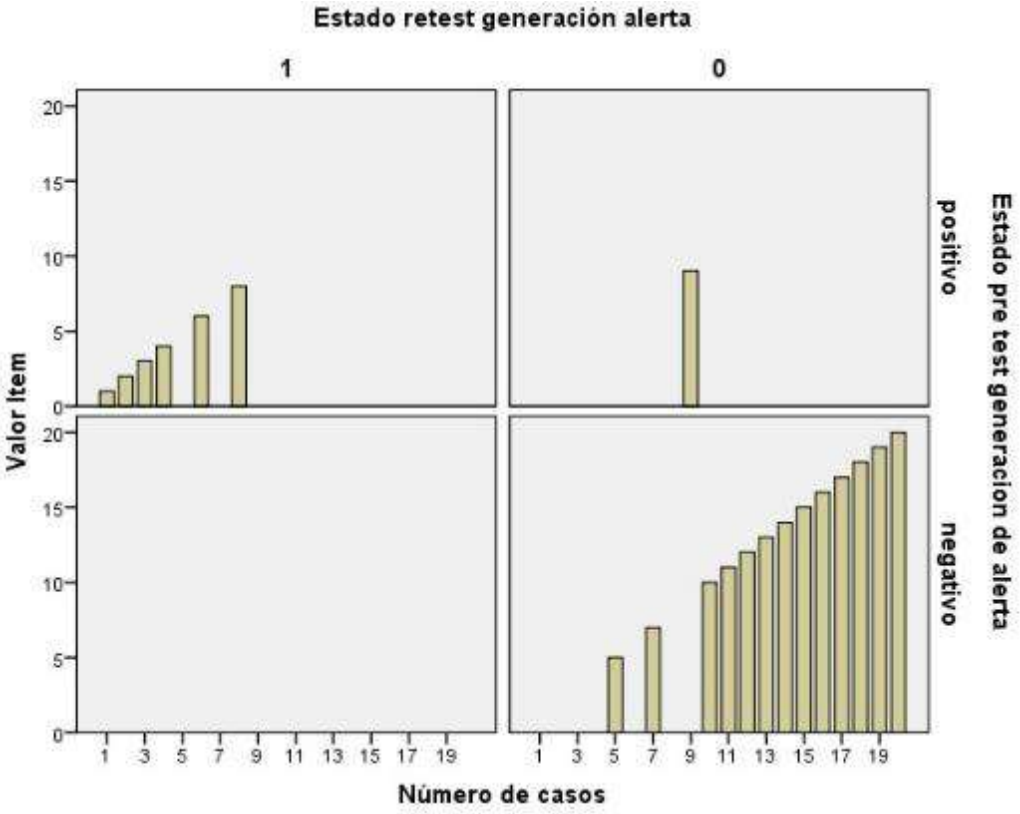
Correlación de Pearson – Generación de alerta

Correlaciones

		Estado pre test generacion de alerta	Estado retest generación alerta
Estado pre test generacion de alerta	Correlación de Pearson	1	,892**
	Sig. (bilateral)		,000
	N	20	20
Estado retest generación alerta	Correlación de Pearson	,892**	1
	Sig. (bilateral)	,000	
	N	20	20

Figura 12

Gráfico de barras por ítem – Generación de alerta



2.4 Procedimientos

2.4.1 Procedimiento de la investigación

a) Prueba de normalidad

Este procedimiento posibilita confirmar la hipótesis planteada. En esta oportunidad, utilizaremos el test de Shapiro Wilk por tener una muestra menor a 50. Con respecto al nivel de significancia, se considera 0.05 como umbral entre de distribución normal si es que pasa de ello, si es menor se designa como no normal.

b) Prueba de hipótesis

Hipótesis

La hipótesis es la afirmación de algo que se requiere comprobar. Por lo tanto, no es un hecho concreto, ya que se debe comparar lo observado en la realidad con las conjeturas previas. (Navarro,2018).

- **Hipótesis General**

  Hipótesis G. Nula: El desarrollo de un aplicativo móvil no permitirá mejorar la detección de Phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

  Hipótesis G. Alterna: El desarrollo de un aplicativo móvil permitirá mejorar la detección de Phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

- **Hipótesis específica 1**

  Hipótesis específica 1 (HE1): El desarrollo de los requerimientos de un aplicativo móvil permitirá que mejore la detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

  Para el cumplimiento de esta hipótesis nos basamos en el cumplimiento de los requerimientos.

  Indicador: Cobertura funcional cubierta al 100% .

  Hipótesis estadística 1

  HE1 nula: El desarrollo de los requerimientos de un aplicativo móvil no permitirá que mejore la detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

  HE1 nula = Cumplimiento de requerimientos < 100%

HE1 alterna: El desarrollo de los requerimientos de un aplicativo móvil permitirá que mejore la detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

HE1 alterna = Cumplimientos de requerimientos = 100%

- **Hipótesis específica 2**

Hipótesis específica 2 (HE2): El desarrollo de un aplicativo móvil permitirá el aumento de la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

Para el cumplimiento de esta hipótesis nos basamos en las siguientes fórmulas:

TPR (%) = CIEP*100/MT

Donde:

CIEP: Cantidad de ítems en estado positivo

MT: Cantidad total de la muestra

TPR: Tasa de verdaderos positivos

La aplicación detecta los ítems de forma individual, analiza y detecta phishing en cada mensaje recibido, los cuales se acumulan, según su estado, en las variable CIEP. Luego, culminado el muestreo, y aplicado con el MT, se tiene el valor del TPR. Para la investigación, nos interesa que el TPR sea el más elevado posible, mientras mayor sea su porcentaje, mayor su eficiencia en el desempeño en la detección de phishing en los mensajes de texto SMS.

Indicador: Tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS).

TPRPRD (pre test) = Tasa de verdaderos positivos en detección de phishing antes de utilizar el aplicativo móvil propuesto.

TPRPOD (post test) = Tasa de verdaderos positivos en detección de phishing después de utilizar el aplicativo móvil propuesto.

Hipótesis estadística 2

HE2 nula: El desarrollo de un aplicativo móvil no permitirá el aumento de la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

HE2 nula = TPRPOD <= TPRPRD

HE2 alterna: El desarrollo de un aplicativo móvil permitirá el aumento de la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

HE2 alterna = TPRPOD > TPRPRD

- **Hipótesis específica 3**

  Hipótesis específica 3 (HE3): El desarrollo de un aplicativo móvil permitirá la generación de alertas de Phishing en cada mensaje de texto (SMS) recibido de dispositivos con sistema operativo Android.

  Para el cumplimiento de esta hipótesis nos basamos en la siguiente fórmula:

  TPR = CIEP*100/MT

  Donde:

  CIEP: Cantidad de ítems en estado positivo

  MT: Cantidad total de la muestra

  TPR: Tasa de verdaderos positivos

  Al igual que en el procedimiento anterior, la aplicación detecta los ítems de forma individual, los cuales se acumulan en la variable CIEP. La diferencia es que en

este indicador no se analiza el mensaje recibido, sino la generación o no de alertas posterior a la recepción del mismo. Culminado el muestreo, el CIEP se opera con el MT obteniendo el valor del TPR. Para la investigación, nos interesa que el TPR sea el más elevado posible, mientras mayor sea su porcentaje, mayor su eficiencia en el desempeño en la generación de alertas luego de recibidos los mensajes de texto (SMS).

Indicador: Tasa de verdaderos positivos (TPR) de generación de alertas en los mensajes de texto SMS recibidos.

TPRPRA (pre test) = Tasa de verdaderos positivos en generación de alertas antes de utilizar el aplicativo móvil propuesto.

TPRPOA (post test) = Tasa de verdaderos positivos en generación de alertas después de utilizar el aplicativo móvil propuesto.

Hipótesis estadística 3

HE3 nula: El desarrollo de un aplicativo móvil no permitirá la generación de alertas de Phishing en cada mensaje de texto (SMS) recibido de dispositivos con sistema operativo Android.

HE3 nula = TPRPOA <= TPRPRA

HE3 alterna: El desarrollo de un aplicativo móvil permitirá la generación de alertas de Phishing en cada mensaje de texto (SMS) recibido de dispositivos con sistema operativo Android.

HE3 alterna = TPRPOA > TPRPRA

2.4.2 Procedimiento de la Ingeniería del aplicativo móvil

Para esta investigación se utilizó la metodología del desarrollo incremental con la intención de realizar un aplicativo móvil que cumpla con lo necesario e indispensable para el cumplimiento de los objetivos y en base a un listado de requerimientos.

Requerimientos del software.

Antes de iniciar con el primer incremento, se determinó los requerimientos del aplicativo móvil, para ello, se realizó una entrevista telefónica a 05 profesionales que laboren actualmente en el área de TIC o que tengan experiencia en el tema. Los objetivos y el perfil de los entrevistados se detallan en la Tabla 2. Las preguntas y respuestas de la entrevista se plasman en las Tablas 3 y 4 respectivamente. La información recopilada sirvió para definir los requerimientos funcionales y no funcionales del aplicativo móvil a desarrollar acorde a los necesitados por la problemática a abordar y empezar a cumplir con el OE1.

En base a los resultados obtenidos en las entrevistas y en base al estándar ISO 25000 a través de sus dimensiones: adecuación funcional, eficiencia de desempeño, usabilidad y mantenibilidad; se realizó un cuadro resumen a manera de síntesis, las cuales, se plasmaron en una tabla de criterios que servirán para realizar los requerimientos del aplicativo móvil, esta tabla se detalla en la Tabla 7.

Tabla 7

Criterios y análisis de respuestas

Adecuación funcional	Lenguaje de programación	Eficiencia de desempeño	Arquitectura	Usabilidad	Tipo de aplicativo	Mantenibilidad

Se indica sobre el tipo de aplicativo, lenguaje, IDE, gestores de BD y arquitectura requerida para el desarrollo.	Se indicó que los más utilizados son Java y Kotlin.	Debe ser ágil	Se recomienda el modelo Cliente-servidor. Utilizar base de datos no dentro del Aplicativo.	Debe ser práctico	Se recomienda ser nativa	Debe ser modular, fácil de realizar mantenimiento.

Con lo recopilado en las entrevistas y la tabla de criterios se pudo elaborar de una forma práctica y objetiva las características que debe tener la solución a desarrollar. Para ello, se procedió a generar un cuadro que detalle los requerimientos del aplicativo móvil, la cual se describe en la Tabla 8.

Tabla 8

Requerimientos del aplicativo móvil.

Item	Descripcion	Etapa de desarrollo
1	La aplicación se debe desarrollar con el lenguaje de programación Java.	Requerimiento no funcional
2	El entorno de desarrollo debe ser Android Studio, especializado para las aplicaciones nativas con sistema operativo Android.	Requerimiento no funcional
3	El modelo utilizado para esta aplicación debe ser Cliente – Servidor.	Diseño
4	La aplicación deberá ser compatible desde el sistema operativo Android 5.0	Requerimiento no funcional
5	La aplicación debe contar con un servidor para la administración de base de datos.	Diseño
6	La conexión con el servidor se debe realizar a través de implementaciones en lenguaje PHP y el paquete de software libre Xampp para la gestión de MYSQL.	Diseño
7	La base de datos debe ser de tipo relacional y se administrará con la herramienta phpMyAdmin.	Diseño

8	La base de datos de referencia, se basará en la recopilación de información de las investigaciones y repositorios oficiales.	Diseño
9	Debe tener una pantalla en donde se agregue usuarios y se acumulen en una base de datos. Deberá contar con alertas de buena y mala conexión.	Diseño
10	El aplicativo debe tener un algoritmo que pueda recibir y leer el contenido de los mensajes de texto SMS recibidos	Diseño
11	Debe contar con una pantalla de detección de phishing, en donde se predice si el mensaje de texto (SMS) está infectado o no con Phishing.	Diseño
12	La aplicación deberá identificar y mostrar en pantalla el mensaje obtenido y el número telefónico del emisor.	Diseño y validacion del software
13	La aplicación debe tener la capacidad de conectarse con la base de datos, para resolver la consulta y recibir la validación en tiempo real sobre detección de Phishing.	Diseño y validacion del software
14	Debe contar con una pantalla de recomendaciones ante ataques de tipo Phishing	Diseño y validacion del software
15	El tiempo de duración entre la recepción y la generación de alerta en la detección de Phishing no debe superar los 02 segundos.	Validacion del software
16	La aplicación deberá generar alertas sobre las detecciones de Phishing a través de notificaciones al recibir cualquier mensaje de texto (SMS).	Validacion del software
17	El código debe ser desarrollado de forma ordenada y modular para ser escalable y flexible en su mantenimiento en futuras versiones.	Requerimiento no funcional
18	La aplicación no debe ocupar más de 20 MB.	Requerimiento no funcional

Las etapas que se desarrollarán en esta investigación está dividida en 03 incrementos, los cuales, cuentan con una tabla de requerimientos iniciales y una tabla de conformidad en cada etapa según se implementó la solución.

a) Primer incremento

En esta primera etapa se desarrolló lo esencial del aplicativo para conectar el mismo con una base de datos local. Se tomó como referencias los requerimientos y se empezó cumpliendo algunas características esenciales como los requerimientos no funcionales. Luego, se diseñó y

desarrollo la etapa de registro de usuario y de esta forma probar la conectividad con la base de datos. En la tabla 9, se ve el alcance del primer incremento.

Tabla 9

Requerimientos – Incremento 1

Item	Descripcion	Etapa de desarrollo
1	La aplicación se debe desarrollar con el lenguaje de programación Java.	Requerimiento no funcional
2	El entorno de desarrollo debe ser Android Studio, especializado para las aplicaciones nativas con sistema operativo Android.	Requerimiento no funcional
3	La aplicación deberá ser compatible desde el sistema operativo Android 5.0	Requerimiento no funcional
4	El código debe ser desarrollado de forma ordenada y modular para ser escalable y flexible en su mantenimiento en futuras versiones.	Requerimiento no funcional
5	La aplicación no debe pesar más de 20 MB.	Requerimiento no funcional
6	El modelo utilizado para esta aplicación debe ser Cliente – Servidor.	Diseño
7	La aplicación debe contar con un servidor web para la administración de base de datos.	Diseño
8	La conexión con el servidor se debe realizar a través de implementaciones en lenguaje PHP y el paquete de software libre Xampp para la gestión de MYSQL.	Diseño
9	La base de datos debe ser de tipo relacional y se administrará con la herramienta phpMyAdmin.	Diseño
10	La base de datos de referencia, se basará en la recopilación de información de las investigaciones y repositorios oficiales.	Diseño
11	Debe tener una pantalla en donde se agregue usuarios y se acumulen en una base de datos. Deberá contar con alertas de buena y mala conexión.	Diseño

Para cumplir con los requerimientos 1 y 2, era necesario elegir el entorno de desarrollo y el lenguaje a utilizar en la programación. Para cumplir con ello, se consideró lo recomendado por los especislistas en TIC de las entrevistas, y se eligió Android Studio y el

lenguaje de programación Java. En el Apéndice B, se presenta el Software y el lenguaje utilizado.

Siguiendo con el avance de este incremento, en el requerimiento 3 se necesitaba que el aplicativo sea compatible con Android 5, para lo cual se procedió a realizar en el SDK Manager de Android Studio, la descarga correspondiente de Android 5.0 (Lollipop) y de esa forma, el aplicativo móvil desarrollado también de respuesta a ese requerimiento. En el Apéndice C, se puede divisar la instalación realizada.

Con respecto al requerimiento 4, se tomó en consideración al iniciar el desarrollo de código de la primera clase en el programa, en este caso: activity_main. Sin embargo, no es posible dar conformidad, ya que el código del aplicativo móvil no está completo, es por ello, que es necesario volverlo a validar en el último incremento.

El requerimiento 5, al igual que el anterior, no fue posible resolver, ya que el aplicativo móvil no está culminado y aún es posible pasar el umbral de los 20Mb propuestos. Hasta el momento el aplicativo móvil pesa 7Mb y cumple, pero aún no se dio la conformidad respectiva para culminar con este requerimiento.

El diseño de la solución propuesta se basó en el modelo cliente- servidor, el cual, tiene un uso frecuente en aplicaciones móviles y en la distribución de tareas a través de servidores de servicios. Los clientes, en este caso son los equipos celulares con el aplicativo instalado, los cuales realizan las consultas, y el servidor, el cual se trata básicamente de una computadora en donde se tiene configurado el servicio, contó con una conexión local y estable a la que el usuario se conectó para la respectiva actualización y validación del ataque en tiempo real. Con el fin de demostrar el cumplimiento del requerimiento 6 sobre el modelo a utilizar, y con el apoyo del sistema de modelo UML, se realizó un diagrama de clases presentado en el Apéndice D y un diagrama de casos de uso en el Apéndice E, y de esa forma, plasmar de forma gráfica

el diseño del aplicativo. Asimismo, para presentar el modelo de comportamiento, se elaboró un cuadro de flujo del proceso de detección y generación de alertas adjunto en el Apéndice F. Asimismo, para dar un panorama general de la infraestructura del hardware y software utilizado y sus medios, se realizó un Diagrama de despliegue, presentado en el Apéndice G.

Con referencia a los actores en los diagramas, se especifica lo siguiente:

- Usuario: Se refiere a la persona o teléfono móvil que ejecuta el aplicativo móvil anti-phishing instalado, recibe los mensajes SMS, realiza la consulta y recibe la respuesta del servidor para su funcionamiento en detección de phishing, posterior a ello genera las alertas o las recomendaciones respectivas.
- Atacante: Se le llamó así, a la persona o teléfono móvil que envía el mensaje de texto (SMS) infectado con phishing al usuario.
- Aplicativo: Se refiere al software SMS SEGURO, el cual es el aplicativo móvil creado para la investigación.
- Administrador: Se refiere a la persona, empresa o sistema que se encargará de actualizar las bases de datos. Asimismo, realiza el mantenimiento y actualización en las versiones del aplicativo.
- El operador de servicio de Telefonía, se compuso por el medio inalámbrico 3G,4G y/o 4.5G contratado para el servicio de recepción y transmisión de voz y datos en el dispositivo móvil.

En el requerimiento 7, se necesita un servidor web para la interacción con los clientes en las respectivas solicitudes de servicio. Para ello, se utilizó un servidor web Apache, el cual se configuró según se detalla en el Apéndice H. Este servidor forma parte del paquete de Software Libre XAMPP, en el cual también se divisa el módulo Mysql gestionado por el aplicativo phpMyadmin.

Según el requerimiento 8, la conexión con el servidor se debe realizar a través de implementaciones en lenguaje PHP y el paquete de software libre Xampp para la gestión de MYSQL. Para cumplir con ello, se implementó web services con código PHP en el software Sublime Text. Para este incremento se implementó los siguientes webs services:

- Conexión: En este web service se realiza la conectividad entre los datos enviados desde el aplicativo hacia la base de datos mySQL.
- Insertar: En este web service se envía los datos del registro realizado por el nuevo usuario desde el aplicativo hacia los registros en la base de datos mySQL.

En el Apéndice I se presenta el código de los webs services realizados para este incremento en el software Sublime Text.

Con respecto al requerimiento 9. Sobre la base de datos relacional y administrada por el aplicativo phpMyadmin, fue necesario crear una base de datos local de pruebas. La base fue de tipo relacional y se administró con la herramienta phpMyAdmin. El objetivo fue tener una base de datos fuera del aplicativo para evitar problemas de procesamiento y hardware. Asimismo, la base de datos tiene pocos campos a razón de interactuar sólo con los registros de usuarios (primer incremento), validación de phishing contenido en los mensajes de texto (SMS) recibidos (segundo incremento) y generación de alertas y recomendaciones (tercer incremento). En el Apéndice J, se detalla el modelo de entidad relación creado de la base de datos. Asimismo, en el Apéndice K, se presenta las tablas de los usuarios y malwares creados para las pruebas y futuro muestreo, todo dentro aplicativo phpMyAdmin.

Para cumplir el requerimiento 10 sobre el tipo de repositorios a utilizar. Para esta investigación, se tomó como referencia la base de datos de Phishing del recopilatorio Phishtank de Cisco, la cual fue cargada a la base de datos creada en esta investigación. El formato elegido fue CSV, la página oficial otorga diferentes formatos para las implementaciones, pero se utilizó

este formato por ser compatible con Excel, de esa forma se pudo ajustar en número de columnas para que pueda ser aceptado sin problemas en el aplicativo phpMyAdmin. En el Apéndice L, se presenta la imagen del repositorio Phistank y como se subió al aplicativo phpMyadmin luego de las modificaciones respectivas.

Para este incremento, también se logró cumplir con el requerimiento 11, en el cual se necesita una pantalla en donde se pueda agregar usuarios y se acumulen en una base de datos, asimismo, generar alertas de buen y mal registro del mismo. Para ello, en el aplicativo cliente se implementó 01 clase llamado: MainActivity.java, y también un layout con el mismo nombre, el cual, genera un formulario con los campos nombre, número de celular y correo electrónico. El usuario deberá completar la información para que los mismos se registren en la base de datos del servidor. Asimismo, se creó un botón de registro el cual ejecuta el envío de los datos al web service correspondiente para su posterior ingreso en la base de datos local. Finalmente, se debe aclarar que para poder ingresar al siguiente Activity del aplicativo, es necesario el registro sea exitoso, solo así se procede a desbloquear el botón de Iniciar, el cual nos llevará al Activity de detección, trabajado en el segundo incremento del aplicativo móvil. Finalmente, se realizó el código posible para la validación de conexión con la base de datos, en el caso que no hubiera, se mostrará en pantalla la alerta: “PROBLEMAS CON EL SERVIDOR, CONTACTAR A SOPORTE TECNICO”, y en el caso que sea exitoso, se mostrará el mensaje: “REGISTRO EXITOSO”. En el Apéndice LL, se presenta el Activity de registro de usuario, y en el Apéndice M y N, se visualiza los procesos y alertas de problemas de conexión y registro exitoso respectivamente.

Según el cuadro de requerimientos del aplicativo móvil, en este incremento se logró completar algunos alcances del total, cumpliendo el objetivo inicial de este primer incremento, los cuales, se detallan en el cuadro de conformidad de la Tabla 10.

Tabla 10

Conformidad de incremento 1

Item	Descripción	Etapa de desarrollo	Resultado
1	La aplicación se debe desarrollar con el lenguaje de programación Java.	Requerimiento no funcional	Conforme
2	El entorno de desarrollo debe ser Android Studio, especializado para las aplicaciones nativas con sistema operativo Android.	Requerimiento no funcional	Conforme
3	La aplicación deberá ser compatible desde el sistema operativo Android 5.0	Requerimiento no funcional	Conforme
4	El código debe ser desarrollado de forma ordenada y modular para ser escalable y flexible en su mantenimiento en futuras versiones.	Requerimiento no funcional	No conforme
5	La aplicación no debe pesar más de 20 MB.	Requerimiento no funcional	No conforme
6	El modelo utilizado para esta aplicación debe ser Cliente – Servidor.	Diseño	Conforme
7	La aplicación debe contar con un servidor web para la administración de base de datos.	Diseño	Conforme
8	La conexión con el servidor se debe realizar a través de implementaciones en lenguaje PHP y el paquete de software libre Xampp para la gestión de MYSQL.	Diseño	Conforme
9	La base de datos debe ser de tipo relacional y se administrará con la herramienta phpMyAdmin.	Diseño	Conforme
10	La base de datos de referencia, se basará en la recopilación de información de las investigaciones y repositorios oficiales.	Diseño	Conforme
11	Debe tener una pantalla en donde se agregue usuarios y se acumulen en una base de datos. Deberá contar con alertas de buena y mala conexión.	Diseño	Conforme

b) Segundo incremento

Continuando con el procedimiento de Ingeniería, en esta segunda etapa, es necesario ya realizar la detección de phishing en mensajes de texto (SMS) a través del aplicativo móvil propuesto. Para ello, se trató de avanzar los requerimientos relacionados a la funcionalidad de

detección a través del diseño, desarrollo y validación del aplicativo móvil. En la Tabla 11 se detalla los requerimientos para el incremento 2.

