Plataforma Web para entrenamiento de ataques de Phishing mediante seguridad y psicología cognitiva

Arévalo Briceño, Diana Anabel y Valarezo Bracho, Darío Ismael

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Trabajo de Integración Curricular, previo a la obtención de título de Ingeniero/a en Tecnologías de la Información

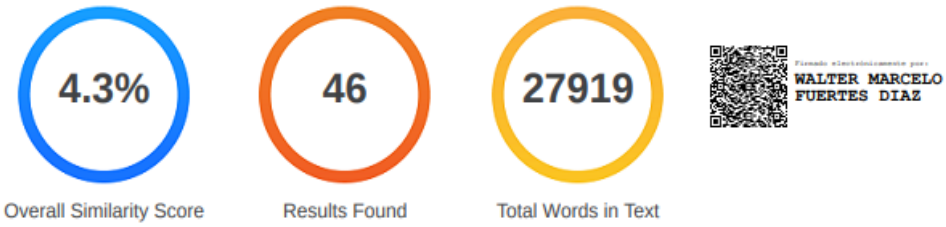
Ing. Fuertes Díaz, Walter Marcelo, PhD

11 de agosto del 2022

COPYLEAKS

Tesis_Arévalo_Valarezo.docx

Scanned on: 21:1 August 11, 2022 UTC



Identical Words	671
Words with Minor Changes	344
Paraphrased Words	0
Omitted Words	4219

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Certificación

Certifico que el trabajo de integración curricular: "**Plataforma Web para entrenamiento de ataques de Phishing mediante seguridad y psicología cognitiva**" fue realizado por la señorita **Arévalo Briceño, Diana Anabel** y el señor **Valarezo Bracho, Darío Ismael,** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 11 de agosto de 2022

Firmado electrónicamente por:
WALTER MARCELO
FUERTES DIAZ

.....

Fuertes Díaz, Walter Marcelo, PhD

C. C 1707017701

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Responsabilidad de Autoría

Nosotros, **Arévalo Briceño, Diana Anabel**, con cédula de ciudadanía N° 1150409397 y **Valarezo Bracho, Darío Ismael**, con cédula de ciudadanía N° 1719314179, declaramos que el contenido, ideas y criterios del trabajo de integración curricular: **Título: Plataforma Web para entrenamiento de ataques de Phishing mediante seguridad y psicología cognitiva,** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 11 de agosto de 2022

.....

Arévalo Briceño Diana Anabel

C.C.: 1150409397

.....

Valarezo Bracho Darío Ismael

C.C.: 1719314179

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Autorización de Publicación

Nosotros **Arévalo Briceño, Diana Anabel**, con cédula de ciudadanía N° 1150409397 y **Valarezo Bracho, Darío Ismael**, con cédula de ciudadanía N° 1719314179, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de integración curricular: **Título: Plataforma Web para entrenamiento de ataques de Phishing mediante seguridad y psicología cognitiva,** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 11 de agosto de 2022

.....

Arévalo Briceño Diana Anabel

C.C.: 1150409397

.....

Valarezo Bracho Darío Ismael

C.C.: 1719314179

DEDICATORIA

El presente trabajo de titulación se lo dedico con todo mi amor a Dios, y a mi querida familia en especial a mi madre Maritza, a mi padre José, a mis hermanos Cristhian y Karen por ser un soporte fundamental en mi vida, por apoyarme en cada momento y confiar en mí. Gracias por enseñarme que en esta vida todo se consigue con humildad, esfuerzo y sacrificio.

A mis familiares, especialmente a mi abuelita Lola, tío Isidro, tía Rosa y primo Steven, por cada uno de sus consejos, por estar siempre presentes e impulsarme para que salga adelante en mis propósitos.

A mis compañeros y amigos, quienes me brindaron su apoyo, amistad y me vieron crecer a lo largo de este proceso.

Finalmente, se la dedico a todas las personas que estuvieron presentes en toda esta etapa de formación profesional, ya que colaboraron de una u otra manera para que este logro se vea cristalizado.

Diana Arévalo.

Todo lo que he conseguido se lo dedico a mi Madre, Padre y Hermano que fueron los que han estado siempre conmigo apoyándome día a día, y todo sin pedir nada a cambio. Ellos son un pilar importante en mi vida, tanto que han formado mi vida para que sea una persona con principios sólidos y que siempre tenga perseverancia en realizar las cosas hasta conseguirlas.

Gracias al cariño y a los consejos que ellos me han brindado he logrado obtener la mejor versión de mí. Los amo con toda mi vida.

También se la dedico a todas las personas que no creen en sí mismo. Quiero que sepan que, trabajando día a día, paso a paso, llegará el momento donde puedan decir que lo consiguieron y cuando eso ocurra será uno de los mejores días de su vida.

Darío Valarezo.