Tabla 11

Requerimientos - incremento 2

Item	Descripción	Etapa de desarrollo
1	El aplicativo debe tener un algoritmo que pueda recibir y leer el contenido de los mensajes de texto SMS recibidos	Diseño
2	Debe contar con una pantalla de detección de phishing, en donde se predice si el mensaje de texto (SMS) está infectado o no con Phishing.	Diseño
3	La aplicación deberá identificar y mostrar en pantalla el mensaje obtenido y el número telefónico del emisor.	Diseño y validacion del software
4	La aplicación debe tener la capacidad de conectarse con la base de datos, para resolver la consulta y recibir la validación en tiempo real sobre detección de Phishing.	Diseño y validacion del software

Con respecto al requerimiento 1, se necesita un algoritmo que pueda leer los mensajes de texto (SMS), para luego poder validar su contenido en el aplicativo. Para cumplir con ello, se utilizó el componente Broadcast Receiver, con el cual podíamos tener acceso a los mensajes de texto recibidos en el sistema, generando un algoritmo en la cual podamos captar y almacenar el mensaje recibido para posteriormente leerlo y filtrarlo. La clase que se encargó de ello se le llamó: Myreceiver.java, el cual, su código se muestra en el Apéndice Ñ.

Continuando con este segundo incremento, se resolvió el requerimiento 2 y 3, los cuales, son complementarios. Para cumplir con ambos requerimientos, es necesario crear un layout nuevo en donde se detecte phishing en tiempo real y muestre los resultados en la misma. Asimismo, este layout debe describir el mensaje recibido y el número telefónico del cual fue enviado.

Para esta parte del proceso de ingeniería, se diseñó e implementó 01 clase más en el aplicativo, llamado: activity_detector.java. Este nuevo Activity, cumple la función de presentar en pantalla en tiempo real, el resultado de la detección de phishing en cada mensaje de texto (SMS) recibido del equipo celular cliente.

La detección se produce bajo ciertas condiciones del algoritmo de trabajo de esta clase. La detección se logró en base a la combinación de dos algoritmos de detección para poder llegar a solucionar una mayor cantidad de incidencias de Phishing. El primer algoritmo compara el contenido del mensaje de texto recibido por la clase Myreceiver.Java, el cual, se compara con la base de datos creada, la cual previamente tiene cargados los registros de la biblioteca Phistank de Cisco. A través de esta comparación el algoritmo valida si está infectado el mensaje de texto (SMS) recibido. El segundo algoritmo trabaja en la detección de malware sospechoso a través de detección de enlaces dentro del mensaje de texto con la cabecera de la dirección web sin certificado SSL. Cualquier mensaje de texto (SMS) que cuente con una dirección web que inicie con Http:// en su contenido, es detectado como sospechoso y por ende considerado como infectado con phishing. En una primera implementación hubo problemas por no reconocer la cadena de texto exacta lo cual se fue afinando el algoritmo hasta poder filtrar de forma adecuada el mensaje de texto (SMS) recibido. Para este aplicativo móvil se utilizó solo estos dos algoritmos de detección, pero por lo ordenado y sencillo de la estructura del código, se puede implementar fácilmente otras formas de detección haciendo al aplicativo móvil escalable y más robusto. En el Apéndice O, se presenta una de las formas de detección a través de un algoritmo que recorre el mensaje de texto SMS recibido en la búsqueda de enlaces sospechosos sin certificación SSL.

El layout de la clase activity_detector se presenta en el Apéndice P de la presente investigación. Asimismo, en el Apéndice Q se muestra ejemplos de detección de phishing,

tanto para una detección positiva y una negativa dentro del mismo layout, en estas imágenes también se observa la detección y visualización del mensaje de texto (SMS) y el número telefónico de envío solicitados en el requerimiento 2 y 3 de este incremento.

Con el fin de poder cumplir con el requerimiento 4, se implementó un web service más, llamado Buscar, el cual, se encarga de enviar palabras clave para la búsqueda de registros en la base de datos y de esa forma poder resolver si hay o no infección en los mensajes de texto (SMS). Hubo problemas en la realización de este web service, en un principio no hubo recepción de datos de la base MySQL creada, así que se tuvo que realizar un artificio en la validación dentro del web service para que pueda funcionar correctamente, para ello, se realizó una validación si el web service devolvía la palabra "correcto", si era así la búsqueda era exitosa y por ende se procedía a realizar las operaciones necesarias para la visualización de resultados en el aplicativo móvil. En el Apéndice R, se presenta el código del web service Buscar en su primera y segunda versión.

Aspectos de la validación de Software:

Continuando con el desarrollo de los requerimientos, es preciso hacer un paréntesis y aclarar lo relacionado a la validación del software, la cual, se realizó en base a las pruebas de funcionamiento en la detección de phishing y posteriormente (tercer incremento) en la generación de alertas, con el fin de comprobar la calidad y efectividad del aplicativo móvil para el cumplimiento de los objetivos propuestos. Para ambas pruebas, se utilizó la muestra de la investigación. El 50% de los mensajes fueron infectados con dominios maliciosos de la base de datos de la web: https://www.phistank.com, se eligió esta base de datos por ser una de las más amplias, confiables y por pertenecer a OPEN DNS, empresa encargada de brindar servicios de navegación segura y que ahora pertenece a CISCO Systems. El otro 50% restante, fueron creados de propia autoría, los cuales contiene direcciones web sospechosas, el 80% con nulo

protocolo SSL y un 20% con protocolo SSL. En la Tabla 12 se detalla las características de los 20 SMS que sirven para el análisis de calidad en la detección de malware y generación de alertas.

Tabla 12

Características de la muestra de estudio

Ítem	Descripción	Cuenta con certificado SSL (Secure socket layer)	Tipo de Infección
1	https://rakuten.grp005.work	Sí	Recopilada de base Phishtank.
2	https://chat-whatsapp-join-hot.duckdns.org	Sí	Recopilada de base Phishtank.
3	https://amazon.co.jp.zbmhw.com/signin	Sí	Recopilada de base Phishtank.
4	https://bit.ly/3swPxhO	Sí	Recopilada de base Phishtank.
5	https://eepayments.net/	Sí	Recopilada de base Phishtank.
6	http://jpl1.top	No	Recopilada de base Phishtank.
7	http://m-faceboook.mypi.co/	No	Recopilada de base Phishtank.
8	http://www.mxrr.com/?p=newcontact&amp	No	Recopilada de base Phishtank.

9	http://activeproductos.com/	No	Recopilada de base Phishtank.
10	http://dealtix.com/pop/	No	Recopilada de base Phishtank.
11	Hola, ingresa a mi nuevo sitio web: http://www.lomasbaratopp.com	No	Fuente propia
12	Ganaste la lotería, ingresa aquí para recibir el premio: http://www.loteriatotalp.com	No	Fuente propia
13	Lotería nueva, boletos gratis en http://www.ganafacilsi.com	No	Fuente propia
14	Hola, somos BVA, acabas de realizar una transferencia bancaria sospechosa. Verifica tus datos en: http://www.bvaalert.com	No	Fuente propia
15	Su bono del gobierno de s/350.00, ya fue depositado. Verifica aquí: https://bonogobierno.com	Sí	Fuente propia
16	Checa tu bono: http://www.bonodelgobierno.com	No	Fuente propia
17	Ganaste un auto, confirma tus datos de inscripción: http://www.autoperugol.com	No	Fuente propia
18	Ganaste un curso gratis: https://www.cursosgratispp.com	Sí	Fuente propia
19	Recoge tu devolución de impuestos. http://www.sunatperugob.com	No	Fuente propia

20	Tu pedido ha sido cancelado. Para devolución de tu dinero, inscribirse aquí: http://www.devoluciones-peru.com	No	Fuente propia

El análisis fue realizado a través de cálculos de porcentaje de detección para este incremento y posteriormente en la generación de alertas y recomendaciones. Ambos cálculos tuvieron la finalidad de ubicar el TPR (Tasa de verdaderos positivos) de ambos indicadores propuestos. La explicación se realizó a través de cuadros comparativos en hojas de cálculo con apoyo de fórmulas matemáticas. El detalle para este incremento, es analizado en las fichas de registro respectivas presentadas en el Apéndice S y Y respectivamente.

Para un mayor detalle del equipamiento utilizado en las pruebas, se elaboró un cuadro con las características iniciales de los dispositivos celulares que se utilizan para las pruebas de calidad de detección. En total fueron dos dispositivos para las pruebas; un dispositivo celular receptor con sistema operativo Android, de gama baja, al cual se le instaló el aplicativo desarrollado; y un dispositivos emisor, de gama media con sistema operativo Android, de donde se envían los mensajes de texto para las pruebas de calidad de detección. Las características de los equipos celulares para las pruebas, se definen en la Tabla 13.

Tabla 13

Características de los equipos celulares para las pruebas.

Ítem	Tipo de equipo en la investigación	Gama	Sistema operativo	Procesador	Almacenamiento	Tipo de Batería
1	Receptor	Baja	Android 5.0	2Gb	8Gb	Li-Ion
2	Emisor	Media	Android 11.0	3Gb	32 Gb	Li-Ion

Las pruebas realizadas para validar el funcionamiento del layout de detección, fue a través del envío de un mensaje sin phishing con el contenido de “hola”, el cual es detectado como un mensaje sin phishing. Posterior a ello, se define un mensaje de prueba con el contenido http://www.malware.com, el cual arroja un resultado positivo en la detección de phishing. Por otro lado, con respecto a las fichas Pre test y Post test, se debe indicar lo siguiente:

a) Pre test: En esta prueba se observa el procedimiento de la recepción de mensajes de texto (SMS) infectados con phishing y la detección generada por otro antimalware, en este caso se utilizó al antivirus Bit Defender.

Bit defender es una solución actual de las más prestigiosas en la detección de virus, Se eligió este producto porque cuenta con una herramienta exclusiva para la detección de phishing en enlaces y SMS. La versión utilizada es la última hasta la fecha (versión 3.3.172.1997). Las pruebas de pre test fueron en su totalidad enviadas al dispositivo celular con este antivirus instalado. En el Apéndice T, se muestra el detalle de la solución instalada para las pruebas.

b) Post test: En esta prueba se observa el procedimiento en la detección de phishing a través del aplicativo móvil: Mensaje Seguro, creado para esta investigación.

El procedimiento de la detección de phishing en las muestras se plasma en los gráficos del Apéndice U.

Para finalizar esta etapa, se presenta el cuadro de conformidad para el incremento 2 en la Tabla 14.

Tabla 14

Conformidad de incremento 2

Item	Descripción	Etapa de desarrollo	Resultado

1	El aplicativo debe tener un algoritmo que pueda recibir y leer el contenido de los mensajes de texto SMS recibidos	Diseño	Conforme
2	Debe contar con una pantalla de detección de phishing, en donde se predice si el mensaje de texto (SMS) está infectado o no con Phishing.	Diseño	Conforme
3	La aplicación deberá identificar y mostrar en pantalla el mensaje obtenido y el número telefónico del emisor.	Diseño y validacion del software	Conforme
4	La aplicación debe tener la capacidad de conectarse con la base de datos, para resolver la consulta y recibir la validación en tiempo real sobre detección de Phishing.	Diseño y validacion del software	Conforme

c) Tercer incremento

En este último incremento del aplicativo móvil, se realizó las funcionalidades de alertas y recomendaciones del aplicativo. Asimismo, se validó algunos requerimientos no funcionales pendientes, para poder culminar con todos los requerimientos propuestos para este aplicativo móvil. En la tabla 15 se presenta el listado completo de los requerimientos para este último incremento.

Tabla 15

Requerimientos - incremento 3

Item	Descripción	Etapa de desarrollo
1	Debe contar con una pantalla de recomendaciones ante ataques de tipo Phishing	Diseño y validacion del software
2	El tiempo de duración entre la recepción y la generación de alerta en la detección de Phishing no debe superar los 02 segundos.	Validacion del software
3	La aplicación deberá generar alertas sobre las detecciones de Phishing a través de notificaciones al recibir cualquier mensaje de texto (SMS).	Validacion del software

4	El código debe ser desarrollado de forma ordenada y modular para ser escalable y flexible en su mantenimiento en futuras versiones.	Requerimiento no funcional
5	La aplicación no debe pesar más de 20 MB.	Requerimiento no funcional

Continuando con el desarrollo del software, se diseñó y desarrolló un tercer layout que servirá de complemento al layout de detección de Phishing. Asimismo, con esta nueva implementación se cumpliría el ítem 1 del requerimiento para este incremento. En esta pantalla, se presenta las recomendaciones en el caso que el aplicativo haya detectado infección en alguno de los mensajes de texto (SMS) recibidos. Se automatizó al botón que lanza al activity de recomendaciones, el cual, solo se visualiza al detectarse un phishing. En el Apéndice V se presenta el activity desarrollado.

Para cumplir el requerimiento 2, en donde se necesita que el proceso desde que se recibe el mensaje de texto (SMS) hasta que se genera la predicción por el aplicativo móvil propuesto, sea menor a dos segundos. Para constatar ello, se necesitó los tiempos medidos en las fichas de registro POST TEST, por tratarse de medir los tiempos con la solución propuesta “SMS SEGURO”, por lo cual, se tomó el promedio de las duraciones desde que llega el mensaje de texto hasta que se genere una alerta en el aplicativo. En la Tabla 16, se detalla un cuadro en base a los tiempos de recepción del mensaje de texto, sacados de la ficha de Generación de alerta Post test, las cuales se comparan con el tiempo en que demora el aplicativo en generar la alerta o recomendación posterior. En este cuadro se puede observar, que la media o promedio de la duración del proceso es de 1.4 segundos, donde se concluye que este requerimiento ha sido resuelto satisfactoriamente.

Tabla 16

Duración de proceso de generación de alertas.

Muestra	Tiempo de recepción	Tiempo de generación de alerta o predicción	Total de segundos del proceso	Media
1	22:22:02	22:22:04	2	1.4 Seg.
2	22:24:26	22:24:28	2	
3	22:24:58	22:24:59	1	
4	22:25:28	22:25:30	2	
5	22:26:02	22:26:04	2	
6	22:27:18	22:27:19	1	
7	22:28:46	22:28:48	2	
8	22:29:13	22:29:15	2	
9	22:29:33	22:29:35	2	
10	22:30:12	22:30:14	2	
11	22:32:11	22:32:12	1	
12	22:33:13	22:33:14	1	
13	22:34:17	22:34:18	1	
14	22:36:19	22:36:20	1	
15	22:37:27	22:37:28	1	
16	22:38:55	22:38:56	1	
17	22:39:48	22:39:49	1	
18	22:40:21	22:40:22	1	
19	22:41:36	22:41:37	1	
20	22:42:47	22:42:48	1	

Con respecto al requerimiento 3, se realizó código complementario para la generación de alertas según la casuística. Las alertas fueron de dos tipos:

- Alertas internas: Son las predicciones visualizadas dentro del layout de detección realizado en el segundo incremento. Los tipos de predicciones que se generan básicamente son dos: “Mensaje Seguro” de color verde, y “Ataque Phishing, no abrir”, de color rojo. Asimismo, para el caso de la Detección positiva de phishing, se genera un botón llamado: RECOMENDACIONES, el cual, nos lleva al layout de complemento en donde se recomienda posibles soluciones al problema. Este tipo de alerta no está

considerada para las mediciones de tiempos en las alertas, por ser una alerta opcional para el usuario. El layout de recomendaciones se presenta en el Apéndice W1.

- Alertas externas: Son aquellas que son presentadas como notificaciones fuera del

  Aplicativo. Las dos principales son: "SMS SEGURO", cuando el mensaje de texto (SMS) no contiene Phishing, y "ATAQUE PHISHING, NO ABRIR SMS!", la cual se genera al detectar phishing en el mensaje de texto (SMS) recibido. Asimismo, se puede citar los generados en el incremento 1: "REGISTRO EXITOSO" y "PROBLEMAS CON EL SERVIDOR, CONTACTAR A SOPORTE TECNICO", los cuales fueron automatizados para realizar acciones de resultado en el registro de usuarios o conectividad con el servidor. En el Apéndice W2, se observa el tipo y el funcionamiento de las alertas implementadas para este incremento 3.

En el Apéndice X, se muestra el procedimiento en la generación de alertas con la muestra de la investigación, tanto para el pre test, a través de la observación en el aplicativo Bit Defender, y el post test en donde se observa el funcionamiento del aplicativo SMS Seguro propuesto.

Con respecto a la validación del Software, y en específico lo referente a la generación de alertas, se utilizó la misma muestra que para la ficha de detección realizada en el incremento 2.

En este incremento, la muestra designada para la investigación se plasma en dos fichas de registro de las cuales se debe indicar lo siguiente:

a) Pre test: En esta prueba se observa el procedimiento de la generación de alertas al recibir mensajes de texto (SMS) con phishing por otro antimalware, en este caso se utilizó al antivirus Bit Defender como herramienta de análisis de los mismos.

b) Post test: En esta prueba se observa el procedimiento en la generación de alertas al recibir mensajes de texto (SMS) por el aplicativo móvil propuesto para esta investigación.

Las fichas sobre la generación de alertas, tanto de Pre test como Post test, se detallan en el Apéndice Y.

Para continuar con el incremento 3, se realizó el cumplimiento del requerimiento 4, el cual, necesita que el aplicativo sea flexible y escalable. Para ello, se tuvo en cuenta, en el desarrollo de código, ser lo más modular posible y sobre todo ordenado, de esa forma se garantiza agilidad en el mantenimiento y escalabilidad del aplicativo móvil. El código concluido de este desarrollo, recién nos sirve para constatar si esta ordenado, flexible y de fácil mantenimiento para futuras mejoras, en el incremento 1 aún no se podía concluir este requerimiento no funcional. En el Apéndice Z, se presenta algunas imágenes de la estructura general del código final. El código de programación completo, y como resultado de los 03 incrementos presentados; se subió al repositorio de GitHub, el cual puede ser constatado en el siguiente enlace: https://github.com/Pablofloresbarrios/sms.git.

Culminando de completar los requerimientos, se trató de resolver el requerimiento no funcional pendiente de la necesidad que el producto final pese menos de 20 MB en total, algo que en el incremento 1 tampoco se podía definir por tener el código del aplicativo móvil incompleto. La finalidad de tener solo 20Mb de tamaño final consiste en brindar agilidad en todo sentido y pueda desplegarse fácilmente en cualquier dispositivo Android desde la versión 5. Para ello, se realizó un cuadro comparativo, al día de hoy, entre los tamaños en Mb de aplicativos más representativos de tipo antivirus para teléfonos celulares Android. Los aplicativos elegidos para la comparativa son los siguientes: Bit defender, Avira Security, Norton 360m Mobile Security, McAfee Security y el aplicativo móvil desarrollado: SMS

SEGURO, el cual ocupa menor espacio de disco, resultando luego del tercer incremento 11.59 MB de tamaño. Con esta comparativa se cumple con el requerimiento 18. La comparativa se presenta a través de las imágenes del Apéndice AA y el resumen en la Tabla 17.

Tabla 17

Resumen de comparativa de antivirus comerciales y SMS seguro.

Antivirus	Ultima actualización	Sistema operativo compatible	Tamaño en MB
Avira	14-Abr-22	Android 6 y posterior	34.52 MB
Bitdefender	27-May-22	Android 5 y posterior	53.07 MB
McAfee	2-May-22	Android 7 y posterior	24.63 MB
Norton	16-May-22	Android 8 y posterior	28 MB
SMS SEGURO	28-May-22	Android 5 y posterior	11.59 MB

Finalmente, en la Tabla 18, se presenta el cuadro de conformidad para el incremento 3, el cual, presenta el cumplimiento total de los requerimientos para este incremento, coincidiendo en completar el cuadro de requerimientos general del aplicativo móvil y por consiguiente cumpiendo con el OE1 de la investigación.

Tabla 18

Conformidad de incremento 3

Item	Descripción	Etapa de desarrollo	Resultado
1	Debe contar con una pantalla de recomendaciones ante ataques de tipo Phishing	Diseño y validacion del software	Conforme
2	El tiempo de duración entre la recepción y la generación de alerta en la detección de Phishing no debe superar los 02 segundos.	Validacion del software	Conforme

3	La aplicación deberá generar alertas sobre las detecciones de Phishing a través de notificaciones al recibir cualquier mensaje de texto (SMS).	Validacion del software	Conforme
4	El código debe ser desarrollado de forma ordenada y modular para ser escalable y flexible en su mantenimiento en futuras versiones.	Requerimiento no funcional	Conforme
5	La aplicación no debe pesar más de 20 MB.	Requerimiento no funcional	Conforme

2.5 Aspectos éticos

En la presente investigación, se consideró aspectos relevantes como las normas APA, el manual de redacción de UPN, los formatos de apoyo y la asesoría de la Universidad Privada del Norte. Con respecto a la preparación, recolección y análisis de los datos obtenidos; se deja constancia que los datos elaborados para las unidades de estudio y los datos obtenidos son fidedignos, confiables y solo interpretados de lo obtenido en las encuestas y las pruebas de calidad realizadas en campo.

Se declara fiel cumplimiento a las normas establecidas por la Universidad con respecto a la obtención de información complementaria, y la ética en la elaboración de esta investigación.

CAPÍTULO III: RESULTADOS

3.1 Análisis Descriptivo

En esta investigación se implementó un aplicativo móvil con la finalidad de detectar phishing en mensajes de texto (SMS) en dispositivos con sistema operativo Android. Asimismo, demostrar la eficiencia del aplicativo en la funcionalidad de detección de phishing y generación de alertas en cada mensaje recibido. Para lograr ello, se realizaron mediciones de cada indicador de la variable dependiente a través de las fichas de registro respectivas.

- Indicador 1: Tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS).

  Para este indicador se obtuvo un 35% de TPR en el Pre test, el cual corresponde al porcentaje representativo de 7 muestras detectadas sobre la muestra total, este porcentaje aumentó en el post test, en donde se detectó en 18 ítems de la muestra, lo cual, equivale a un total de 90% de detección de Phishing. Con lo cual, hubo un aumento de eficiencia en un 55%.

  En la Tabla 19 se muestra un resumen del indicador 1 y el cuadro descriptivo completo resultante del software SPSS se presenta en la figura 13. Asimismo, en las figuras 14 y 15, se presentan los histogramas del Pre test y Post test de la detección de phishing observada.

Tabla 19

Resumen de indicador 1

Estadística descriptiva – Indicador 01				
	Cantidad de muestra	Cantidad de muestra en estado positivo	Cantidad de muestra en estado negativo	Promedio

Pre Test – TPR Detección de Phishing	20	7	13	35%
Post Test – TPR Detección de Phishing	20	18	2	90%

Figura 13

Cuadro descriptivo obtenido desde el SPSS del indicador 1

Descriptivos

			Estadístico	Error típ.
Estado pre test Detección de Phishing	Media		,35	,109
	Intervalo de confianza para la media al 95%	Límite inferior	,12	
		Límite superior	,58	
	Media recortada al 5%		,33	
	Mediana		,00	
	Varianza		,239	
	Desv. típ.		,489	
	Mínimo		0	
	Máximo		1	
	Rango		1	
	Amplitud intercuartil		1	
	Asimetría		,681	,512
	Curtosis		-1,719	,992
Estado post test detección de phishing	Media		,90	,069
	Intervalo de confianza para la media al 95%	Límite inferior	,76	
		Límite superior	1,04	
	Media recortada al 5%		,94	
	Mediana		1,00	
	Varianza		,095	
	Desv. típ.		,308	
	Mínimo		0	
	Máximo		1	
	Rango		1	
	Amplitud intercuartil		0	
	Asimetría		-2,888	,512
	Curtosis		7,037	,992

Figura 14

Histograma Pre test de detección de phishing

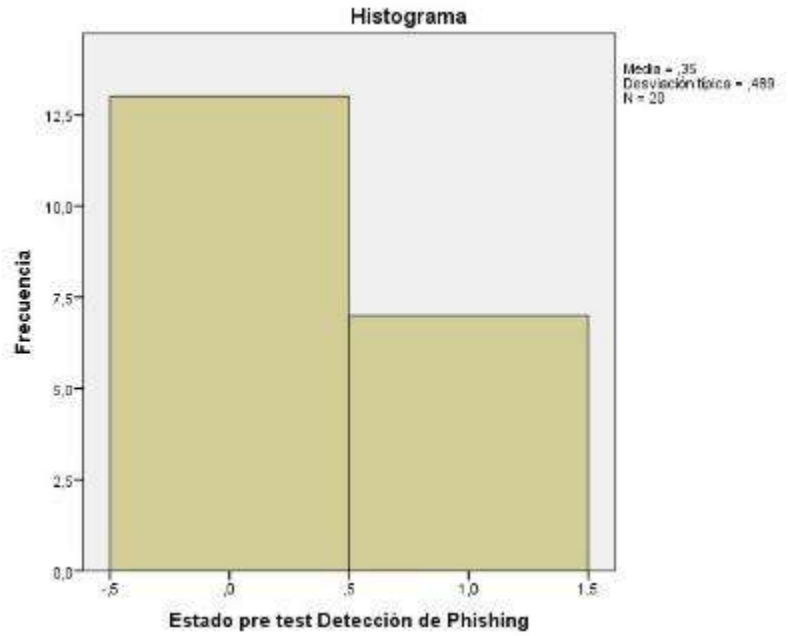
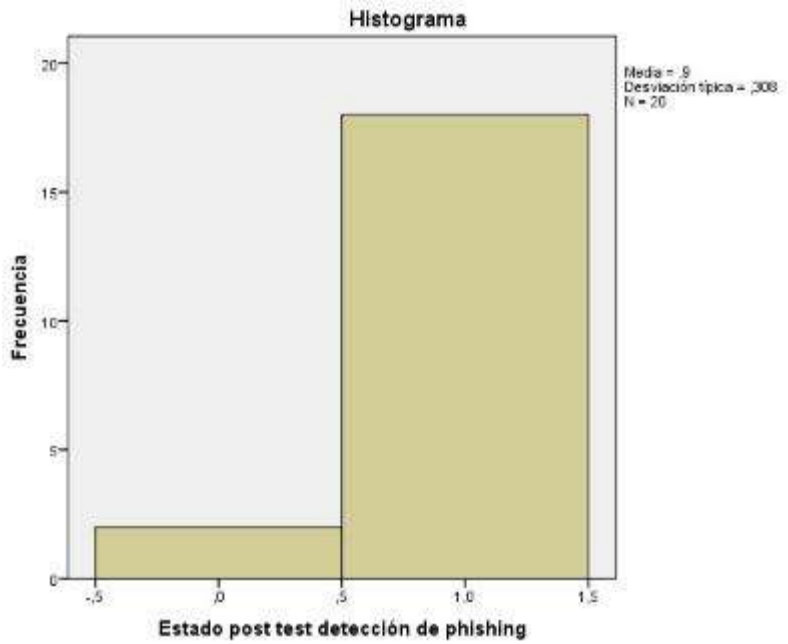


Figura 15

Histograma Post test de detección de phishing



- Indicador 2: Tasa de verdaderos positivos (TPR) de generación de alertas en los mensajes de texto SMS recibidos.

En este segundo indicador, se obtuvo también un 35% de TPR en el Pre test, equivalente a una generación de alertas de 7 ítems en total, este porcentaje aumentó en el post test, el cual brindó un total de generación de alertas en 18 ítems, es decir, un 90% de la muestra total. Con lo cual, también hubo un aumento de eficiencia en un 55%. En la Tabla 20 se muestra un resumen del indicador 2 y el cuadro descriptivo completo resultante del software SPSS se presenta en la figura 16. Asimismo, en las figuras 17 y 18, se presentan los histogramas del Pre test y Post test de la detección de phishing observada.

Tabla 20

Resumen de indicador 2

Estadistica descriptiva - indicador 02				
	Cantidad de muestra	Cantidad de muestra en estado positivo	Cantidad de muestra en estado negativo	Promedio
Pre Test - TPR Generación de alertas	20	7	13	35%
Post Test - TPR Generacion de alertas	20	18	2	90%

Figura 16

Cuadro descriptivo obtenido desde el SPSS del indicador 2

Descriptivos

			Estadístico	Error típ.
Estado pre test generacion alerta	Media		,35	,109
	Intervalo de confianza para la media al 95%	Límite inferior	,12	
		Límite superior	,58	
	Media recortada al 5%		,33	
	Mediana		,00	
	Varianza		,239	
	Desv. típ.		,489	
	Mínimo		0	
	Máximo		1	
	Rango		1	
	Amplitud intercuartil		1	
	Asimetría		,681	,512
	Curtosis		-1,719	,992
Estado post test generacion de alerta	Media		,90	,069
	Intervalo de confianza para la media al 95%	Límite inferior	,76	
		Límite superior	1,04	
	Media recortada al 5%		,94	
	Mediana		1,00	
	Varianza		,095	
	Desv. típ.		,308	
	Mínimo		0	
	Máximo		1	
	Rango		1	
	Amplitud intercuartil		0	
	Asimetría		-2,888	,512
	Curtosis		7,037	,992

Figura 17

Histograma Pre test de generación de alerta

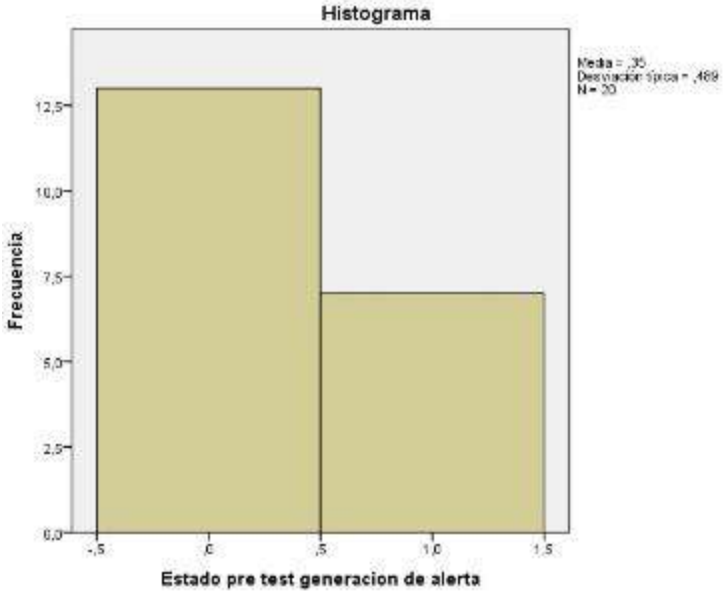
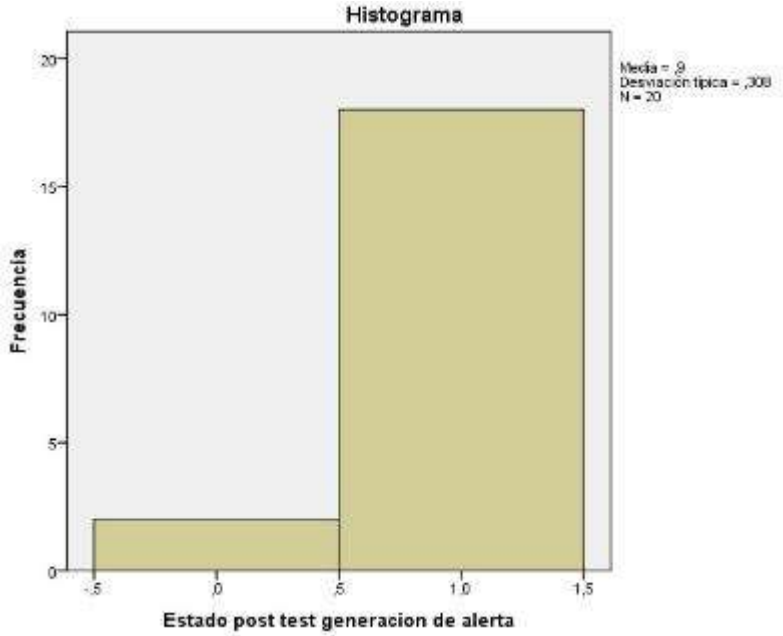


Figura 18

Histograma Post test de generación de alerta



3.2 Análisis Inferencial

Para realizar el análisis Inferencial, es necesario ejecutar una prueba de normalidad.

Existen diversos tipos de prueba de normalidad, para esta investigación se utilizará la prueba Shapiro Wilk, la cual, es utilizada cuando la cantidad total de la muestra es menor a 50, ya que en esta investigación se utilizó 20, se puede aplicar correctamente su uso. Esta prueba se utilizará para los dos indicadores de la variable dependiente: Tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS) y Tasa de verdaderos positivos (TPR) de generación de alertas en los mensajes de texto SMS recibidos.

Para el análisis se utilizó el Software SPSS, se consideró lo siguiente:

a) nivel confiabilidad: 95%

b) Significancia:

- Si la significancia (Sig) < 0.05 es una distribución no normal.
- Si la significancia (Sig) >= 0.05 es una distribución normal.

Indicador 1: Tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS)

Figura 19

Prueba de normalidad – Indicador de detección Phishing

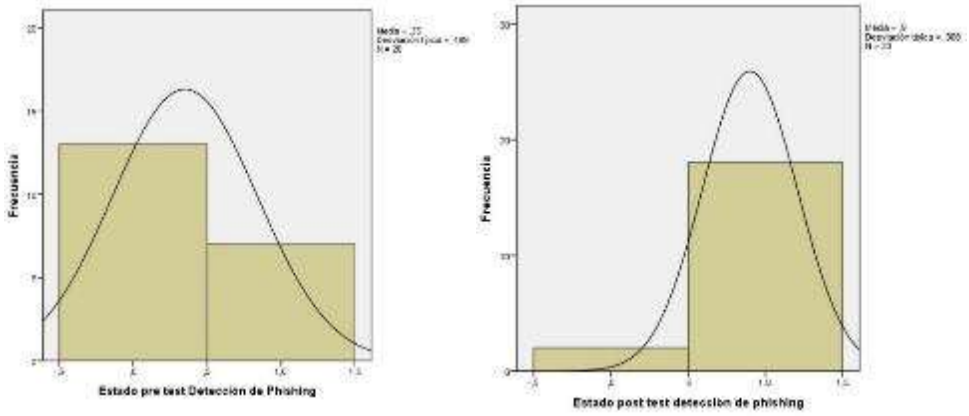
Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Estado pre test Detección de Phishing	,413	20	,000	,608	20	,000
Estado post test detección de phishing	,527	20	,000	,351	20	,000

En esta prueba de normalidad, se tomará solo la prueba de Shapiro-Wilk por contar con una muestra menor a 50. En este cuadro, indica que el nivel de significancia para el estado de pre test Detección de phishing y post test detección de phishing, resulta menor a 0.05, por lo tanto, se concluye que es una distribución no normal.

Figura 20

Comparación de frecuencia pre test y post test de detección de phishing.



Indicador 2: Tasa de verdaderos positivos (TPR) de generación de alertas en los mensajes de texto SMS recibidos

Figura 21

Prueba de normalidad – Indicador de generación de alerta

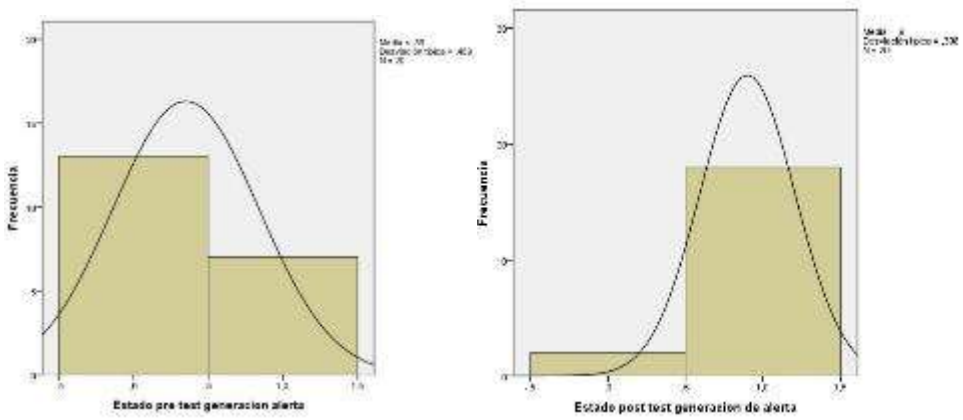
Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Estado pre test generacion alerta	,413	20	,000	,608	20	,000
Estado post test generacion de alerta	,527	20	,000	,351	20	,000

En esta prueba de normalidad, también sólo se tomará la prueba de Shapiro-Wilk por contar con una muestra menor a 50. En este cuadro, indica que el nivel de significancia para el estado de pre test generación de alerta y post test generación de alerta, resulta menor a 0.05, por lo tanto, se concluye que también es una distribución no normal.

Figura 22

Comparación de frecuencia pre test y post test de la generación de alertas.



3.3 Prueba de hipótesis

Luego de recolectar las evidencias y realizar los respectivos análisis, es necesario realizar la respectiva prueba de hipótesis para aceptar o rechazar las mismas.

Criterio de decisión:

p>= 0.05, se acepta la HE2 Nula y se rechaza la HE alternativa.

P< 0.05, se acepta la HE2 alternativa y se rechaza la HE nula.

Prueba: Wilcoxson

- **Hipótesis específica 2 = HE2**

Hipótesis específica 2 (HE2): El desarrollo de un aplicativo móvil permitirá el aumento de la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

Indicador 1: Tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS).

TPRPRD (pre test) = Tasa de verdaderos positivos en detección de phishing antes de utilizar el aplicativo móvil propuesto.

TPRPOD (post test) = Tasa de verdaderos positivos en detección de phishing después de utilizar el aplicativo móvil propuesto.

Hipótesis estadística 2

HE2 nula: El desarrollo de un aplicativo móvil no permitirá el aumento de la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

HE2 nula = TPRPOD <= TPRPRD

HE2 alterna: El desarrollo de un aplicativo móvil permitirá el aumento de la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

HE2 alterna = TPRPOD > TPRPRD

Se puede constatar a través del análisis el claro aumento de la Tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto SMS al comparar el 35% de TPR del pre test con el 90% de TPR resultante del post test.

Según el análisis realizado con el Software SPSS, se observa que la muestra sigue el comportamiento de una distribución no normal, por lo tanto, es necesaria realizar una prueba no paramétrica: Wilcoxon, la cual se detalla en las siguientes figuras.

Figura 23

Test de Wilcoxon para variables detección de phishing

Estadísticos de contraste[a]

	Estado post test detección de phishing - Estado pre test Detección de Phishing
Z	-3,317[b]
Sig. asintót. (bilateral)	,001

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

Figura 24

Resultado de Test de Wilcoxon – Detección de phishing

Resumen de prueba de hipótesis

	Hipótesis nula	Test	Sig.	Decisión
1	La mediana de las diferencias entre Estado pre test Detección de Phishing y Estado post test detección de phishing es igual a 0.	Prueba de Wilcoxon de los rangos con signo de muestras relacionadas	,001	Rechazar la hipótesis nula.

Según el test de wilcoxon, la significancia asintótica bilateral es 0.001. Este valor es menor al 0.005 lo cual se rechaza la hipótesis específica nula 2 quedando válida la hipótesis específica alternativa 2. Es decir, El desarrollo del aplicativo móvil propuesto permitirá el aumento de la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

- **Hipótesis específica 3 = HE3**

  Hipótesis específica 3 (HE3): El desarrollo de un aplicativo móvil permitirá la generación de alertas de Phishing en cada mensaje de texto (SMS) recibido de dispositivos con sistema operativo Android.

  Indicador 2: Tasa de verdaderos positivos (TPR) de generación de alertas en los mensajes de texto SMS recibidos.

  TPRPRA (pre test) = Tasa de verdaderos positivos en generación de alertas antes de utilizar el aplicativo móvil propuesto.

  TPRPOA (post test) = Tasa de verdaderos positivos en generación de alertas después de utilizar el aplicativo móvil propuesto.

  Hipótesis estadística 3

HE3 nula: El desarrollo de un aplicativo móvil no permitirá la generación de alertas de Phishing en cada mensaje de texto (SMS) recibido de dispositivos con sistema operativo Android.

HE3 nula = TPRPOA <= TPRPRA

HE3 alterna: El desarrollo de un aplicativo móvil permitirá la generación de alertas de Phishing en cada mensaje de texto (SMS) recibido de dispositivos con sistema operativo Android.

HE3 alterna = TPRPOA > TPRPRA

Se puede constatar a través del análisis el claro aumento de la Tasa de verdaderos positivos (TPR) de generación de alertas en mensajes de texto SMS al comparar el 35% de TPR del pre test con el 90% de TPR resultante del post test.

Según el análisis realizado con el Software SPSS, se observa que la muestra sigue el comportamiento de una distribución no normal, por lo tanto, es necesaria realizar una prueba de Wilcoxon, la cual se detalla en las siguientes figuras.

Figura 25

Test de Wilcoxon para variables de generación de alerta

Estadísticos de contraste[a]

	Estado post test generacion de alerta - Estado pre test generacion alerta
Z	-3,317[b]
Sig. asintót. (bilateral)	,001

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

Figura 26

Resultado de Test de Wilcoxon – Generación de alertas

Resumen de prueba de hipótesis

	Hipótesis nula	Test	Sig.	Decisión
1	La mediana de las diferencias entre Estado pre test Detección de Phishing y Estado post test detección de phishing es igual a 0.	Prueba de Wilcoxon de los rangos con signo de muestras relacionadas	,001	Rechazar la hipótesis nula.

Según el test de wilcoxon, la significancia asintótica bilateral es 0.001. Este valor es menor al 0.005 lo cual se rechaza la hipótesis específica nula 3 quedando válida la hipótesis específica alternativa 3. Es decir, el desarrollo del aplicativo móvil propuesto permitirá la generación de alertas de Phishing en cada mensaje de texto (SMS) recibido de dispositivos con sistema operativo Android.

CAPÍTULO IV: DISCUSIÓN Y CONCLUSIONES

4.1. Discusión

En el aplicativo móvil desarrollado para cumplir con los objetivos de la investigación, es una aplicación desarrollada para el sistema operativo Android. Existen otras investigaciones que trataron el tema antimalware, pero con sus respectivas particularidades, las cuales fueron referenciadas en esta investigación:

a) **"Detección automática de sitios web fraudulentos" (Coronado, et al.,2020).**

   Coincidencias:

   -Utiliza como parte de su sistema de detección una lista negra de URL, también utiliza el repositorio Phishtank para su entrenamiento y posterior detección.

   -Lee y extrae características de la URL en el proceso de detección.

   -Utiliza base de datos local

   -Detecta ataques de día cero.

   Diferencias:

   -Utiliza lenguaje de programación Python, Framework Flask y algoritmos de aprendizaje automático.

   -Cuenta con mayor cantidad de muestras, por el hecho de realizar un entrenamiento de inteligencia artificial previo a las pruebas de detección.

   -Es una aplicación web no un aplicativo móvil dedicado para un sistema operativo en específico.

b) **"Detectando aplicaciones maliciosas en Smartphone con sistema Android a través del uso de una aplicación" (Mejía, 2019)**

   Coincidencias:

   -Se realizó para el sistema operativo Android.

-Utilizó el IDE Android Studio.

-Genera alertas de detección de malware.

-Proceso de detección en tiempo real.

Diferencias:

- Detecta aplicaciones maliciosas no enlaces URL o contenido sospechoso.
- Se utilizó equipos de prueba, pero con sistema operativo Android v4 o superior.
- Se utilizó API

Asimismo, según la metodología de desarrollo del aplicativo y en comparación con las entrevistas y buenas prácticas, se podría citar algunas investigaciones con respecto a este tema:

c) "Metodología de selección de IDE para el desarrollo de aplicaciones Android" (Moreyra & Pusdá, 2018)

Coincidencias:

- Recomienda saber desde un inicio, el lenguaje de programación, IDE y tipo de aplicación.
- Utiliza una entrevista a expertos para fortalecer la selección de IDE a trabajar.
- Utiliza norma de calidad de software, en este caso fue la ISO/IES 9126, la cual antecede al conjunto de normas ISO 25000.

Diferencias:

-Según sus entrevistas, consideran más popular el ID Eclipse en cuanto Al desarrollo de aplicaciones móviles. El IDE Android Studio, el cual se utilizó en esta investigación quedó como segundo más recomendado.

d) Comparativa de tendencias de desarrollo de software móvil. (Cárdenas et al., 2021).

Coincidencias:

- La inteligencia artificial aún es poco viable para su uso comercial, debido al alto consumo de hardware y poca integración.
- Las aplicaciones basadas en la nube son las más populares.

Se debe aclarar que el aplicativo móvil propuesto fue desarrollado por el investigador y es la primera versión para su posterior mejora o integración con otros sistemas antimalware. El aplicativo fue desarrollado con la intención de ser práctico, económico y escalable.

4.1.1 Implicancias

-El aplicativo es fácil de usar y es automático. El aplicativo trabaja en segundo plano, el usuario sólo deberá instalarlo y registrarse, posterior a ello, el aplicativo se encargará de detectar, alertar y recomendar para que el usuario realice la opción que más convenga.

-El aplicativo tiene una base de datos sencilla y escalable, puede implementarse una mayor cantidad de registros de malware en la lista negra u otras bases de datos que aporten en la eficiente detección de phishing.

-La base de datos es relacional, pero se recomienda una no relacional a medida que la cantidad de registros a leer (lista negra de phishing) aumente con la escalabilidad posible del aplicativo móvil.

-El aplicativo consume pocos recursos de hardware como la batería, espacio de disco y procesador.

-El aplicativo cuenta con poco código, es estructurado, flexible y escalable para las futuras mejoras e integraciones.

4.1.2 Limitaciones

-Con respecto a las buenas prácticas del ISO 25000, hay dimensiones que deben aún tener en cuenta como la madurez y capacidad a fallos, los cuales, tienen mayor importancia en el tiempo

de uso, a través de futuras versiones o integraciones con otras propuestas relacionadas a la detección de Phishing.

-Debido a lo práctico del aplicativo móvil propuesto, se ha obviado la seguridad del mismo, lo cual debe tenerse en cuenta en futuras versiones.

-El aplicativo móvil cuenta con una base de datos local, lo cual, debería variar en caso se implemente masivamente, lo más adecuado es implementarlo en la nube.

-El aplicativo necesita de conexión a la base de datos para funcionar.

-El aplicativo cuenta con una base de datos relacional, aunque no implementada en su totalidad, solo cuenta con las tablas para el registro de usuarios y el repositorio de malwares.

4.2 Conclusiones

Luego de la discusión se desprende algunas conclusiones finales para la presente investigación.

a) Los requerimientos propuestos para el aplicativo móvil, fueron cumplidos en su totalidad. El modelo incremental ayudó en la organización y orden para el desarrollo del aplicativo y con ello, el cumplimiento del objetivo específico 1 (OE1) propuesto.
b) Hubo una mejora de un 55% en el indicador de tasa de verdaderos positivos en la detección de phishing en mensajes de texto (SMS), cumpliendo con el segudno objetivo específico (OE2) de la investigación.
c) El aplicativo móvil propuesto genera alertas en tiempo real, dentro y fuera del aplicativo, lo cual, cumple con el segundo objetivo específico (OE3) de la investigación.

d) Se acepta la hipótesis general, el desarrollo de un aplicativo móvil sí mejora el proceso de detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.

REFERENCIAS

Almada, S. (2019). U*tilización de los métodos de validación y confiabilidad de los instrumentos de recolección de datos en los trabajos de tesis de postgrado*. Universidad Tecnológica Intercontinental UTIC San Lorenzo. Repositorio utic.edu.py

Altamirano, J., & Bayona S. (2017). *Políticas de seguridad de la información: Revisión sistemática de las teorías que explican su cumplimiento*. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, 25, 112–134. https://doi.org/10.17013

Avast. (2021). *Historia de Phishing: la creciente amenaza para las empresas*. Avast. https://blog.avast.com/es/phishing-and-its-growing-threat-to-your-business-avast

Banco Mundial. (2020). *Suscripciones a telefonía celular móvil | Data*. Banco Mundial BIRF -AIF. https://datos.bancomundial.org/indicator/IT.CEL.SETS?end=2020&start=1960&view=chart

Barquero, M. (2016). *Las apps como nuevo soporte de interacción entre la entidad universitaria y sus stakeholders*. 32(11) 15-34. http://www.redalyc.org/articulo.oa?id=31048902002

Bendezú, L., & Chahuara, P. (2012). *Caracterización de la Demanda de Telefonía Fija y Móvil en el Perú. Un Análisis Descriptivo al 2012*. OSIPTEL. https://repositorio.osiptel.gob.pe/bitstream/handle/20.500.12630/329/ Caracterización_Demanda_de_Telefonía-w.pdf (osiptel.gob.pe)

Cárdenas, O., Zea, M., Valarezo, M., y Ramón, R. (2021). *Comparativa de tendencias de desarrollo de software móvil*. 3C TIC. Cuadernos de desarrollo aplicados a las TIC, 9(4), 123-147. https://doi. org/10.17993/3ctic.2021.101.123-147

Castañeda, R. (2013). *Propuesta de diseño de sistema anti-spam para SMS aplicado a Movistar Perú.* Universidad Nacional de Trujillo. Repositorio institucional - UNITRU

Coronado, H., Han, A. & Sanz, L. (2020). *Detección automática de sitios web fraudulentos.* Universidad Complutense de Madrid. Repositorio institucional de la UCM

Demertzis, K., & Iliadis, L. (2017). *Computational intelligence anti-malware framework for android OS*. Vietnam Journal of Computer Science, 4(4), 245–259. https://doi.org/10.1007/s40595-017-0095-3

EFE News Services, Inc. (2019). *Crece la suplantación de identidad online y baja el "ransomware": CIBERSEGURIDAD CRÍMENES.* EFE: Agencia EFE. https://www.efe.com/efe/america/tecnologia/crece-la-suplantacion-de-identidad-online-y-baja-el-ransomware/20000036-3997885

Firdaus, A., Anuar, N. B., Razak, M. F. A., & Sangaiah, A. K. (2018). Bio-inspired computational paradigm for feature investigation and malware detection: interactive analytics. *Multimedia Tools and Applications*, *77*(14), 17519–17555. https://doi.org/10.1007/s11042-017-4586-0.