AGRADECIMIENTO

Primeramente, quiero agradecer a Dios y a la Virgen Santísima por guiarme en cada momento, por darme la vida, la salud y no dejarme caer a pesar de las circunstancias. Agradezco infinitamente a mis padres, en especial a mi mamá Maritza, que con su cariño y trabajo me educaron y apoyaron a lo largo de mis estudios, por crear en mí una persona humilde y perseverante. A mis queridos hermanos Cristhian y Karen, por su apoyo incondicional y anhelar siempre lo mejor para mi vida, gracias por ser mi motor y ejemplo de superación.

A la Universidad de las Fuerzas Armadas ESPE, por darme la oportunidad de formarme profesionalmente en sus aulas y conocer personas maravillosas. A mis docentes universitarios, en especial al Ing. Walter Fuertes, por sus enseñanzas, consejos, por la confianza y por brindarme la oportunidad de participar en sus proyectos de investigación. A la Dra. María Fernanda Cazares, por su guía y apoyo, gracias por la estima y colaboración en el desarrollo de este proceso investigativo.

A mi compañero de titulación y amigo Darío, por su apoyo y perseverancia en el desarrollo del presente estudio y por brindarme su amistad absoluta en cada momento.

Gracias a mis amigos en especial a Omar, Carlos, Daniel, Carolina, por creer en mí y brindarme siempre su motivación. De igual manera a Cristhian S., por su apoyo incondicional.

Gracias infinitas a todas y cada una de las personas que contribuyeron y formaron parte de este proceso en mi vida, el cual me deja muchas experiencias vividas y la satisfacción del deber cumplido.

Diana Arévalo.

En primer lugar, quiero agradecer a mis padres, que significan mucho para mí.

A mi madre Cecilia que es la persona que ha estado conmigo siempre y la que me ha dado todo su apoyo y cariño cuando más lo he necesitado, estaré eternamente agradecido por ser la persona que eres conmigo, te amo mucho mami.

A mi padre Antonio que admiro muchísimo, gracias por no dejarme solo y por los consejos que siempre me da, es mi ejemplo a seguir.

También agradezco a mi hermano Antony, eres muy importante para mí. Gracias por ser buena persona conmigo y siempre ayudarme cuando te lo pido.

A la maravillosa Universidad de las Fuerzas Armadas ESPE, por todas las vivencias que he pasado, por las excelentes personas que he conocido ahí y el conocimiento brindado.

A mis docentes universitarios, sobre todo al Ing. Walter Fuertes por confiar en mi para participar en sus proyectos, gracias por la oportunidad. A la Dra. María Fernanda Cazares por brindarnos su ayuda y guía a conseguir los objetivos de este presente trabajo.

A mi amiga de trabajo de titulación Dianita, por ser una excelente persona conmigo y siempre apoyarnos mutuamente cuando más lo necesitamos.

A mis amigos, sobre todo a los de la universidad por todo lo que hemos pasado hasta llegar a cumplir la meta de graduarnos y por ser una parte importante en mi vida, especialmente a Omar, Carlos y Daniel por ser buenos amigos.

A Nickol por ser incondicional conmigo.

Darío Valarezo.

Contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

En la actualidad se vive un proceso pos pandémico en el que el auge de los ataques de Ingeniería Social especialmente tipo Phishing, se aprovechan del eslabón más débil de la ciberseguridad que es el ser humano. Los usuarios están ahora expuestos constantemente en Internet y al uso de dispositivos electrónicos por lo que son susceptibles a este tipo de ataques. El objetivo del presente estudio es desarrollar una plataforma web para entrenamiento de ataques de Phishing en correos electrónicos mediante la utilización de metodologías ágiles, al combinar seguridad y psicología cognitiva. Para el cumplimiento del mismo, se utilizaron los lineamientos de la metodología de diseño de la ciencia. Así mismo, para la revisión de literatura se aplicó la guía metodológica de Bárbara Kitchenham, cuyos resultados indican que una manera de implementar seguridad cognitiva es mediante la aplicación de teorías de juego. Por esta razón, se diseñó e implementó un algoritmo con teorías de juego capaz de clasificar por el nivel de conocimiento para el proceso de entrenamiento de los usuarios en la plataforma web, la cual se desarrolló mediante la metodología ágil SCRUM. Los resultados del entrenamiento revelan que, en una población de 59 usuarios, entre ellos 33 estudiantes y 26 profesionales, los profesionales según su score fueron en su mayoría por los caminos establecidos como difíciles, es decir tuvieron una alta tasa de éxito y por ende una alta detección. Por el contrario, los estudiantes fueron por los caminos intermedios y difíciles, con un nivel de detección media. Cabe recalcar que se realizó un análisis del nivel de detección por la edad y género. Por otra parte, se implementó en la plataforma un cuestionario de percepción de riesgo con el fin de obtener el nivel de percepción de los usuarios. No obstante, este es un primer pilotaje para lograr su validación a nivel psicológico.

Palabras clave: Phishing, seguridad cognitiva, psicología cognitiva, percepción de riesgo.