FORTINET (2021). *América Latina sufrió más de 289 mil millones de intentos de ciberataques en 2021*. FORTINET. https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-reporte-ciberataques-america-latina-2021

Gómez, J. (2009). *Optimización de sistemas de detección de intrusos en red utilizando técnicas computacionales avanzadas*. Universidad Almería.

Hernandez, A. & Baluja, W. (2021). *Principales mecanismos para el enfrentamiento al Phishing en las redes de datos*. Ediciones Futuro. IV Conferencia Científica Internacional UCIENCIA2021. Universidad de las ciencias Informaticas (UCI). https://www.redalyc.org/journal/3783/378370462024/html/

Hilt, J. A.(julio de 2019). *Dependencia del celular, hábitos y actitudes hacia la lectura y su relación con el rendimiento académico*.Revista de investigación apuntes universitarios. 9(3). 103-117. https://doid.org/10.17162/au.v9i3.384

ISO25000 (2022). *ISO 25000 Calidad de Software y datos*. ISO 25000. https://iso25000.com/index.php/normas-iso-25000/iso-25010

Jancachagua, J. (2021). *Mejoramiento de la seguridad de la información para reducir los ciberataques del tipo Phishing en una entidad financiera*. Universidad Tecnológica del Perú. Repositorio institucional de la UTP.

Jang, J. wook, Yun, J., Mohaisen, A., Woo, J., & Kim, H. K. (2016). *Detecting and classifying method based on similarity matching of Android malware behavior with profile*. *SpringerPlus*, *5*(1). 1-23. https://doi.org/10.1186/s40064-016-1861-x

Kjaer, A. L. (2014, May 1). *Five ways mobile tech will shake up your financial future.* CNN BUSINESS. Retrieved from CNN: http://edition.cnn.com/2014/02/26/business/five-ways-mobile-tech-will-shake-up-your-financial-future/

Marulanda López, J. (2014). *Aseguramiento de la calidad en el diseño del software*. Universidad EAFIT. Repository.eafit.edu.co

Mejía, J. (2019). *Detectando aplicaciones maliciosas en Smartphone con sistema Android a través del uso de una aplicación*. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *31*, 82–93. https://doi.org/10.17013/risti.31.82-93

Miró Llinares, F. (2013). L*a respuesta penal al ciberfraude*. ´Revista electrónica de Ciencia, Penal y Criminología. 15(12), 1-56. http://criminet.ugr.es/recpc15-12.pdf

Moreyra, M., & Pusdá, E. (2018). *Metodología de selección de IDE para el desarrollo de aplicaciones Android*. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*. E15, 214-220. https://www.proquest.com/scholarly-journals/metodología-de-selección-ide-para-el-desarrollo/docview/2041144079/se-2?accountid=36937

Navarro Hudiel, S. (2018). *Estadísticas*. https://sjnavarro.files.wordpress.com/2018/05/documento-final-estadc3adsticas.pdf

News Center Microsoft Latinoamérica (2021). *Marsh y Microsoft: ingeniería social o phishing es el ciberataque que más aumentó en Latinoamérica a raíz de la pandemia*. Microsoft.

https://news.microsoft.com/es-xl/marsh-y-microsoft-ingenieria-social-o-phishing-es-el-ciberataque-que-mas-aumento-en-latinoamerica-a-raiz-de-la-pandemia/

Nissim, N., Moskovitch, R., BarAd, O., Rokach, L., & Elovici, Y. (2016). *ALDROID: efficient update of Android anti-virus software using designated active learning methods*. Knowledge and Information Systems, 49(3), 795–833. https://doi.org/10.1007/s10115-016-0918-z

Ortega, S., Raygoza, J., Sandoval F., Pedroza, A. & Carrazco, M. (2012). *Ambiente de pruebas para verificación y cobertura funcional con metodología UVM.* Jornadas Arteco – Universidad de Alicante. http://www.jornadassarteco.org/js2012/papers/paper_51.pdf

Oxman, N. (2013). *Estafas informáticas a través de internet: acerca de la imputación penal del "phishing" y el "pharming*". Revista Derecho, XLI 2do Semestre. 211-262. https://www.proquest.com/scholarly-journals/estafas-informáticas-través-de-internet-acerca-la/docview/1509070562/se-2?accountid=36937

Parra Velasco, L. Y., & Vázquez Martínez, M. G. (2017). *Muestreo probabilístico y no probabilístico.* https://www.gestiopolis.com/wp-content/uploads/2017/02/muestreo-probabilistico-no-probabilistico-guadalupe.pdf

Roa, J. (2013). *Seguridad informática.* McGraw-Hill/Interamericana de España, S. L.

Rumbaugh, J., Jacobson, I., & Booch, G. (2006). *El lenguaje Unificado de Modelado Manual de referencia*. Pearson Addison-Wesley.

Serna, S. & Pardo, C. (2017). *Diseño de interfaces en aplicaciones móviles.* Grupo Editorial RA-MA. https://books.google.com.pe/books?id=SI-fDwAAQBAJ&dq=Dise%C3%B1o+de+interfaces+en+aplicaciones+m%C3%B3viles&hl=es&source=gbs_navlinks_s

Sommerville, I. (2005). *Ingeniería del Software*. Ed. 7. Pearson Educacion S.A.

Ventura – León (2017). *La importancia de reportar la validez y confiabilidad en los instrumentos de medición: Comentarios a Arancibia et al.* http://dx.doi.org/10.4067/s0034-98872017000700955.

Wang, X., Yang, Y., & Zeng, Y. (2015). *Accurate mobile malware detection and classification in the cloud*. SpringerPlus, *4*(1), 1–24. https://doi.org/10.1186/s40064-015-1356-1

Wibowo, K., & Ali, A. (2016). *Mobile Security: Suggested Security Practices for Malware Threats.* Competition Forum, *14*(1), 119-126. https://www.proquest.com/docview/1837562677?pq-origsite=gscholar&fromopenview=true

Wirth, A. (2017). *Responding to Ever-Evolving Threats*. Biomedical Instrumentation & Technology May/*June 2017*, 269–274. https://www.proquest.com/docview/1903824032?pq-origsite=gscholar&fromopenview=true

APÉNDICES

Apéndice A. Matriz de consistencia.

MATRIZ DE CONSISTENCIA						
Problemática	**Objetivos**	**Hipótesis**	**Variables**	**Indicadores**	**Instrumentos**	**Tecnicas**
General	General	General	Variable independiente: Aplicativo móvil	Cobertura funcional: Cumplimiento de requerimientos	Guia de entrevista	Entrevista
¿Cómo desarrollar un aplicativo móvil que mejore la detección de Phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android?	Desarrollar un aplicativo móvil que mejore la detección de Phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.	El desarrollo de un aplicativo móvil permitirá mejorar la detección de Phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.				
Especificos	**Especificos**	**Especificos**		Test de validación	Ficha de registro.	Observación
1. ¿Cómo desarrollar los requerimientos de un aplicativo móvil que mejore la detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android?	1. Desarrollar los requerimientos de un aplicativo móvil que mejore la detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.	1.El desarrollo de los requerimientos de un aplicativo móvil permitirá que mejore la detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.		Test de validación	Ficha de registro.	Observación
2. ¿Cómo desarrollar un aplicativo móvil que mejore la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android?	2. Desarrollar un aplicativo móvil que permita la mejora en la tasa de verdaderos positivos (TPR) en la detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.	2. El desarrollo de un aplicativo móvil permitirá el aumento de la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS) de dispositivos con sistema operativo Android.	Variable dependiente: Detección de Phishing	Tasa de verdaderos positivos (TPR) de detección de phishing de una muestra de 20 mensajes SMS.	Ficha de registro.	Observación
3. ¿Cómo desarrollar un aplicativo móvil que genere alertas de Phishing en cada mensaje de texto (SMS) recibido en dispositivos con sistema operativo Android?	3. Desarrollar un aplicativo móvil que permita la generación de alertas de Phishing en cada mensaje de texto (SMS) recibido en dispositivos con sistema operativo Android.	3.El desarrollo de un aplicativo móvil permitirá la generación de alertas de Phishing en cada mensaje de texto (SMS) recibido en dispositivos con sistema operativo Android.		Tasa de verdaderos positivos (TPR) de generación de alertas en los mensajes de texto SMS recibidos.	Ficha de registro.	Observación

Apéndice B. Entorno de desarrollo y lenguaje utilizado.

Figura B1

Android Studio versión 4.1.1

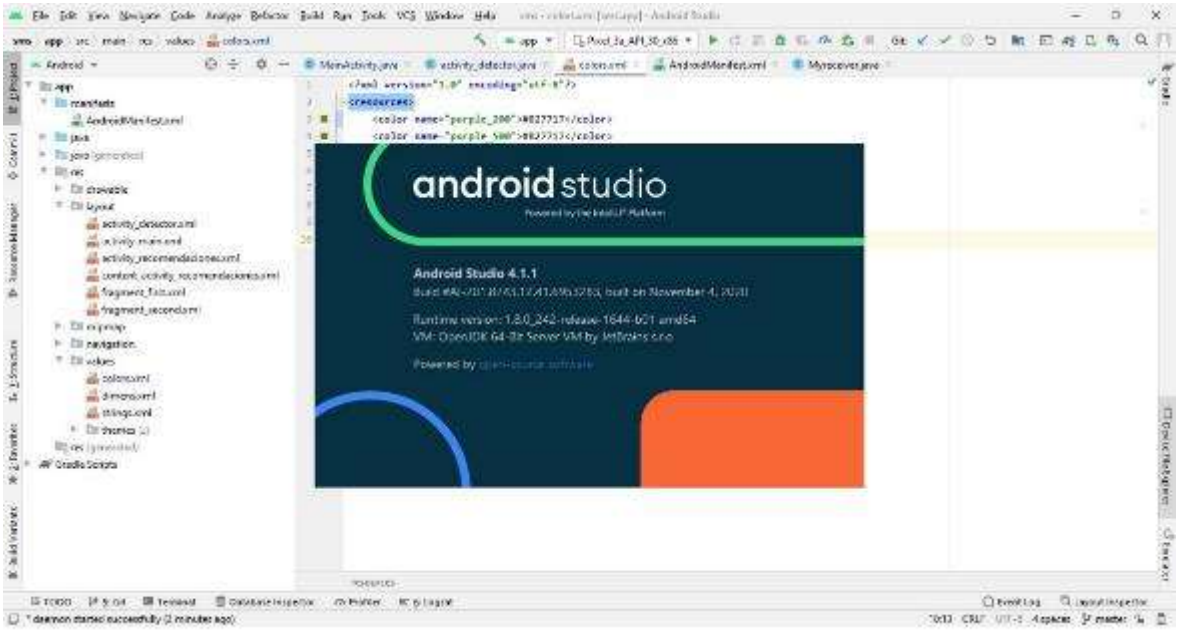
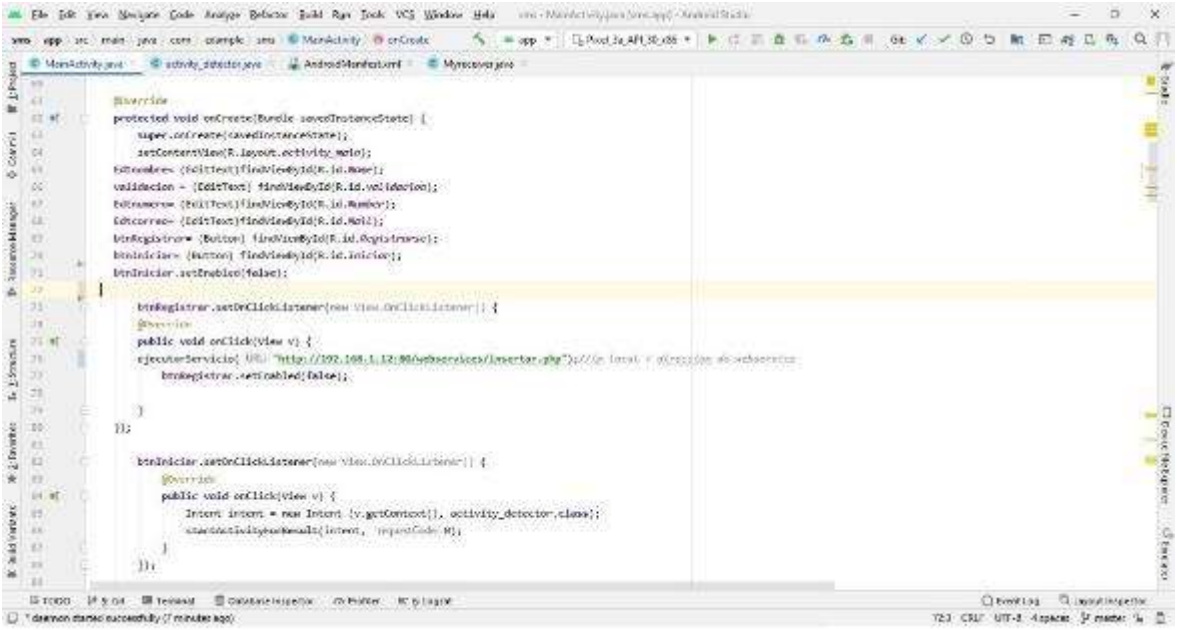
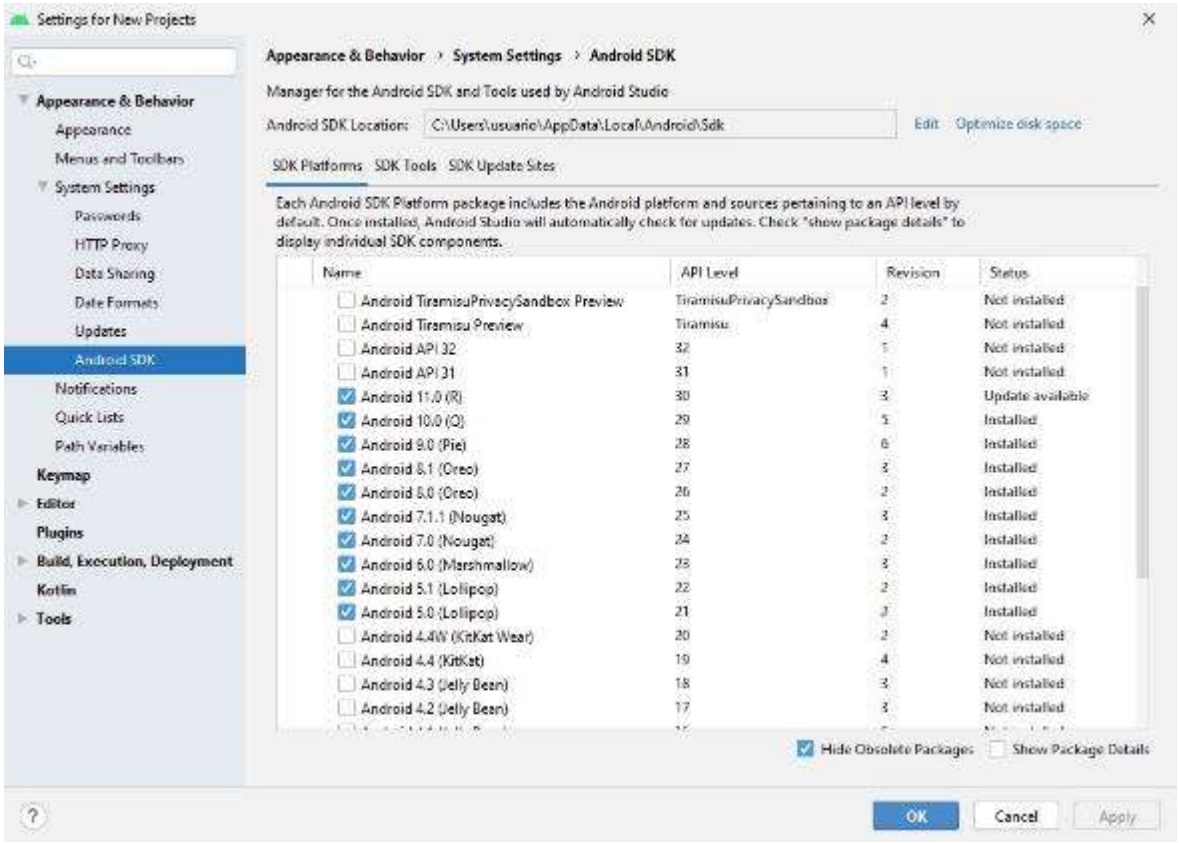


Figura B2

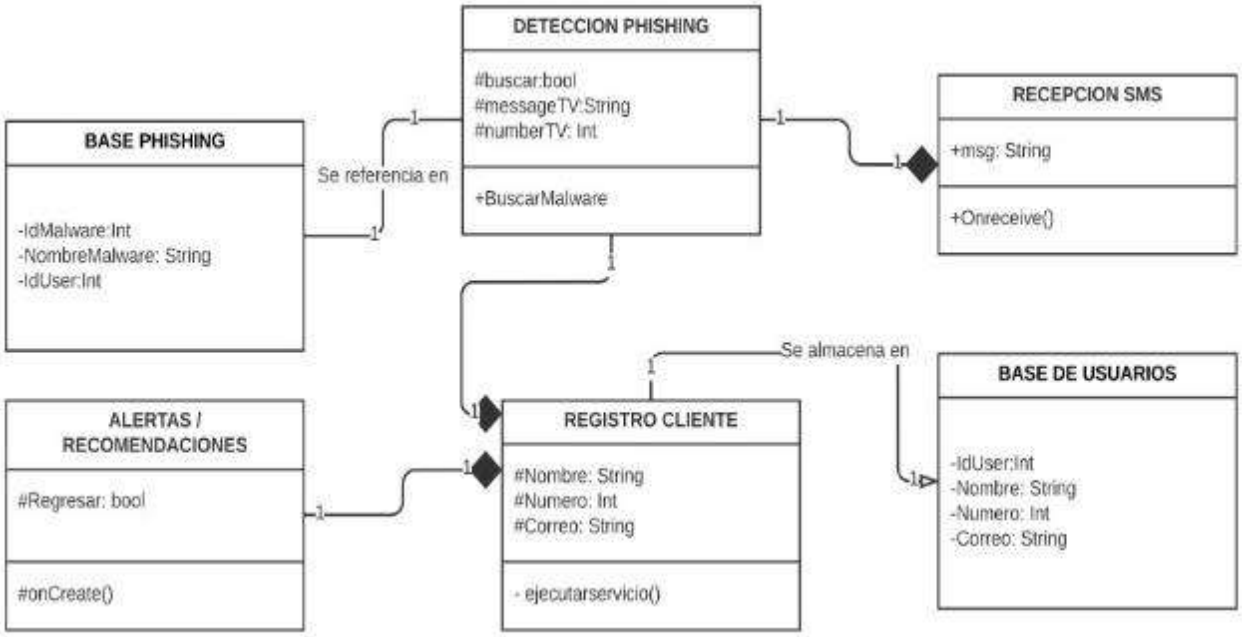
Lenguaje Java, fragmento del Activity principal



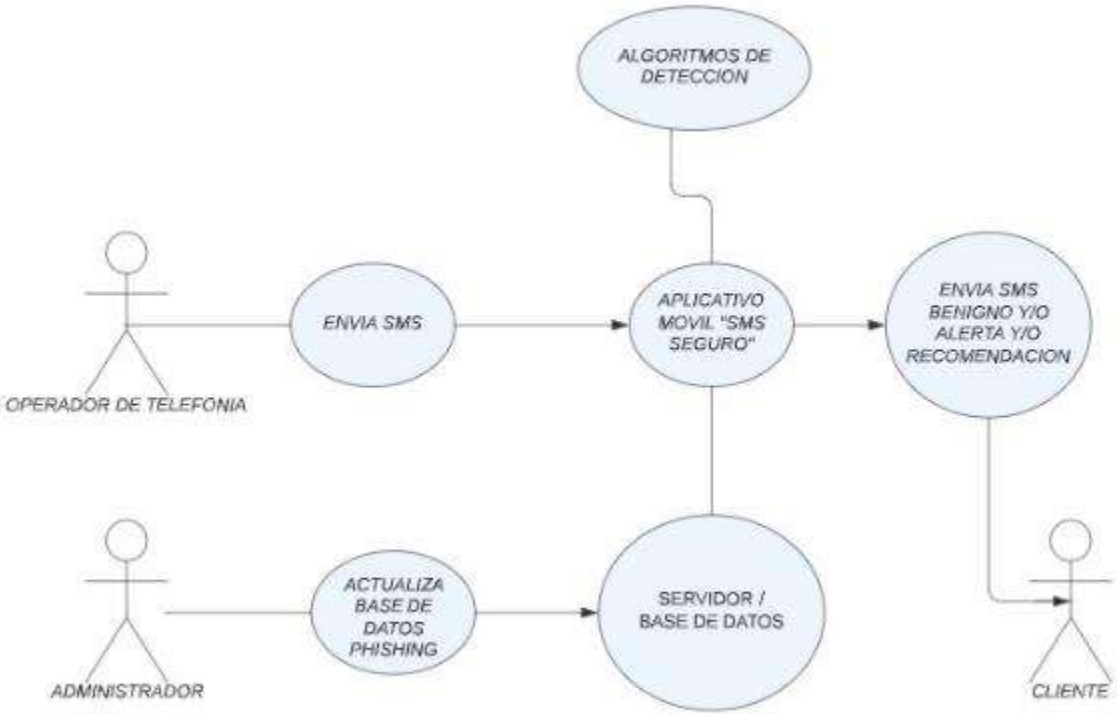
Apéndice C. Descarga e instalación de Android 5.0 en Android studio.



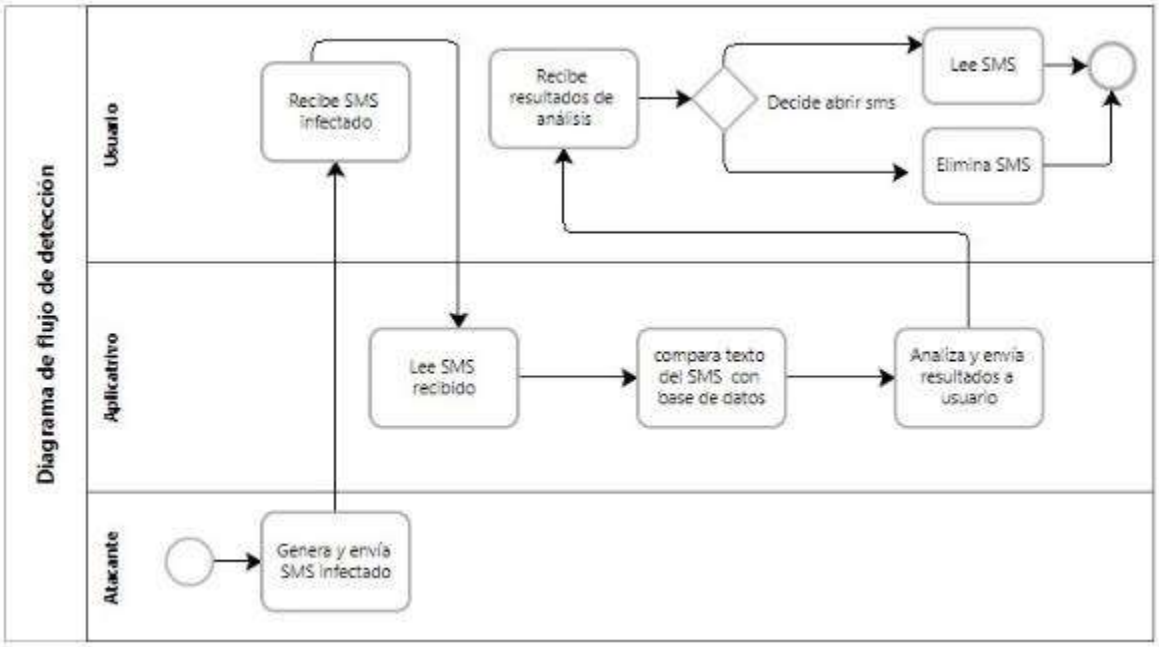
Apéndice D. Diagrama de clases.



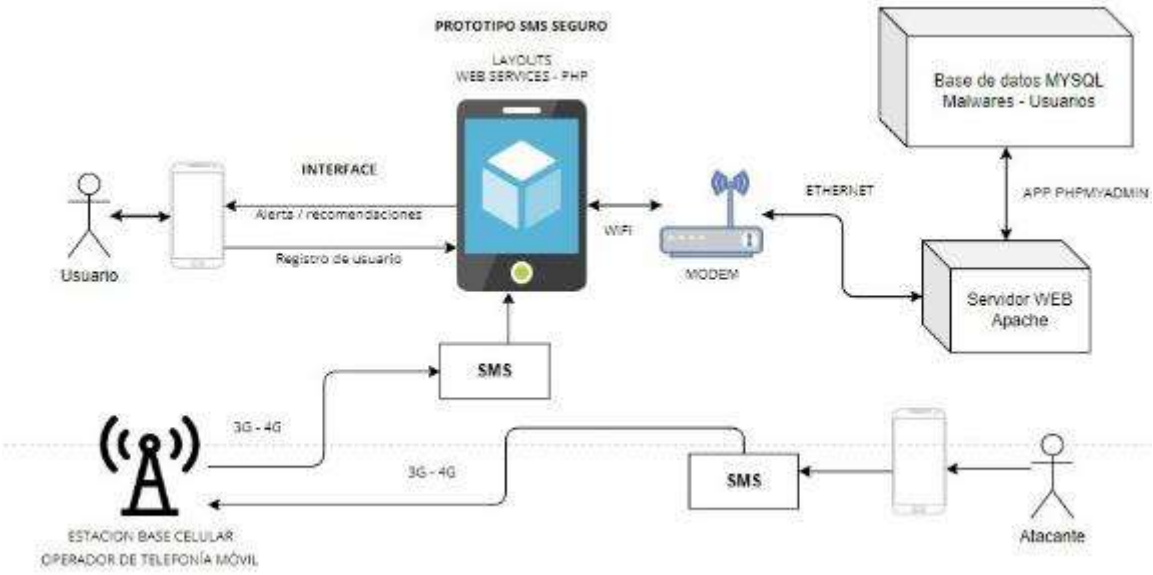
Apéndice E. Diagrama de casos de uso.



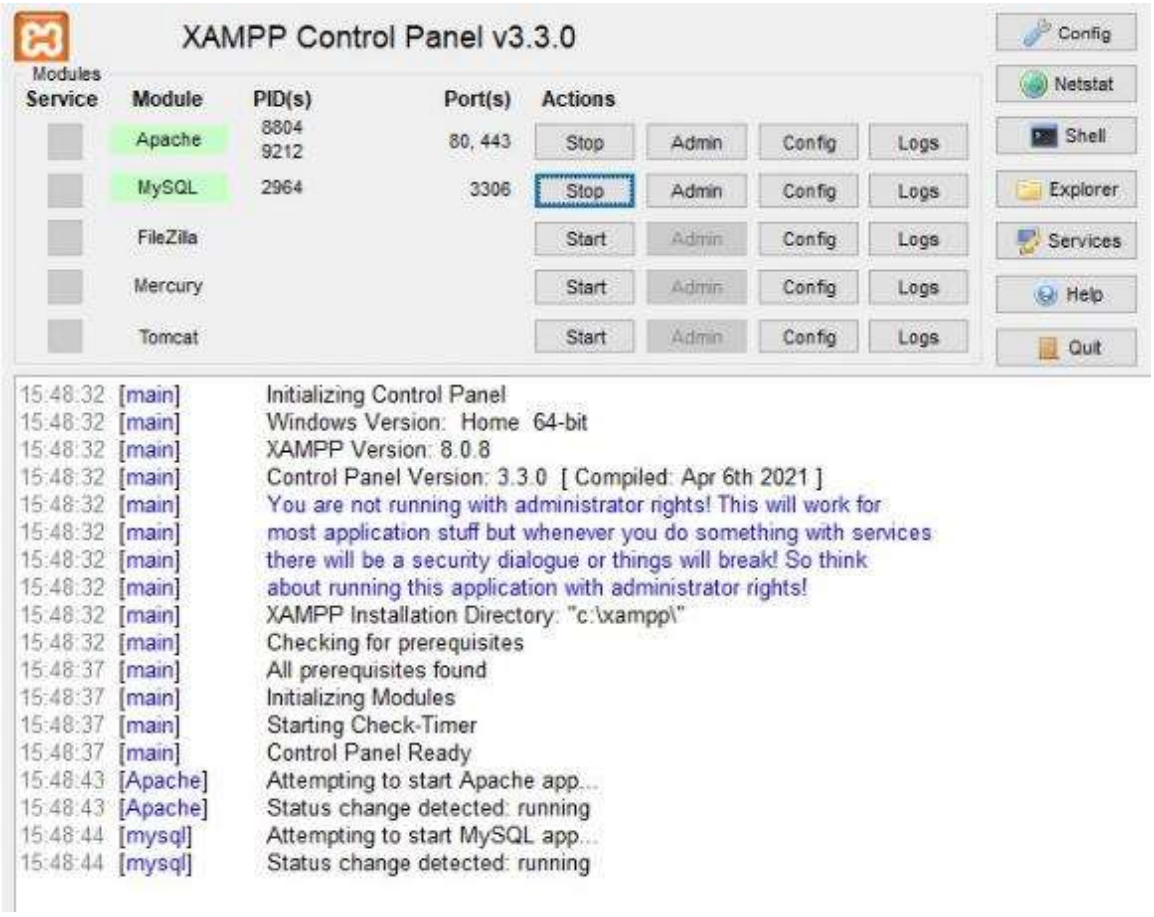
Apéndice F. Diagrama de flujo de detección de phishing y generación de alertas.



Apéndice G. Diagrama de despliegue.



Apéndice H. Configuración de servidor web.



Apéndice I. Web services del primer incremento.

Figura I1

Web service - Conexión

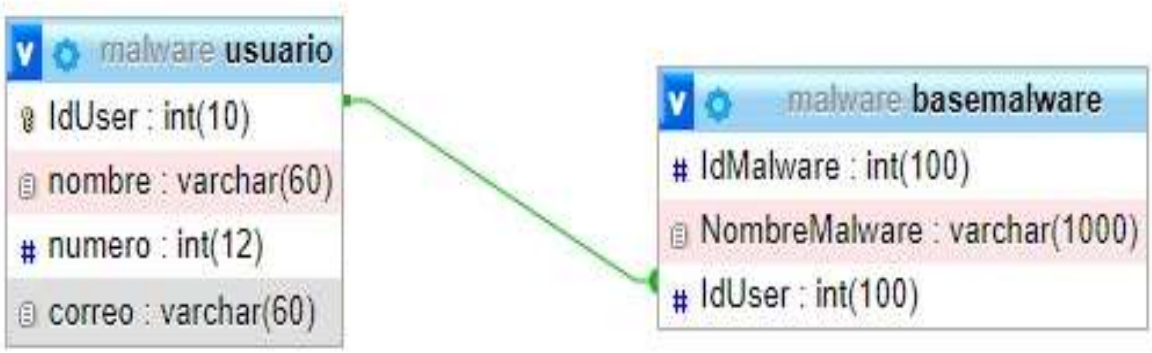
```php
<?php

$hostname='localhost';
$database='malware';
$username='root';
$password='';

$conexion= new mysqli($hostname,$username,$password,$database);
if($conexion -> connect_errno){
    echo "SITIO WEB EN MANTENIMIENTO";
}


 ?>

```

Figura I2

Web service – Registro de usuarios

```php
<?php

include 'conexion.php';

$IdUser = $_POST['IdUser'];
$nombre = $_POST['nombre'];
$numero = $_POST['numero'];
$correo = $_POST['correo'];



$consulta= "insert into usuario values('".$IdUser."','".$nombre."','".$numero."','".$correo."')";
mysqli_query($conexion,$consulta) or die (mysqli_error());
mysqli_close($conexion);

 ?>

```

Apéndice J. Diagrama de modelo entidad relación.



Apéndice K. Registros en base de datos.

Figura K1

Registro de malwares

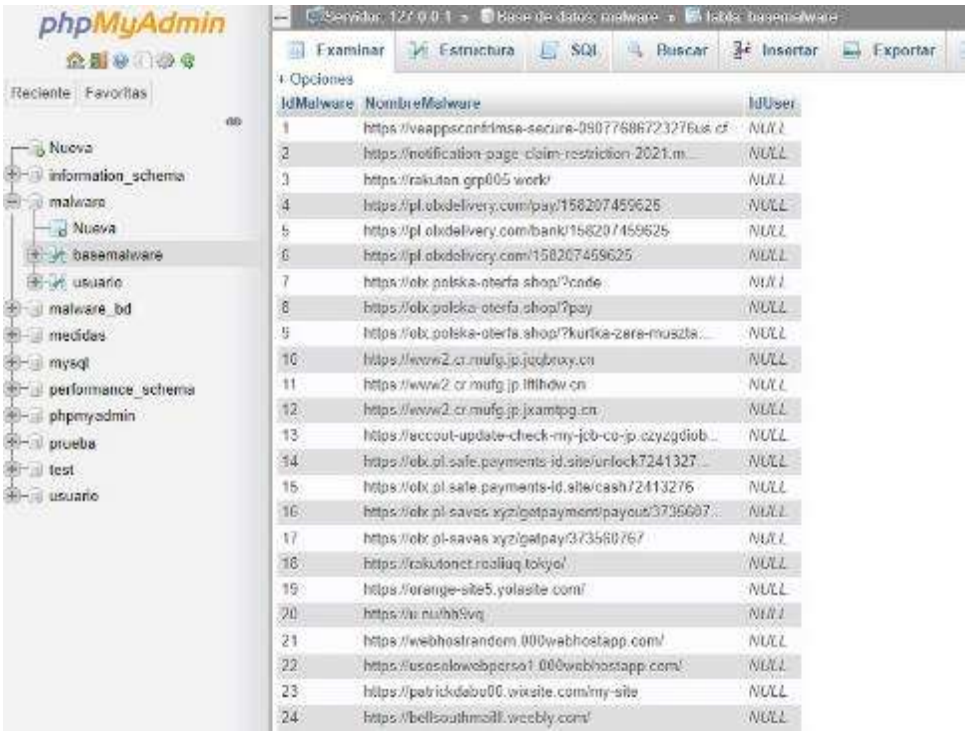
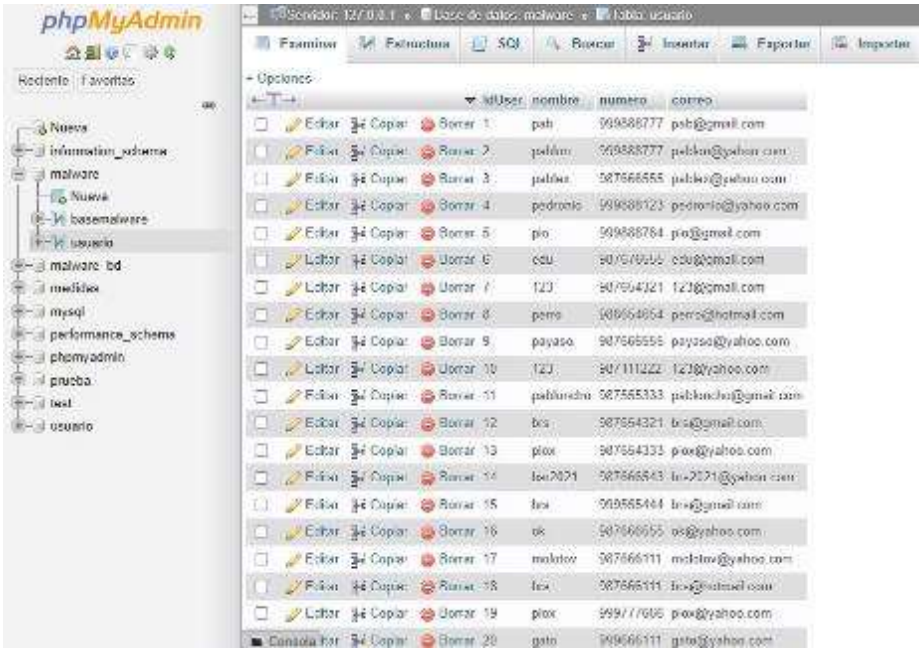


Figura K2

Registro de malwares



Apéndice L: Base de datos referencial Phishtank.

Figura L1

Base de datos de repositorio Phishtank

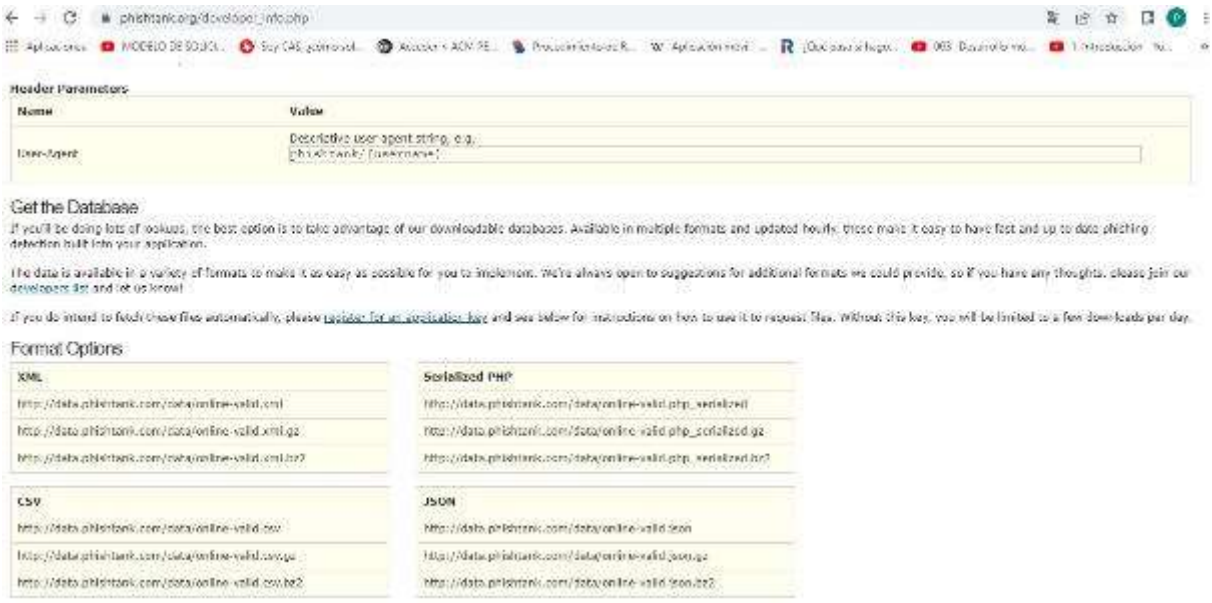
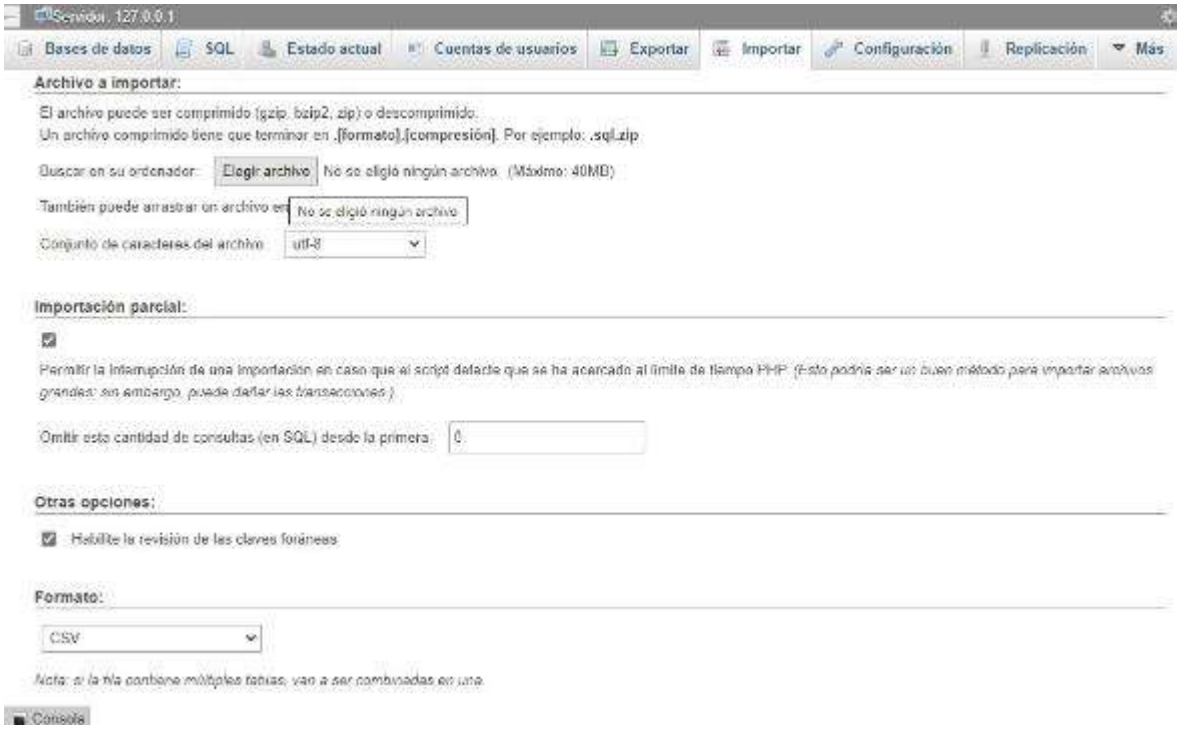


Figura L2

Procedimiento de subida de base de datos en phpMyAdmin.



Apéndice LL. Pantalla inicial: Registro de usuarios.

Apéndice M. Alerta de mala conexión cliente - servidor

Apéndice N. Alerta de registro exitoso.

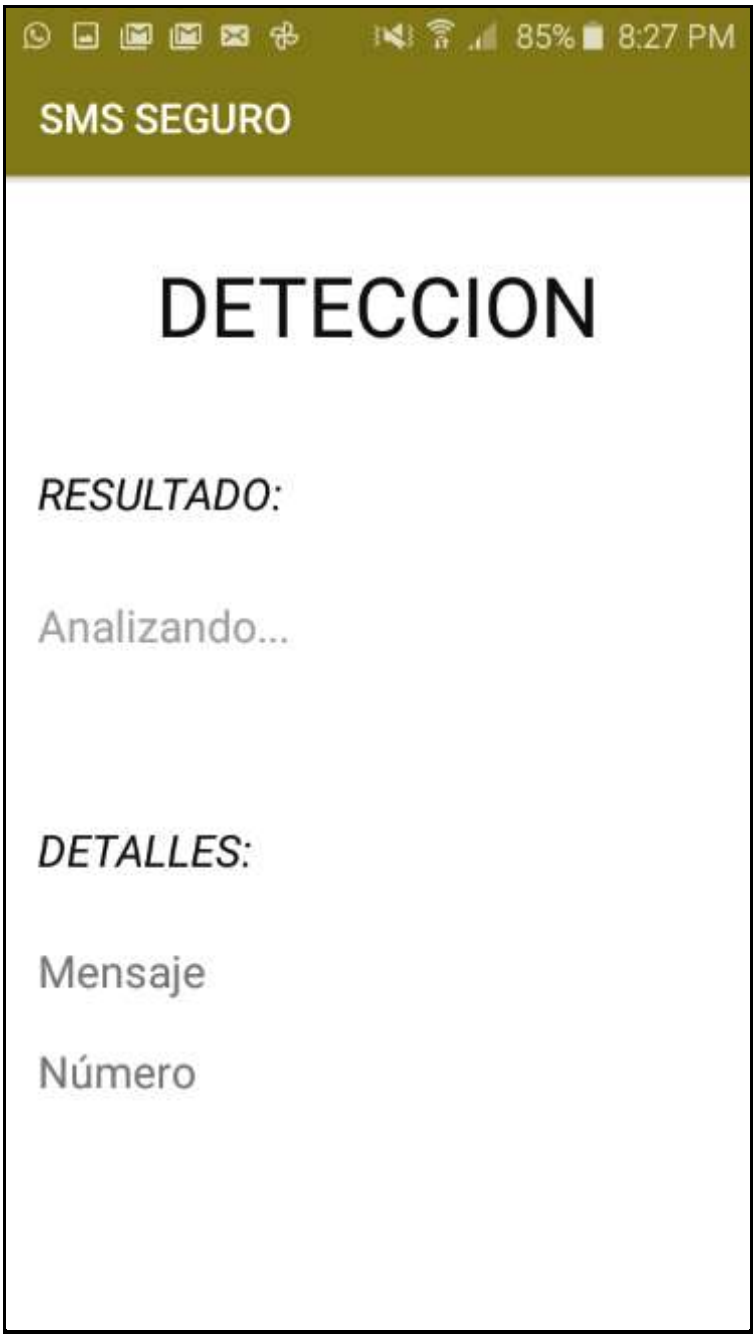
Apéndice Ñ: Algoritmo de detección de mensajes de texto

```
private static final String TAG = "SmsBroadcastReceiver";
String msg, phoneNO="";
@Override
public void onReceive(Context context, Intent intent) {

    Log.i(TAG, msg: "Intent Received: " + intent.getAction());
    if(intent.getAction() == SMS_RECEIVED)
    {
        Bundle dataBundle =intent.getExtras();
        if(dataBundle!=null) {
            //creando PDU (protocol data unit) objeto para el protocolo de transferencia de mensajes
            Object[] mypdu = (Object[]) dataBundle.get("pdus");
            final SmsMessage[] messages = new SmsMessage[mypdu.length];
           // if (messages.toString().startsWith("ok")==true)

            for (int i = 0; i < mypdu.length; i++) {

                if (Build.VERSION.SDK_INT >= Build.VERSION_CODES.M) {
                    String format = dataBundle.getString( key: "format");
                    //desde el PDU se puede obtener todos los objetos y los objetos mensaje siguiendo la linea de código
                    messages[i] = SmsMessage.createFromPdu((byte[]) mypdu[i], format);
                } else {
                  messages[i] = SmsMessage.createFromPdu((byte[]) mypdu[i]);
                }
                msg = messages[i].getMessageBody();
                phoneNO = messages[i].getOriginatingAddress();
            }
          }
    }
}
```

Apéndice O. Algoritmo de detección de phishing.

```
validacion.setText(msg);
buscar.performClick();
while(encontradobase==2 || encontradobase==0) {

    if (msg.indexOf(palabra_objetivo, posicion) >= 0 || msg.indexOf(palabra_objetivo.toLowerCase(), posicion) >= 0 ||
        msg.indexOf(palabra_objetivo.toUpperCase(), posicion) >= 0 ) {
        messageTV.setText("ATAQUE PHISHING, NO ABRIR!");
        numberTv.setText("El numero es: " + phoneNO);
        analizador.setText("El mensaje es: " + msg);
        messageTV.setTextColor(Color.RED);
        Toast.makeText( context: activity_detector.this,  text: "ATAQUE PHISHING, NO ABRIR SMS!", Toast.LENGTH_SHORT).show();
        reco.setVisibility(View.VISIBLE);
        encontradobase = 1;
    } else
    {
        messageTV.setText("El Mensaje es seguro");//.
        numberTv.setText("El numero es: " + phoneNO);
        analizador.setText("El mensaje es: " + msg);
        messageTV.setTextColor(Color.parseColor( colorString: "#689F38"));
        veces_hallada = 0;
        reco.setVisibility(View.GONE);
        encontradobase = 1;
    }
}
```

Apéndice P. Layout de detección de phishing.



Apéndice Q. Ejemplos de detección y no detección de phishing.

Apéndice R. Web service para detección y validación en base.

Figura R1

Web service – Buscar, primera versión

```php
<?php

include 'conexion.php';

$nombre = $_GET['nombre'];

//$NombreMalware = $_GET['NombreMalware'];

$consulta= "select * from usuario where nombre = '$nombre'";
//$consulta= "select * from basemalware where
//NombreMalware = '$NombreMalware'"; //así debe estar para la otra base a buscar.
$resultado = $conexion -> query($consulta);

while($fila=$resultado -> fetch_array()){
    $nombre[] = array_map('utf8_encode', $fila);

}

echo json_encode($nombre);
$resultado -> close();

 ?>
```

Figura R2

Web service – Buscar, segunda versión con validación.

```php
<?php

include 'conexion.php';
//$usuario= $_GET['NombreMalware'];

$usuario = $_GET['NombreMalware'];
$sentencia=$conexion->prepare("SELECT * FROM basemalware WHERE NombreMalware=?");
$sentencia->bind_param('s',$usuario); //este es igual a la variable que contiene el post.
$sentencia->execute();

$resultado = $sentencia->get_result();
if ($fila =$resultado->fetch_assoc()){
    echo json_encode($fila,JSON_UNESCAPED_UNICODE);
    echo "correcto";
}
else{
    echo "No funciona";
}
$sentencia->close();
$conexion->close();

?>
```

Apéndice S. Fichas de registro de detección.

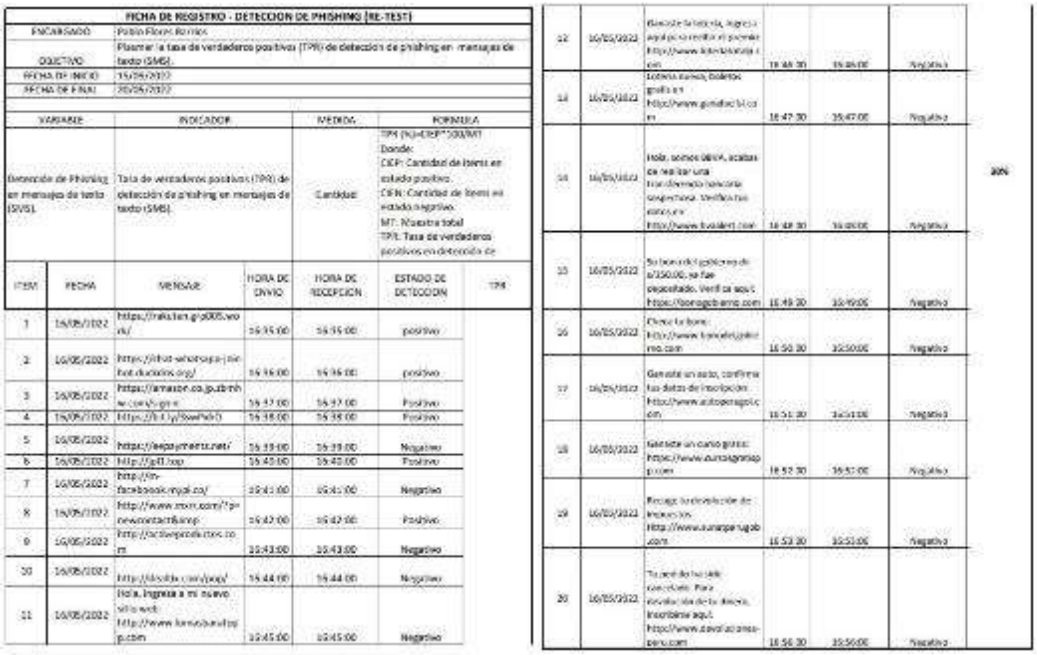
Figura S1

Ficha de registro de detección de Phishing – Pre Test

FICHA DE REGISTRO - DETECCION DE PHISHING (PRE-TEST)						
ENCARGADO	Pablo Flores Barrios					
OBJETIVO	Plasmar la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS)					
FECHA DE INICIO	15/05/2022					
FECHA DE FINAL	20/05/2022					
VARIABLE	INDICADOR		MEDIDA	FORMULA		
Detección de Phishing en mensajes de texto (SMS)	Tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS)		Cantidad	TPR (%)=CIEP*100/MT Donde: CIEP: Cantidad de items en estado positivo MT: Muestra total TPR: Tasa de verdaderos positivos en detección de phishing		
ITEM	FECHA	MENSAJE	HORA DE ENVIO	HORA DE RECEPCION	ESTADO DE DETECCION	TPR
1	16/05/2022	https://rakuten.grp005.work/	15:54	15:54	positivo	
2	16/05/2022	https://chat-whatsapp-join-hot.duckdns.org/	15:55	15:55	positivo	
3	16/05/2022	https://inmacon.co.jp.rbwhw.com/signin	15:59	15:59	Positivo	
4	16/05/2022	https://bit.ly/3swFehO	16:00	16:00	Positivo	
5	16/05/2022	https://eepayments.net/	16:01	16:01	Negativo	
6	16/05/2022	http://gk1.top	16:02	16:02	Positivo	
7	16/05/2022	http://m-facebook.mypi.co/	16:05	16:05	Negativo	
8	16/05/2022	http://www.msn.com/?p=newcontact&amp	16:06	16:06	Positivo	
9	16/05/2022	http://activapracticos.com	16:07	16:07	Positivo	
10	16/05/2022	http://dwallix.com/pop/	16:08	16:08	Negativo	
11	16/05/2022	Hola, ingresa a mi nuevo sitio web http://www.lomasbaratop.com	16:09	16:09	Negativo	
12	16/05/2022	Ganaste la lotería, ingresa aquí para recibir el premio: http://www.loteriaestrella.com	16:11	16:11	Negativo	
13	16/05/2022	Lotería nueva, boletos gratis en http://www.gasafarmi.com	16:12	16:12	Negativo	
14	16/05/2022	Hola, somos BBVA, acabas de realizar una transferencia bancaria sospechosa. Verifica tus datos en: http://www.bvaalert.com	16:13	16:13	Negativo	
15	16/05/2022	Tu bono del gobierno de s/150.00, ya fue depositado. Verifica aquí: https://bonogobierno.com	16:17	16:17	Negativo	
16	16/05/2022	Chaca tu bono: http://www.bonodelgobierno.com	16:22	16:22	Negativo	
17	16/05/2022	Ganaste un auto, confirma tus datos de inscripción: http://www.autosperugol.com	16:23	16:23	Negativo	
18	16/05/2022	Ganaste un curso gratis: https://www.cursosgratisp.com	16:24	16:24	Negativo	
19	16/05/2022	Recoge tu devolución de impuestos: https://www.sunatperugob.com	16:25	16:25	Negativo	
20	16/05/2022	Tu pedido ha sido cancelado. Para devolución de tu dinero, ingresa aquí: http://www.devolucionesperu.com	16:27	16:27	Negativo	

Figura S2

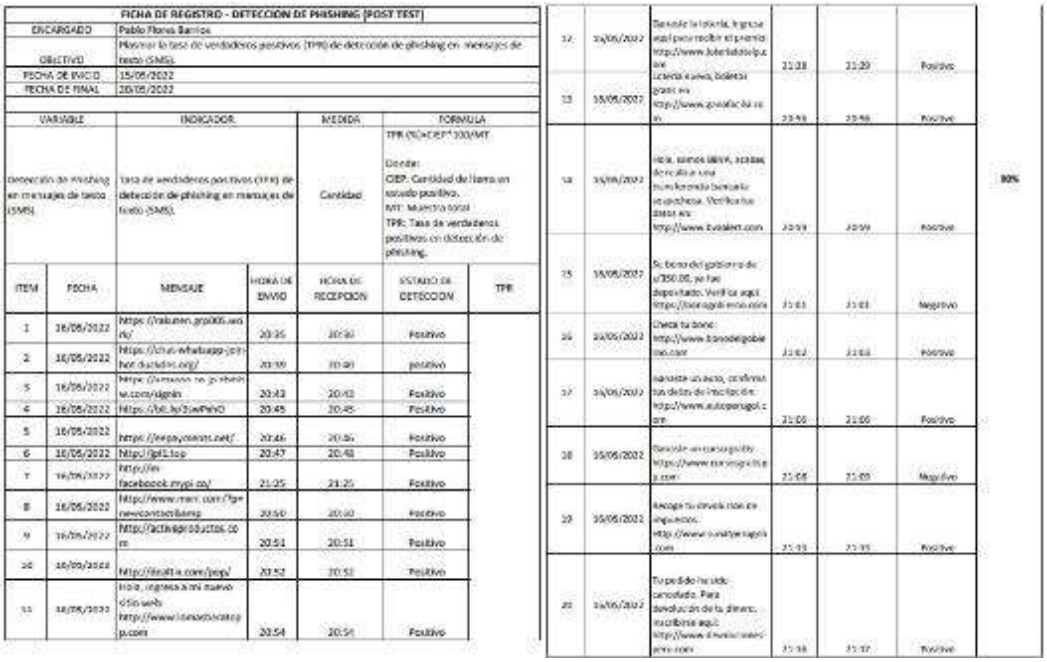
Ficha de registro de detección de Phishing – Re Test



FICHA DE REGISTRO - DETECCION DE PHISHING (RE-TEST)						
ENCARGADO	Pablo Flores Barrios					
OBJETIVO	Plasmar la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS).					
FECHA DE INICIO	15/09/2022					
FECHA DE FINAL	20/09/2022					
VARIABLE	INDICADOR		MEDIDA	FORMULA		
Detección de Phishing en mensajes de texto (SMS).	Tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS).		Cantidad	TPR (%)=CEP*100/MT Donde: CEP: Cantidad de items en estado positivo. CEN: Cantidad de items en estado negativo. MT: Muestra total TPR: Tasa de verdaderos positivos en detección de		
ITEM	FECHA	MENSAJE	HORA DE ENVIO	HORA DE RECEPCION	ESTADO DE DETECCION	TPR
1	16/05/2022	https://rakuten.grp005.work/	16:35:00	16:35:00	positivo	
2	16/05/2022	https://chat-whatsapp-join-bot.duckdns.org/	16:36:00	16:36:00	positivo	
3	16/05/2022	https://amazze.co.jp.dbnh.w.com/s-gp-s	16:37:00	16:37:00	Positivo	
4	16/05/2022	https://bit.ly/3wPNrO	16:38:00	16:38:00	Positivo	
5	16/05/2022	https://wepayments.net/	16:39:00	16:39:00	Negativo	
6	16/05/2022	http://gd1.top	16:40:00	16:40:00	Positivo	
7	16/05/2022	http://in-facebook-mypi.co/	16:41:00	16:41:00	Negativo	
8	16/05/2022	http://www.mxn.com/?p=newscontact&smp	16:42:00	16:42:00	Positivo	
9	16/05/2022	http://activeproductos.com	16:43:00	16:43:00	Negativo	
10	16/05/2022	http://krolli.com/pop/	16:44:00	16:44:00	Negativo	
11	16/05/2022	Hola, ingresa a mi nuevo sitio web http://www.lanautosac.pe.com	16:45:00	16:45:00	Negativo	
12	16/05/2022	Buscale la lotería, ingresa aquí para recibir el premio http://www.loteriadelnorte.com	16:46:30	16:46:00	Negativo	80%
13	16/05/2022	Lotería nueva, boletos gratis en http://www.gonalac.lo.com	16:47:30	16:47:00	Negativo	
14	16/05/2022	Hola, somos BBVA, acabas de realizar una transferencia bancaria sospechosa. Verifica tus datos en http://www.bvalert.com	16:48:30	16:48:00	Negativo	
15	16/05/2022	Su bono del gobierno de s/350.00, ya fue depositado. Verifica aquí https://banagobierno.com	16:49:30	16:49:00	Negativo	
16	16/05/2022	Checa tu bono http://www.bancodelgobierno.com	16:50:30	16:50:00	Negativo	
17	16/05/2022	Garantiz un auto, confirma tus datos de inscripción http://www.autopersugol.com	16:51:30	16:51:00	Negativo	
18	16/05/2022	Garantiz un curso gratis: http://www.cursogratuito.com	16:52:30	16:52:00	Negativo	
19	16/05/2022	Recoge tu devolución de impuestos http://www.europe-rugob.com	16:53:30	16:53:00	Negativo	
20	16/05/2022	Tu pedido ha sido cancelado. Para devolución de tu dinero, inscribirse aquí. https://www.devolucionesperu.com	16:56:30	16:56:00	Negativo	

Figura S3

Ficha de registro de detección de Phishing – Post Test



FICHA DE REGISTRO - DETECCION DE PHISHING (POST TEST)						
ENCARGADO	Pablo Flores Barrios					
OBJETIVO	Plasmar la tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS).					
FECHA DE INICIO	15/09/2022					
FECHA DE FINAL	20/09/2022					
VARIABLE	INDICADOR		MEDIDA	FORMULA		
Detección de Phishing en mensajes de texto (SMS).	Tasa de verdaderos positivos (TPR) de detección de phishing en mensajes de texto (SMS).		Cantidad	TPR (%)=CEP*100/MT Donde: CEP: Cantidad de items en estado positivo. MT: Muestra total TPR: Tasa de verdaderos positivos en detección de phishing.		
ITEM	FECHA	MENSAJE	HORA DE ENVIO	HORA DE RECEPCION	ESTADO DE DETECCION	TPR
1	16/05/2022	https://rakuten.grp005.work/	20:35	20:35	Positivo	
2	16/05/2022	https://chat-whatsapp-join-bot.duckdns.org/	20:39	20:39	positivo	
3	16/05/2022	https://amazze.co.jp.dbnh.w.com/signin	20:43	20:43	Positivo	
4	16/05/2022	https://bit.ly/3wPNrO	20:45	20:45	Positivo	
5	16/05/2022	https://wepayments.net/	20:46	20:46	Positivo	
6	16/05/2022	http://gd1.top	20:47	20:48	Positivo	
7	16/05/2022	http://in-facebook-mypi.co/	21:25	21:25	Positivo	
8	16/05/2022	http://www.mxn.com/?p=newscontact&smp	20:50	20:50	Positivo	
9	16/05/2022	http://activeproductos.com	20:51	20:51	Positivo	
10	16/05/2022	http://krolli.com/pop/	20:52	20:53	Positivo	
11	16/05/2022	Hola, ingresa a mi nuevo sitio web http://www.lanautosac.pe.com	20:54	20:54	Positivo	
12	16/05/2022	Buscale la lotería, ingresa aquí para recibir el premio http://www.loteriadelnorte.pe.com	21:28	21:29	Positivo	80%
13	16/05/2022	Lotería nueva, boletos gratis en http://www.gonalac.lo.com	21:46	21:46	Positivo	
14	16/05/2022	Hola, somos BBVA, acabas de realizar una transferencia bancaria sospechosa. Verifica tus datos en http://www.bvalert.com	21:59	21:59	Positivo	
15	16/05/2022	Su bono del gobierno de s/350.00, ya fue depositado. Verifica aquí https://banagobierno.com	21:01	21:01	Negativo	
16	16/05/2022	Checa tu bono http://www.bancodelgobierno.com	21:02	21:03	Positivo	
17	16/05/2022	Garantiz un auto, confirma tus datos de inscripción http://www.autopersugol.com	21:05	21:05	Positivo	
18	16/05/2022	Garantiz un curso gratis http://www.cursogratuito.com	21:08	21:09	Negativo	
19	16/05/2022	Recoge tu devolución de impuestos http://www.europe-rugob.com	21:33	21:33	Positivo	
20	16/05/2022	Tu pedido ha sido cancelado. Para devolución de tu dinero, inscribirse aquí. http://www.devolucionesperu.com	21:37	21:37	Positivo	

Apéndice T. Implementación de Bit defender para las pruebas del Pre Test.

Apéndice U. Proceso de muestreo con el aplicativo móvil.

Figura U1

Proceso de muestreo del ítem 3 en la detección de phishing Pre Test.

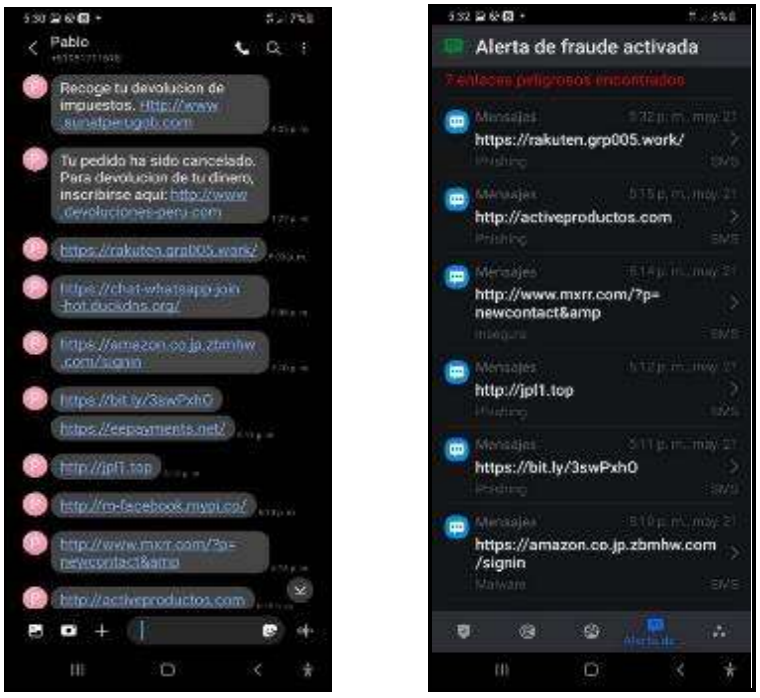


Figura U2

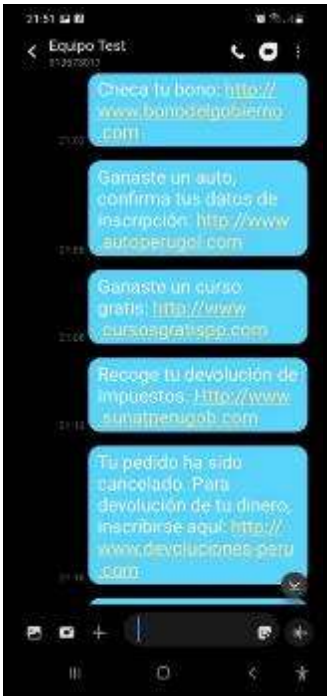
Proceso de muestreo del ítem 19 en la detección de phishing Pre Test.

Figura U3

Proceso de muestreo del ítem 03 en la detección de phishing Post Test.

Figura U4

Proceso de muestreo del ítem 19 en la detección de phishing Post Test.



Apéndice V. Activity recomendaciones.

Apéndice W. Tipos de generación de alertas.

Figura W1

Layout de Recomendaciones

Figura W2

Notificaciones de SMS seguro o Ataque Phishing.

Apéndice X. Procedimiento de generación de alertas.

Figura X1

Proceso de muestreo del ítem 03 en la generación de alertas Pre Test.

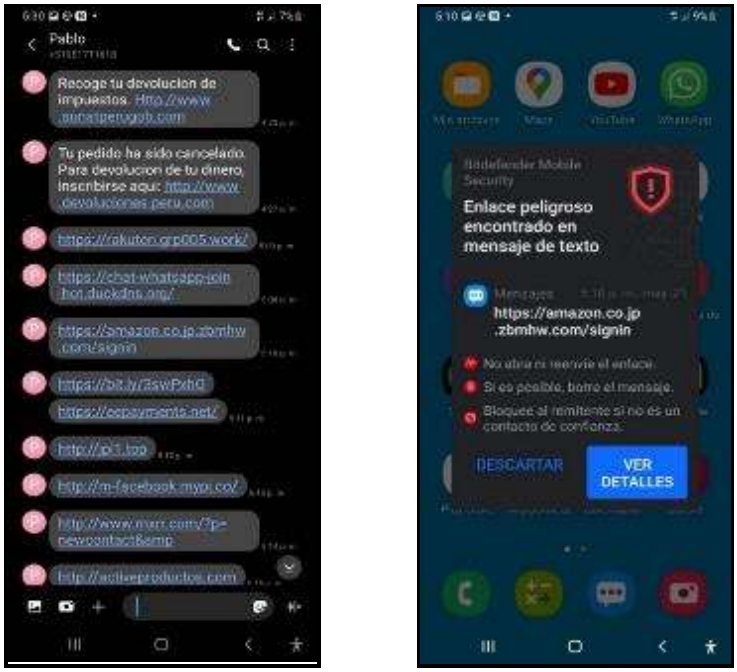


Figura X2

Proceso de muestreo del ítem 19 en la generación de alertas Pre Test.

Figura X3

Proceso de muestreo del ítem 03 en la generación de alertas Post Test.

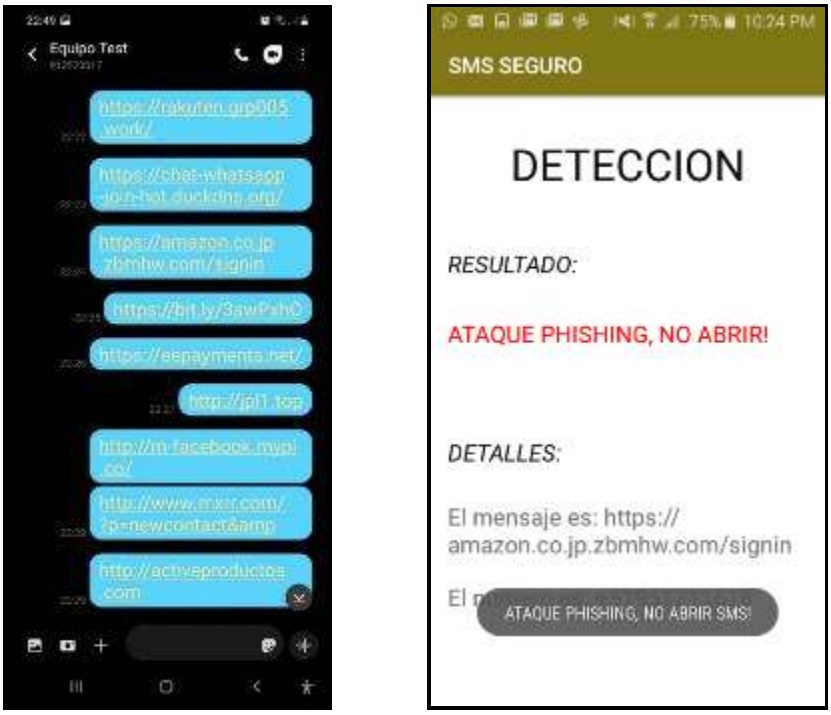
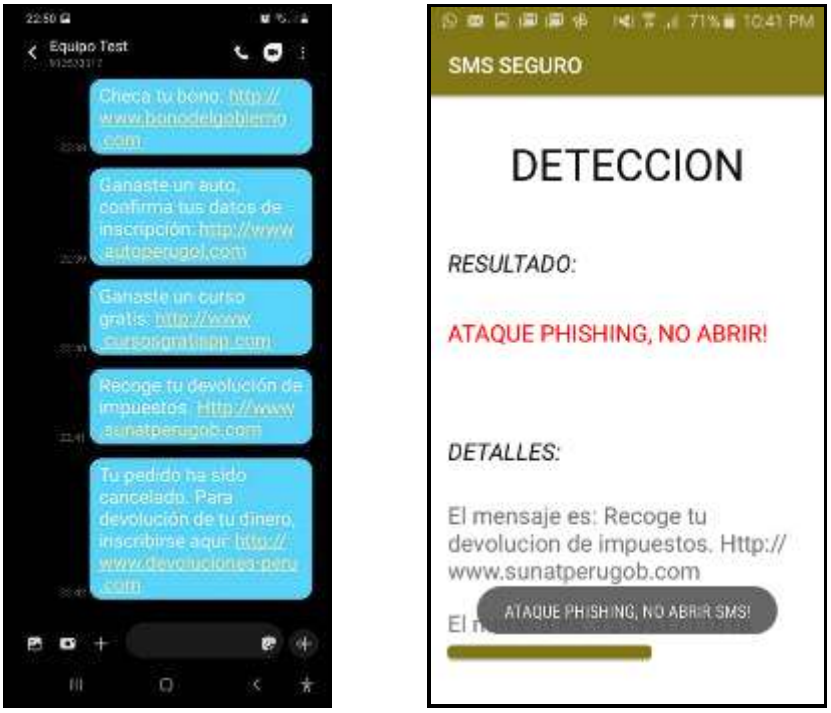


Figura X4

Proceso de muestreo del ítem 19 en la generación de alertas Post Test.



Apéndice Y. Fichas de registro de generación de alertas.

Figura Y1

Ficha de registro de generación de alertas – Pre Test.

FICHA DE REGISTRO - GENERACION DE ALERTAS (PRE- TEST)	
ENCARGADO	Pablo Flores Barrios
OBJETIVO	Plasmar la tasa de verdaderos positivos (TPR) de generación de alertas y/o recomendaciones por cada ítem de la muestra.
FECHA DE INICIO	15/05/2022
FECHA DE FINAL	20/05/2022

VARIABLE	INDICADOR	MEDIDA	FORMULA
Detección de Phishing en mensajes de texto (SMS)	Tasa de verdaderos positivos (TPR) de generación de alertas o recomendaciones en los mensajes de texto SMS recibidos.	Cantidad	TPR (%)=CIEP*100/MT Donde: CIEP: Cantidad de items en estado positivo MT: Muestra total TPR: Tasa de verdaderos positivos en generación de alertas.

ITEM	FECHA	MENSAJE	HORA DE ENVIO	HORA DE RECEPCION	ESTADO DE GENERACION DE ALERTA	TPR
1	16/05/2022	https://rakuten.grp005.work/	[illegible]	[illegible]	positivo	
2	16/05/2022	https://chat-whatsapp-join-hot.duckdns.org/	17:08	17:08	positivo	
3	16/05/2022	https://amazon.co.jp.zbmhw.com/signin	17:10	17:10	Positivo	
4	16/05/2022	https://bit.ly/3swPxhO	17:10	17:10	Positivo	
5	16/05/2022	https://eepayments.net/	17:11	17:11	negativo	
6	16/05/2022	http://jp01.top	[illegible]	[illegible]	positivo	
7	16/05/2022	http://m-facebook.mypi.co/	17:13	17:13	negativo	
8	16/05/2022	http://www.mxrr.com/?p=sewcontact&amp	17:14	17:14	positivo	
9	16/05/2022	http://actiweproductos.com	17:15	17:15	positivo	
10	16/05/2022	http://dealtb.com/pop/	17:16	17:16	negativo	
11	16/05/2022	Hola, ingresa a mi nuevo sitio web: http://www.lomasbaratoapp.com	17:16	17:22	negativo	
12	16/05/2022	Ganaste la lotería, ingresa aquí para recibir el premio: http://www.loteriatotalp.com	17:22	17:22	negativo	
13	16/05/2022	Lotería nueva, boletos gratis en: http://www.ganafacil.com	17:22	17:22	negativo	
14	16/05/2022	Hola, somos BBVA, acabas de realizar una transferencia bancaria sospechosa. Verifica tus datos en: http://www.bvaalert.com	17:23	17:23	negativo	35%
15	16/05/2022	Su bono del gobierno de s/350.00, ya fue depositado. Verifica aquí: https://bonogobierno.com	17:24	17:24	negativo	
16	16/05/2022	Checa tu bono: http://www.bonodelgobierno.com	17:25	17:25	negativo	
17	16/05/2022	Ganaste un auto, confirma tus datos de inscripción: http://www.autoperusol.com	17:26	17:26	negativo	
18	16/05/2022	Ganaste un curso gratis: https://www.cursosgratisapp.com	17:26	17:26	negativo	
19	16/05/2022	Recoge tu devolución de impuestos: https://www.sunatpersgob.com	17:27	17:27	negativo	
20	16/05/2022	Tu pedido ha sido cancelado. Para devolución de tu dinero, inscribirse aquí: http://www.devoluciones-peru.com	17:28	17:28	negativo	

Figura Y2

Ficha de registro de generación de alertas – Re Test.

FICHA DE REGISTRO - GENERACION DE ALERTAS (RE- TEST)	
ENCARGADO	Pablo Flores Barrios
OBJETIVO	Plasmar la tasa de verdaderos positivos (TPR) de generación de alertas y/o recomendaciones por cada ítem de la muestra.
FECHA DE INICIO	15/05/2022
FECHA DE FINAL	30/05/2022

VARIABLE	INDICADOR	MEDIDA	FORMULA
Detección de Phishing en mensajes de texto (SMS).	Tasa de verdaderos positivos (TPR) de generación de alertas en los mensajes de texto SMS recibidos.	Cantidad	TPR (%)=CIEP*100/MT Donde: CIEP: Cantidad de items en estado positivo. CIEN: Cantidad de items en estado negativo. MT: Muestra total TPR: Tasa de verdaderos positivos en generación de alertas.

ITEM	FECHA	MENSAJE	HORA DE ENVIO	HORA DE RECEPCION	ESTADO DE GENERACION DE ALERTA	TPR
1	16/05/2022	https://rakuten.grp005.work/	18:01:00	18:01:00	positivo	
2	16/05/2022	https://chat-whatsapp-join-hot.duckdns.org/	18:02:00	18:02:00	positivo	
3	16/05/2022	https://amazon.co.jp.zbmhw.com/signin	18:03:00	18:03:00	Positivo	
4	16/05/2022	https://bit.ly/3swPxhO	18:04:00	18:04:00	Positivo	
5	16/05/2022	https://eepayments.net/	18:05:00	18:05:00	negativo	
6	16/05/2022	http://jp01.top	18:06:00	18:06:00	positivo	
7	16/05/2022	http://m-facebook.mypi.co/	18:07:00	18:07:00	negativo	
8	16/05/2022	http://www.mxrr.com/?p=sewcontact&amp	18:08:00	18:08:00	positivo	
9	16/05/2022	http://actiweproductos.com	18:09:00	18:09:00	negativo	
10	16/05/2022	http://dealtb.com/pop/	18:10:00	18:10:00	negativo	
11	16/05/2022	Hola, ingresa a mi nuevo sitio web: http://www.lomasbaratoapp.com	18:11:00	18:11:00	negativo	
12	16/05/2022	Ganaste la lotería, ingresa aquí para recibir el premio: http://www.loteriatotalp.com	18:12:00	18:12:00	negativo	
13	16/05/2022	Lotería nueva, boletos gratis en: http://www.ganafacil.com	18:13:00	18:13:00	negativo	
14	16/05/2022	Hola, somos BBVA, acabas de realizar una transferencia bancaria sospechosa. Verifica tus datos en: http://www.bvaalert.com	18:14:00	18:14:00	negativo	[illegible]
15	16/05/2022	Su bono del gobierno de s/350.00, ya fue depositado. Verifica aquí: https://bonogobierno.com	18:15:00	18:15:00	negativo	
16	16/05/2022	Checa tu bono: http://www.bonodelgobierno.com	18:16:00	18:16:00	negativo	
17	16/05/2022	Ganaste un auto, confirma tus datos de inscripción: http://www.autoperusol.com	18:18:00	18:18:00	negativo	
18	16/05/2022	Ganaste un curso gratis: https://www.cursosgratisapp.com	18:19:00	18:19:00	negativo	
19	16/05/2022	Recoge tu devolución de impuestos: https://www.sunatpersgob.com	18:21:00	18:22:00	negativo	
20	16/05/2022	Tu pedido ha sido cancelado. Para devolución de tu dinero, inscribirse aquí: http://www.devoluciones-peru.com	18:23:00	18:23:00	negativo	

Figura Y3

Ficha de registro de generación de alertas – Post Test.

FICHA DE REGISTRO - GENERACION DE ALERTAS (POST TEST)			
ENCARGADO	Pablo Flores Barrios		
OBJETIVO	Plasmar la tasa de verdaderos positivos (TPR) de generación de alertas y/o recomendaciones por cada item de la muestra.		
FECHA DE INICIO	15/05/2022		
FECHA DE FINAL	20/05/2022		
VARIABLE	INDICADOR	MEDIDA	FORMULA
Detección de Phishing en mensajes de texto (SMS).	Tasa de verdaderos positivos (TPR) de generación de alertas o recomendaciones en los mensajes de texto SMS recibidos.	Cantidad	TPR (%)=CIEP*100/MT Donde: CIEP: Cantidad de items en estado positivo MT: Muestra total TPR: Tasa de verdaderos positivos en generación de alertas.

ITEM	FECHA	MENSAJE	HORA DE ENVIO	HORA DE RECEPCION	ESTADO DE GENERACION DE ALERTA	TPR
1	16/05/2022	https://rakuten.grp005.work/	22:12	22:22	positivo	90%
2	16/05/2022	https://chat-whatsapp-join-hot.duckdns.org/	22:23	22:24	positivo	
3	16/05/2022	https://amazon.co.jp.dbmhw.com/signin	22:24	22:24	positivo	
4	16/05/2022	https://bit.ly/3swPxhO	22:25	22:25	positivo	
5	16/05/2022	https://eepayments.net/	22:26	22:26	positivo	
6	16/05/2022	http://jp11.top	22:27	22:27	positivo	
7	16/05/2022	http://m-facebook.mypl.co/	22:27	22:28	positivo	
8	16/05/2022	http://www.marr.com/?pme=wcontact&amp	22:28	22:29	positivo	
9	16/05/2022	http://activaproductos.com	22:28	22:29	positivo	
10	16/05/2022	http://dealtis.com/pop/	22:30	22:30	positivo	
11	16/05/2022	Hola, ingresa a mi nuevo sitio web: http://www.lomasbaratopp.com	22:32	22:32	positivo	
12	16/05/2022	Ganaste la lotería, ingresa aquí para recibir el premio: http://www.loteriaonline.com	22:33	22:33	positivo	
13	16/05/2022	Sorteo nuevo, boletos gratis en: http://www.gratisticket.com	22:34	22:34	positivo	
14	16/05/2022	Hola, somos BBVA, acabas de realizar una transferencia bancaria sospechosa. Verifica tus datos en: http://www.bvaalert.com	22:36	22:36	positivo	
15	16/05/2022	Su bono del gobierno de s/350.00, ya fue depositado. Verifica aquí: https://bonogobierno.com	22:37	22:37	negativo	
16	16/05/2022	Checa tu bono: http://www.bonodelgobierno.com	22:38	22:38	positivo	
17	16/05/2022	Ganaste un auto, confirma tus datos de inscripción: http://www.autoperugob.com	22:39	22:39	positivo	
18	16/05/2022	Ganaste un curso gratis: https://www.cursosgratisapp.com	22:40	22:40	negativo	
19	16/05/2022	Recoge tu devolución de impuestos: http://www.sunatperugob.com	22:41	22:41	positivo	
20	16/05/2022	Tu pedido ha sido cancelado. Para devolución de tu dinero, inscríbete aquí: http://www.devolucionesperu.com	22:42	22:42	positivo	

Apéndice Z: Estructura general del código del aplicativo móvil propuesto.

Figura Z1

Total de clases del aplicativo móvil propuesto, ordenados por funciones.

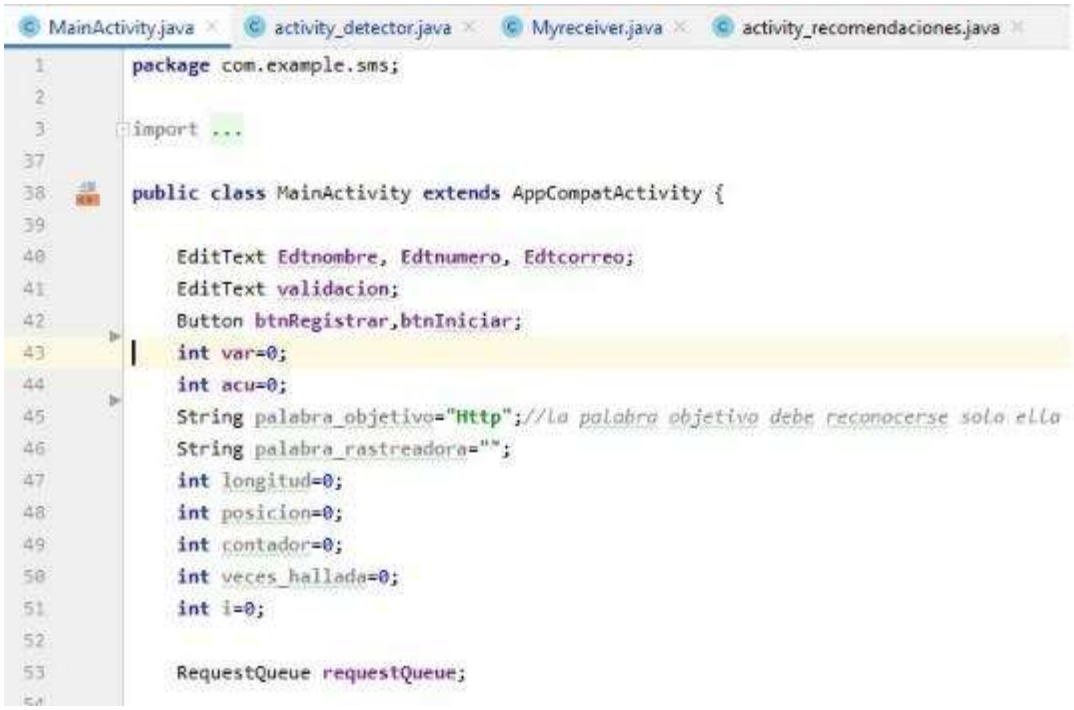
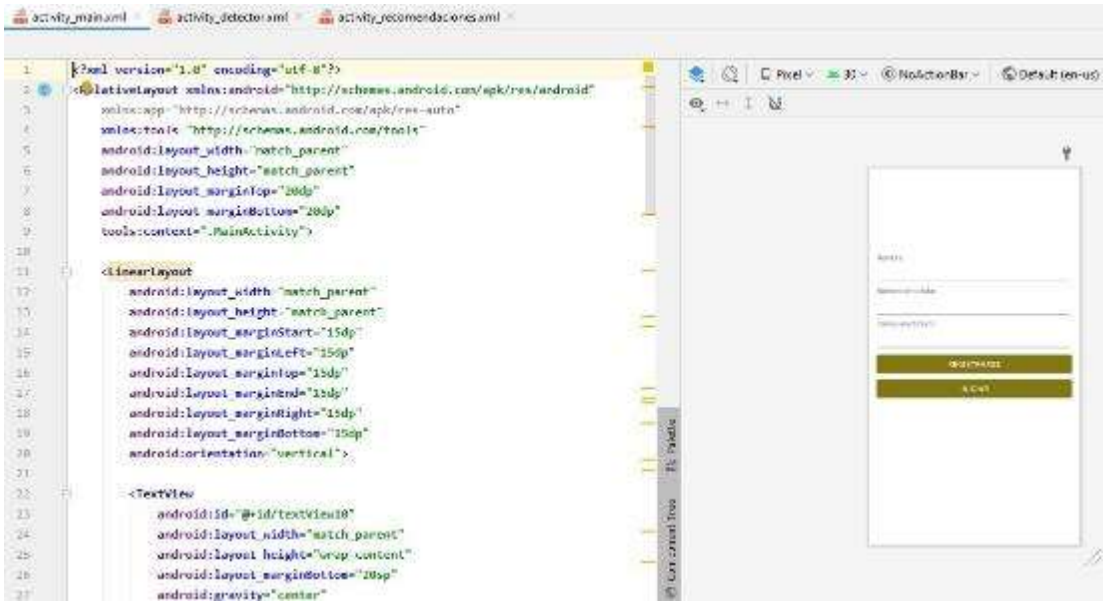
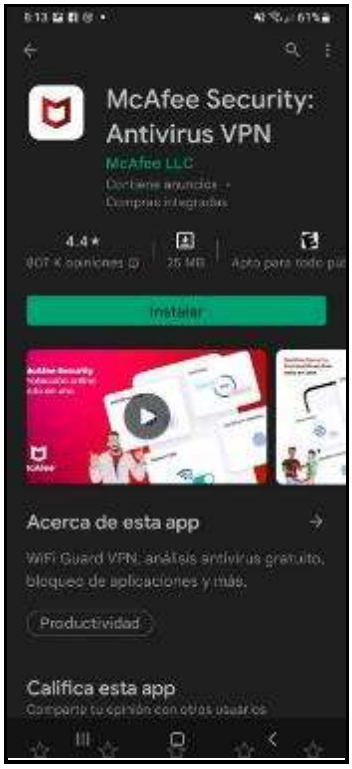


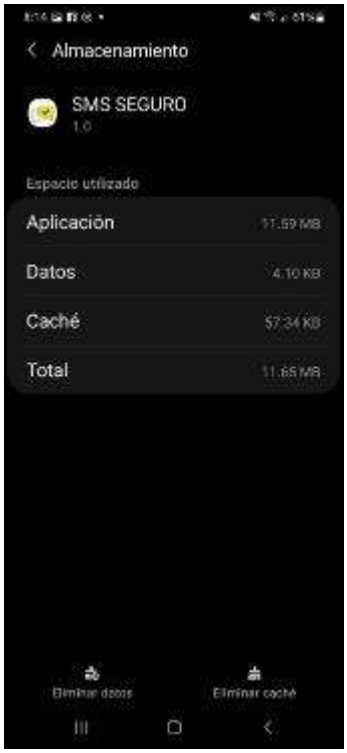
Figura Z2

Total de layouts del aplicativo móvil propuesto, ordenados por funciones.



Apéndice AA. Comparativa de antivirus para teléfonos celulares según tamaño en MB.





Apéndice AB. Juicio de experto 1 – Ficha de registro Pre test de detección de phishing.

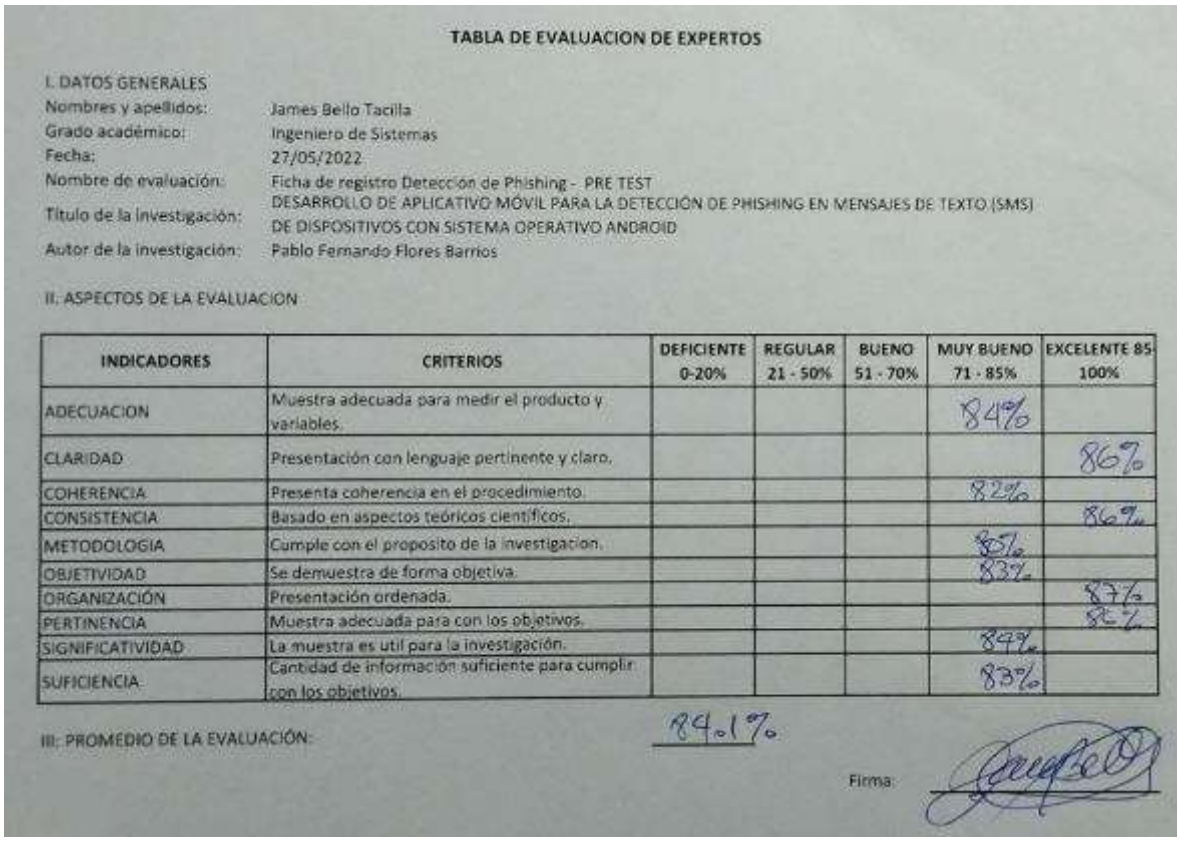


TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES

Nombres y apellidos: James Bello Tacilla
Grado académico: Ingeniero de Sistemas
Fecha: 27/05/2022
Nombre de evaluación: Ficha de registro Detección de Phishing - PRE TEST
Título de la investigación: DESARROLLO DE APLICATIVO MÓVIL PARA LA DETECCIÓN DE PHISHING EN MENSAJES DE TEXTO (SMS) DE DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID
Autor de la investigación: Pablo Fernando Flores Barrios

II. ASPECTOS DE LA EVALUACION

INDICADORES	CRITERIOS	DEFICIENTE 0-20%	REGULAR 21 - 50%	BUENO 51 - 70%	MUY BUENO 71 - 85%	EXCELENTE 85-100%
ADECUACION	Muestra adecuada para medir el producto y variables.				84%	
CLARIDAD	Presentación con lenguaje pertinente y claro.					86%
COHERENCIA	Presenta coherencia en el procedimiento.				82%	
CONSISTENCIA	Basado en aspectos teóricos científicos.					86%
METODOLOGIA	Cumple con el proposito de la investigacion.				85%	
OBJETIVIDAD	Se demuestra de forma objetiva.				83%	
ORGANIZACIÓN	Presentación ordenada.					87%
PERTINENCIA	Muestra adecuada para con los objetivos.					87%
SIGNIFICATIVIDAD	La muestra es util para la investigación.				84%	
SUFICIENCIA	Cantidad de información suficiente para cumplir con los objetivos.				83%	

III. PROMEDIO DE LA EVALUACIÓN: 89.1%

Firma:

Apéndice AC. Juicio de experto 2 – Ficha de registro Pre test de detección de phishing.

TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES

Nombres y apellidos: Leoncio Roca Rojas
Grado académico: Ingeniero Químico
Fecha: 26/05/2022
Nombre de evaluación: Ficha de registro Detección de Phishing - PRE TEST
Titulo de la investigación: DESARROLLO DE APLICATIVO MÓVIL PARA LA DETECCIÓN DE PHISHING EN MENSAJES DE TEXTO (SMS) DE DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID
Autor de la investigación: Pablo Fernando Flores Barrios

II. ASPECTOS DE LA EVALUACION

INDICADORES	CRITERIOS	DEFICIENTE 0-20%	REGULAR 21 - 50%	BUENO 51 - 70%	MUY BUENO 71 - 85%	EXCELENTE 85-100%
ADECUACION	Muestra adecuada para medir el producto y variables.				85	
CLARIDAD	Presentación con lenguaje pertinente y claro.				80	
COHERENCIA	Presenta coherencia en el procedimiento.				85	
CONSISTENCIA	Basado en aspectos teóricos científicos.				79	
METODOLOGIA	Cumple con el proposito de la investigacion.				85	
OBJETIVIDAD	Se demuestra de forma objetiva.					90
ORGANIZACIÓN	Presentación ordenada.					90
PERTINENCIA	Muestra adecuada para con los objetivos.					90
SIGNIFICATIVIDAD	La muestra es util para la investigación.					90
SUFICIENCIA	Cantidad de información suficiente para cumplir con los objetivos.				85	

III. PROMEDIO DE LA EVALUACIÓN: 85.9

Firma:

Apéndice AD. Juicio de experto 3 – Ficha de registro Pre test de detección de phishing.

TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES

Nombres y apellidos: Luis Catalán Fonseca
Grado académico: Ingeniero Electrónico
Fecha: 22/05/2022
Nombre de evaluación: Ficha de registro Detección de Phishing - PRE TEST
Titulo de la investigación: DESARROLLO DE APLICATIVO MÓVIL PARA LA DETECCIÓN DE PHISHING EN MENSAJES DE TEXTO (SMS) DE DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID
Autor de la investigación: Pablo Fernando Flores Barrios

II. ASPECTOS DE LA EVALUACION

INDICADORES	CRITERIOS	DEFICIENTE 0-20%	REGULAR 21 - 50%	BUENO 51 - 70%	MUY BUENO 71 - 85%	EXCELENTE 85-100%
ADECUACION	Muestra adecuada para medir el producto y variables.					90
CLARIDAD	Presentación con lenguaje pertinente y claro.				75	
COHERENCIA	Presenta coherencia en el procedimiento.					90
CONSISTENCIA	Basado en aspectos teóricos científicos.					90
METODOLOGIA	Cumple con el proposito de la investigacion.					90
OBJETIVIDAD	Se demuestra de forma objetiva.					90
ORGANIZACIÓN	Presentación ordenada.					90
PERTINENCIA	Muestra adecuada para con los objetivos.					90
SIGNIFICATIVIDAD	La muestra es util para la investigación.					90
SUFICIENCIA	Cantidad de información suficiente para cumplir con los objetivos.					90

III: PROMEDIO DE LA EVALUACIÓN: 88.5

Firma:

Apéndice AE. Juicio de experto 1 – Ficha de registro Post test de detección de phishing.

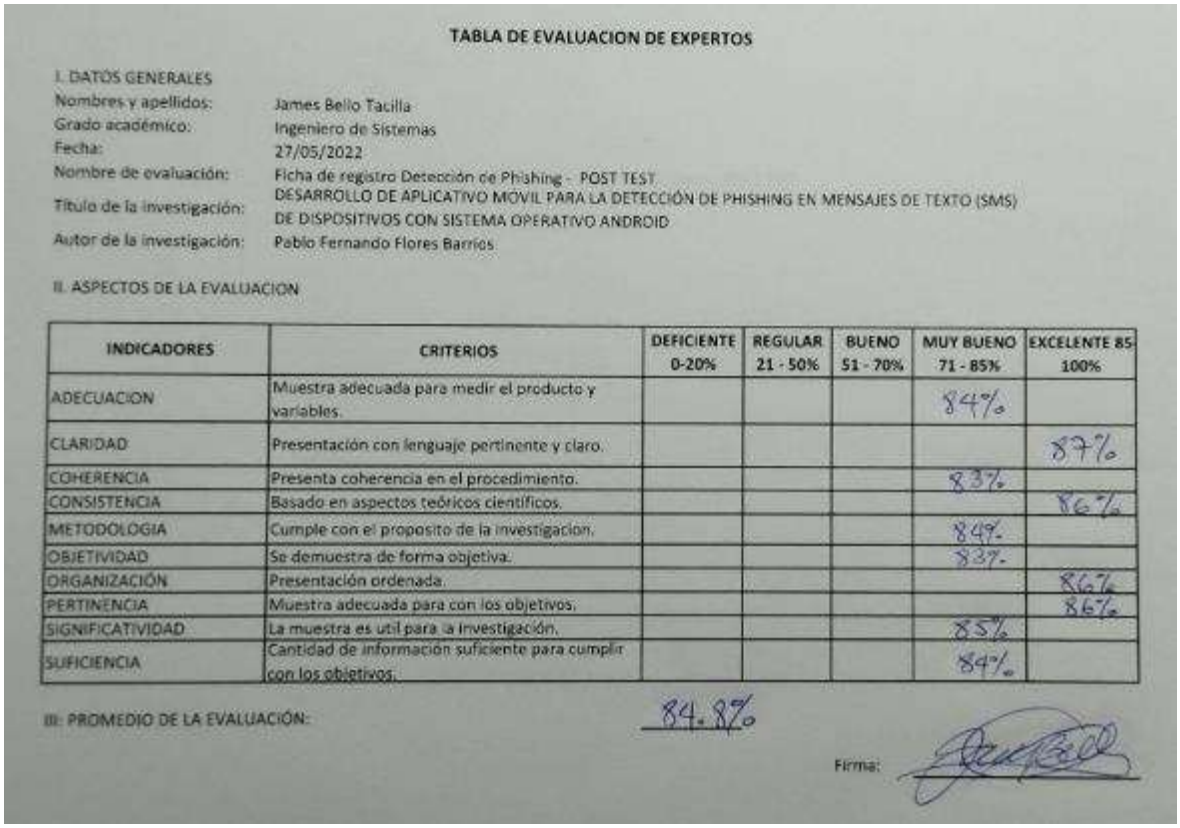


TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES

Nombres y apellidos: James Bello Tacilla
Grado académico: Ingeniero de Sistemas
Fecha: 27/05/2022
Nombre de evaluación: Ficha de registro Detección de Phishing - POST TEST
Título de la investigación: DESARROLLO DE APLICATIVO MOVIL PARA LA DETECCIÓN DE PHISHING EN MENSAJES DE TEXTO (SMS) DE DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID
Autor de la investigación: Pablo Fernando Flores Barrios

II. ASPECTOS DE LA EVALUACION

INDICADORES	CRITERIOS	DEFICIENTE 0-20%	REGULAR 21 - 50%	BUENO 51 - 70%	MUY BUENO 71 - 85%	EXCELENTE 85 100%
ADECUACION	Muestra adecuada para medir el producto y variables.				84%	
CLARIDAD	Presentación con lenguaje pertinente y claro.					87%
COHERENCIA	Presenta coherencia en el procedimiento.				83%	
CONSISTENCIA	Basado en aspectos teóricos científicos.					86%
METODOLOGIA	Cumple con el proposito de la investigacion.				849.	
OBJETIVIDAD	Se demuestra de forma objetiva.				837.	
ORGANIZACIÓN	Presentación ordenada.					86%
PERTINENCIA	Muestra adecuada para con los objetivos.					86%
SIGNIFICATIVIDAD	La muestra es util para la investigación.				85%	
SUFICIENCIA	Cantidad de información suficiente para cumplir con los objetivos.				84%	

III. PROMEDIO DE LA EVALUACIÓN: 84.8%

Firma:

Apéndice AF. Juicio de experto 2 – Ficha de registro Post test de detección de phishing.

TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES

Nombres y apellidos: Leoncio Roca Rojas
Grado académico: Ingeniero Químico
Fecha: 26/05/2022
Nombre de evaluación: Ficha de registro Detección de Phishing - POST TEST
Título de la investigación: DESARROLLO DE APLICATIVO MÓVIL PARA LA DETECCIÓN DE PHISHING EN MENSAJES DE TEXTO (SMS) DE DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID
Autor de la investigación: Pablo Fernando Flores Barrios

II. ASPECTOS DE LA EVALUACION

INDICADORES	CRITERIOS	DEFICIENTE 0-20%	REGULAR 21 - 50%	BUENO 51 - 70%	MUY BUENO 71 - 85%	EXCELENTE 85-100%
ADECUACION	Muestra adecuada para medir el producto y variables.					92
CLARIDAD	Presentación con lenguaje pertinente y claro.					90
COHERENCIA	Presenta coherencia en el procedimiento.					96
CONSISTENCIA	Basado en aspectos teóricos científicos.					95
METODOLOGIA	Cumple con el proposito de la investigacion.					94
OBJETIVIDAD	Se demuestra de forma objetiva.					87
ORGANIZACIÓN	Presentación ordenada.					89
PERTINENCIA	Muestra adecuada para con los objetivos.					93
SIGNIFICATIVIDAD	La muestra es util para la investigación.					95
SUFICIENCIA	Cantidad de información suficiente para cumplir con los objetivos.					90

III: PROMEDIO DE LA EVALUACIÓN: 92.1

Firma:

Apéndice AG. Juicio de experto 3 – Ficha de registro Post test de detección de phishing.

TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES

Nombres y apellidos:	Luis Catalán Fonseca
Grado académico:	Ingeniero Electrónico
Fecha:	22/05/2022
Nombre de evaluación:	Ficha de registro Detección de Phishing - POST TEST
Título de la investigación:	DESARROLLO DE APLICATIVO MÓVIL PARA LA DETECCIÓN DE PHISHING EN MENSAJES DE TEXTO (SMS) DE DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID
Autor de la investigación:	Pablo Fernando Flores Barrios

II. ASPECTOS DE LA EVALUACION

INDICADORES	CRITERIOS	DEFICIENTE 0-20%	REGULAR 21 - 50%	BUENO 51 - 70%	MUY BUENO 71 - 85%	EXCELENTE 85 100%
ADECUACION	Muestra adecuada para medir el producto y variables.					90
CLARIDAD	Presentación con lenguaje pertinente y claro.				75	
COHERENCIA	Presenta coherencia en el procedimiento.					90
CONSISTENCIA	Basado en aspectos teóricos científicos.					90
METODOLOGIA	Cumple con el proposito de la investigacion.					90
OBJETIVIDAD	Se demuestra de forma objetiva.					90
ORGANIZACIÓN	Presentación ordenada.					90
PERTINENCIA	Muestra adecuada para con los objetivos.					90
SIGNIFICATIVIDAD	La muestra es util para la investigación.					90
SUFICIENCIA	Cantidad de información suficiente para cumplir con los objetivos.					90

III: PROMEDIO DE LA EVALUACIÓN: 88.5

Firma:

Apéndice AH. Juicio de experto 1 – Ficha de registro Pre test de generación de alertas.

TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES

Nombres y apellidos: James Bello Tacilla
Grado académico: Ingeniero de Sistemas
Fecha: 27/05/2022
Nombre de evaluación: Ficha de registro Generación de alertas y recomendaciones - PRE TEST
Título de la investigación: DESARROLLO DE APLICATIVO MÓVIL PARA LA DETECCIÓN DE PHISHING EN MENSAJES DE TEXTO (SMS) DE DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID
Autor de la investigación: Pablo Fernando Flores Barrios

II. ASPECTOS DE LA EVALUACION

INDICADORES	CRITERIOS	DEFICIENTE 0-20%	REGULAR 21 - 50%	BUENO 51 - 70%	MUY BUENO 71 - 85%	EXCELENTE 85 100%
ADECUACION	Muestra adecuada para medir el producto y variables.				85%	
CLARIDAD	Presentación con lenguaje pertinente y claro.					86%
COHERENCIA	Presenta coherencia en el procedimiento.				84%	
CONSISTENCIA	Basado en aspectos teóricos científicos.					87%
METODOLOGIA	Cumple con el propósito de la investigación.				82%	
OBJETIVIDAD	Se demuestra de forma objetiva.				83%	
ORGANIZACIÓN	Presentación ordenada					86%
PERTINENCIA	Muestra adecuada para con los objetivos.					87%
SIGNIFICATIVIDAD	La muestra es útil para la investigación.				83%	
SUFICIENCIA	Cantidad de información suficiente para cumplir con los objetivos.				84%	

III. PROMEDIO DE LA EVALUACIÓN: 84.7%

Firma:

Apéndice AI. Juicio de experto 2 – Ficha de registro Pre test de generación de alertas.

TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES

Nombres y apellidos: Leoncio Roca Rojas
Grado académico: Ingeniero Quimico
Fecha: 26/05/2022
Nombre de evaluación: Ficha de registro Generación de alertas y recomendaciones - PRE TEST
Título de la investigación: DESARROLLO DE APLICATIVO MÓVIL PARA LA DETECCIÓN DE PHISHING EN MENSAJES DE TEXTO (SMS) DE DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID
Autor de la investigación: Pablo Fernando Flores Barrios

II. ASPECTOS DE LA EVALUACION

INDICADORES	CRITERIOS	DEFICIENTE 0-20%	REGULAR 21 - 50%	BUENO 51 - 70%	MUY BUENO 71 - 85%	EXCELENTE 85-100%
ADECUACION	Muestra adecuada para medir el producto y variables.					90
CLARIDAD	Presentación con lenguaje pertinente y claro.				85	
COHERENCIA	Presenta coherencia en el procedimiento.					90
CONSISTENCIA	Basado en aspectos teóricos científicos.					90
METODOLOGIA	Cumple con el proposito de la investigacion.				85	
OBJETIVIDAD	Se demuestra de forma objetiva.				80	
ORGANIZACIÓN	Presentación ordenada.					90
PERTINENCIA	Muestra adecuada para con los objetivos.				85	
SIGNIFICATIVIDAD	La muestra es util para la investigación.					95
SUFICIENCIA	Cantidad de información suficiente para cumplir con los objetivos.				80	

III: PROMEDIO DE LA EVALUACIÓN: 87

Firma:

Apéndice AJ. Juicio de experto 3 – Ficha de registro Pre test de generación de alertas.

TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES

Nombres y apellidos:	Luis Catalán Fonseca
Grado académico:	Ingeniero Electrónico
Fecha:	22/05/2022
Nombre de evaluación:	Ficha de registro Generación de alertas y recomendaciones - PRE TEST
Titulo de la investigación:	DESARROLLO DE APLICATIVO MÓVIL PARA LA DETECCIÓN DE PHISHING EN MENSAJES DE TEXTO (SMS) DE DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID
Autor de la investigación:	Pablo Fernando Flores Barrios

II. ASPECTOS DE LA EVALUACION

INDICADORES	CRITERIOS	DEFICIENTE 0-20%	REGULAR 21 - 50%	BUENO 51 - 70%	MUY BUENO 71 - 85%	EXCELENTE 85 100%
ADECUACION	Muestra adecuada para medir el producto y variables.					90
CLARIDAD	Presentación con lenguaje pertinente y claro.				75	
COHERENCIA	Presenta coherencia en el procedimiento.					90
CONSISTENCIA	Basado en aspectos teóricos científicos.					90
METODOLOGIA	Cumple con el proposito de la investigacion.					90
OBJETIVIDAD	Se demuestra de forma objetiva.					90
ORGANIZACIÓN	Presentación ordenada.					90
PERTINENCIA	Muestra adecuada para con los objetivos.					90
SIGNIFICATIVIDAD	La muestra es util para la investigación.					90
SUFICIENCIA	Cantidad de información suficiente para cumplir con los objetivos.					90

III: PROMEDIO DE LA EVALUACIÓN: 88.5

Firma:

Apéndice AK. Juicio de experto 1 – Ficha de registro Post test de generación de alertas.

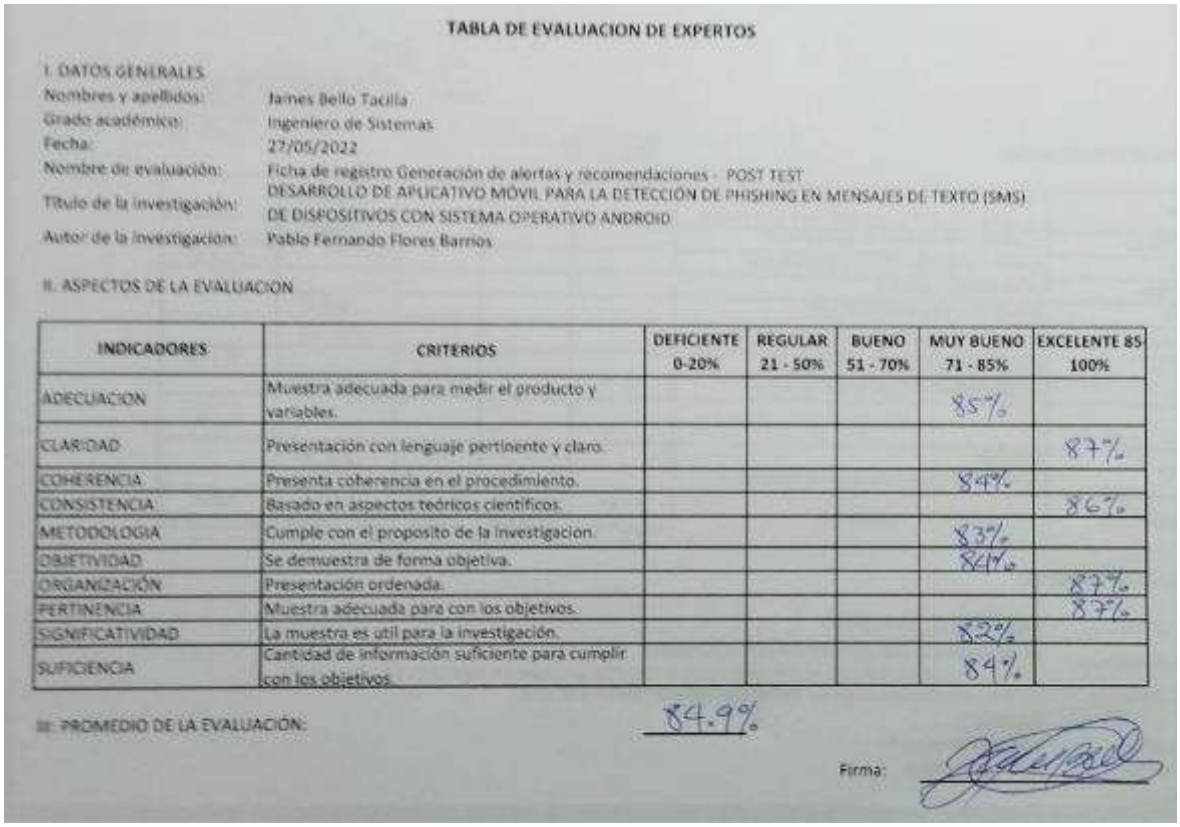


TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES

Nombres y apellidos: James Bello Tacilla
Grado académico: Ingeniero de Sistemas
Fecha: 27/05/2022
Nombre de evaluación: Ficha de registro Generación de alertas y recomendaciones - POST TEST
Título de la investigación: DESARROLLO DE APLICATIVO MÓVIL PARA LA DETECCIÓN DE PHISHING EN MENSAJES DE TEXTO (SMS) DE DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID
Autor de la investigación: Pablo Fernando Flores Barrios

II. ASPECTOS DE LA EVALUACION

INDICADORES	CRITERIOS	DEFICIENTE 0-20%	REGULAR 21 - 50%	BUENO 51 - 70%	MUY BUENO 71 - 85%	EXCELENTE 85 100%
ADECUACION	Muestra adecuada para medir el producto y variables.				85%	
CLARIDAD	Presentación con lenguaje pertinente y claro.					87%
COHERENCIA	Presenta coherencia en el procedimiento.				84%	
CONSISTENCIA	Basado en aspectos teóricos científicos.					86%
METODOLOGIA	Cumple con el propósito de la investigación.				83%	
OBJETIVIDAD	Se demuestra de forma objetiva.				84%	
ORGANIZACIÓN	Presentación ordenada.					87%
PERTINENCIA	Muestra adecuada para con los objetivos.					87%
SIGNIFICATIVIDAD	La muestra es útil para la investigación.				82%	
SUFICIENCIA	Cantidad de información suficiente para cumplir con los objetivos				84%	

III. PROMEDIO DE LA EVALUACIÓN: 84.9%

Firma:

Apéndice AL. Juicio de experto 2 – Ficha de registro Post test de generación de alertas.

TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES

Nombres y apellidos: Leoncio Roca Rojas
Grado académico: Ingeniero Químico
Fecha: 26/05/2022
Nombre de evaluación: Ficha de registro Generación de alertas y recomendaciones - POST TEST
Título de la investigación: DESARROLLO DE APLICATIVO MÓVIL PARA LA DETECCIÓN DE PHISHING EN MENSAJES DE TEXTO (SMS) DE DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID
Autor de la investigación: Pablo Fernando Flores Barrios

II. ASPECTOS DE LA EVALUACION

INDICADORES	CRITERIOS	DEFICIENTE 0-20%	REGULAR 21 - 50%	BUENO 51 - 70%	MUY BUENO 71 - 85%	EXCELENTE 85-100%
ADECUACION	Muestra adecuada para medir el producto y variables.					86
CLARIDAD	Presentación con lenguaje pertinente y claro.					90
COHERENCIA	Presenta coherencia en el procedimiento.					95
CONSISTENCIA	Basado en aspectos teóricos científicos.					95
METODOLOGIA	Cumple con el proposito de la investigacion.					90
OBJETIVIDAD	Se demuestra de forma objetiva.					88
ORGANIZACIÓN	Presentación ordenada.					92
PERTINENCIA	Muestra adecuada para con los objetivos.					95
SIGNIFICATIVIDAD	La muestra es util para la investigación.					97
SUFICIENCIA	Cantidad de información suficiente para cumplir con los objetivos.					90

III: PROMEDIO DE LA EVALUACIÓN: 91.8

Firma:

Apéndice ALL. Juicio de experto 3 – Ficha de registro Post test de generación de alertas.

TABLA DE EVALUACION DE EXPERTOS

I. DATOS GENERALES

Nombres y apellidos:	Luis Catalán Fonseca
Grado académico:	Ingeniero Electrónico
Fecha:	22/05/2022
Nombre de evaluación:	Ficha de registro Generación de alertas y recomendaciones - POST TEST
Título de la investigación:	DESARROLLO DE APLICATIVO MÓVIL PARA LA DETECCIÓN DE PHISHING EN MENSAJES DE TEXTO (SMS) DE DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID
Autor de la investigación:	Pablo Fernando Flores Barrios

II. ASPECTOS DE LA EVALUACION

INDICADORES	CRITERIOS	DEFICIENTE 0-20%	REGULAR 21 - 50%	BUENO 51 - 70%	MUY BUENO 71 - 85%	EXCELENTE 85-100%
ADECUACION	Muestra adecuada para medir el producto y variables.					90
CLARIDAD	Presentación con lenguaje pertinente y claro.				75	
COHERENCIA	Presenta coherencia en el procedimiento.					90
CONSISTENCIA	Basado en aspectos teóricos científicos.					90
METODOLOGIA	Cumple con el proposito de la investigacion.					90
OBJETIVIDAD	Se demuestra de forma objetiva.					90
ORGANIZACIÓN	Presentación ordenada.					90
PERTINENCIA	Muestra adecuada para con los objetivos.					90
SIGNIFICATIVIDAD	La muestra es util para la investigación.					90
SUFICIENCIA	Cantidad de información suficiente para cumplir con los objetivos.					90

III: PROMEDIO DE LA EVALUACIÓN: 88.5

Firma:

Apéndice AM. Ficha de de registro - Corrección funcional

TEST DE VALIDACION CORRECCION FUNCIONAL

ITEM	FUNCIONALIDAD DEL APLICATIVO	OBJETIVO AL QUE APORTA	ESTADO
1	SE CONECTA CON SERVIDOR LOCAL	OBJETIVO ESPECIFICO 2	VALIDADO
2	DETECTA PHISHING EN SMS	OBJETIVO ESPECIFICO 2	VALIDADO
3	VALIDA PHISHING CON BASE DE DATOS	OBJETIVO ESPECIFICO 2	VALIDADO
4	REGISTRA USUARIOS	OBJETIVO ESPECIFICO 1	VALIDADO
5	GENERA RECOMENDACIONES ANTIPHISHING	OBJETIVO ESPECIFICO 1	VALIDADO
6	LEE DE FORMA AUTOMATICA LOS SMS ENTRANTES	OBJETIVO ESPECIFICO 2	VALIDADO
7	PRESENTA EN PANTALLA DE FORMA AUTOMATICA EL RESULTADO DE LA VALIDACION DE PHISHING	OBJETIVO ESPECIFICO 2	VALIDADO
8	LAS ALERTAS SIEMPRE SON GENERADAS DE FORMA AUTOMATICA AL DETECTAR UN MENSAJE NUEVO	OBJETIVO ESPECIFICO 3	VALIDADO
9	GENERA ALERTAS DE DETECCION DE PHISHING	OBJETIVO ESPECIFICO 3	VALIDADO
10	GENERA ALERTAS DE NO CONEXIÓN CON LA BASE DE DATOS	OBJETIVO ESPECIFICO 3	VALIDADO
11	GENERA ALERTAS DE CONEXIÓN CON BASE DE DATOS	OBJETIVO ESPECIFICO 3	VALIDADO
12	PRESENTA EN PANTALLA DE FORMA AUTOMATICA EL MENSAJE Y NÚMERO ENVIADA POR EL EMISOR	OBJETIVO ESPECIFICO 3	VALIDADO

Apéndice AN. Ficha de de registro - Pertinencia funcional

TEST DE VALIDACION PERTINENCIA FUNCIONAL

ITEM	FUNCIONALIDAD DEL APLICATIVO	PERFIL DE USUARIO	ESTADO
1	EL APLICATIVO OCUPA POCO ALMACENAMIENTO	AUTOMÁTICO, ÁGIL Y PRÁCTICO	VALIDADO
2	EL APLICATIVO ES NATIVO PARA ANDROID		VALIDADO
3	EL APLICAIVO GENERA DE FORMA AUTOMÁTICA LAS ALERTAS		VALIDADO
4	EL APLICATIVO LEE DE FORMA AUTOMÁTICA LOS MENSAJES SMS		VALIDADO
5	EL APLICATIVO DETECTA DE FORMA AUTOMÁTICA EL PHISHING		VALIDADO
6	EL APLICATIVO PRESENTA DE FORMA AUTOMÁTICA LA VALIDACIÓN DE PHISHIN		VALIDADO
7	EL APLICATIVO SOLO PIDE UN REGISTRO INICIAL AL USUARIO.		VALIDADO
8	EL APLICATIVO DEMORA MENOS DE 2 SEGUNDOS EL PROCESO DE VALIDACIÓN Y GENERACIÓN DE ALERTA DE PHISHING		VALIDADO
9	EL APLICATIVO MUESTRA EL MENSAJE Y NÚMERO DEL EMISOR DEL SMS DE FORMA AUTOMÁTICA.		VALIDADO
10	EL APLICATIVO TRABAJA EN SEGUNDO PLANO.		VALIDADO
11	EL APLICATIVO NO REQUIERE AUTENTICACIÓN.		VALIDADO