Abstract

We are currently experiencing a post-pandemic process in which the rise of social engineering attacks, especially phishing attacks, are taking advantage of the weakest link in cybersecurity, which is the human being. Users are constantly exposed to the Internet and electronic devices and are therefore susceptible to this attack. This study aims to develop a web platform for training Phishing attacks in emails using agile methodologies, combining security and cognitive psychology. For the fulfillment of the same, we used the guidelines of the Design Science methodology. Likewise, for the literature review, Barbara Kitchenham's methodological guide was applied, whose results indicate that one way to implement cognitive security is by using game theories. For this reason, an algorithm with game theories capable of classifying by knowledge level was designed and implemented for the user training process on the web platform, which we developed using the agile SCRUM methodology. The training results reveal that, in a population of 59 users, including 33 students and 26 professionals, the professionals, according to their score, mainly went through the paths established as complex, i.e., they had a high success rate and therefore a high detection. On the contrary, the students went through the intermediate and challenging paths with a medium detection level. We should emphasize that we perform an analysis of the level of detection by age and gender. On the other hand, a risk perception questionnaire was implemented on the platform to obtain the users' level of perception. However, this is the first pilot to achieve its validation at a psychological level.

Keywords: Phishing, cognitive security, cognitive psychology, risk perception.

Capítulo I

Aspectos Generales

Antecedentes

El crecimiento de las tecnologías ha sido considerable en los últimos años, el estudio de (Kemp, 2022) menciona que los usuarios de Internet en todo el mundo ascendieron a 4950 millones a principios de 2022 que ahora representa el 62,5 % de la población total del mundo. Los datos indican que los usuarios de Internet han crecido en 192 millones (+4,0 por ciento) durante el año pasado. Sin embargo, las restricciones actuales a la investigación y los informes debido al COVID-19 significan que las tendencias de crecimiento reales pueden ser considerablemente más altas de lo que sugieren estas cifras.

Cada vez, los ciberdelincuentes obtienen acceso a través de la ingeniería social, de tal forma que convencen a los usuarios para que permitan instrucciones sin saberlo. La forma más común de ingeniería social son los ataques de Phishing, en los que el agresor se disfraza de persona de confianza (*Brief*, 2021), tiene como objetivo manipular a las personas y alentarlas a exponer su información confidencial. Los métodos y técnicas más comunes utilizados para el Phishing son correos electrónicos, chats o sitios web (A Younis & Musbah, 2020) . El hecho de que nuestras formas de vivir, estudiar y trabajar hayan cambiado drásticamente como resultado de la pandemia de COVID ha creado muchas nuevas preocupaciones de seguridad cibernética, en particular, ha aumentado la cantidad de correos electrónicos de Phishing que amenazan a los empleados (Carroll et al., 2022).

Los ciberdelincuentes se aprovechan del enorme potencial de error humano dentro de cualquier negocio, donde un clic accidental en un correo electrónico de Phishing puede permitir el acceso a redes corporativas completas, un error costoso de cometer.

Con estos precedentes, una forma de mitigar los ataques de ingeniería social es hacer

hincapié en la educación y la formación de las personas más susceptibles a los ataques de ingeniería social (Sumner & Yuan, 2019). La identificación de los usuarios más vulnerables para orientarlos hacia programas de formación es deseable para aumentar la eficacia de los mismos (Albladi & Weir, 2020). Si bien la tecnología tiene un papel que desempeñar en la reducción del impacto de los ataques de ingeniería social, la vulnerabilidad reside en el comportamiento humano, los impulsos humanos y las predisposiciones psicológicas. De la misma forma, la literatura respalda los peligros de las susceptibilidades psicológicas en los ataques de ingeniería social, la inversión en campañas de educación organizacional ofrece optimismo de que los ataques de ingeniería social pueden reducirse (Conteh & Schmick, 2021).

Problemática

El Phishing continúa como un problema tanto para individuos como para organizaciones con miles de millones de dólares perdidos cada año (Nicholson et al., 2017). El predominio y la eficacia de los ataques de Phishing, a pesar de la presencia de una amplia gama de técnicas de defensa, se deben en gran medida al hecho de que los atacantes se dirigen despiadadamente al que denominan el eslabón más débil del sistema: el ser humano (Williams & Li, 2017). Los correos electrónicos exitosos emplean armas psicológicas de influencia y dominios de vida relevantes (Oliveira et al., 2017).

Los correos electrónicos de Phishing constituyen un significativo problema de salud pública, relacionado con resultados sanitarios negativos debidos al fraude y la explotación (Hakim et al., 2019). Así mismo, el aumento de la sofisticación de los ataques de Phishing supone miles de millones de dólares en pérdidas financieras, pérdida de propiedad intelectual y daños a la reputación de las organizaciones (Tian & Jensen, 2019).

En el artículo de (Cui et al., 2017) monitorearon un total de 19,066 ataques de Phishing durante un período de diez meses y descubrieron que más del 90% de estos ataques eran en realidad réplicas o variaciones de otros ataques en la base de datos existentes en Internet.

Entre febrero y marzo de 2020, mientras las organizaciones se apresuraban a permitir que sus empleados trabajaran desde casa durante la primera ola de la pandemia, la cantidad de correos electrónicos de Phishing aumentó en un asombroso 667 %, ya que los atacantes no perdieron tiempo en capitalizar sobre el período del miedo y la incertidumbre (Jones, 2021).

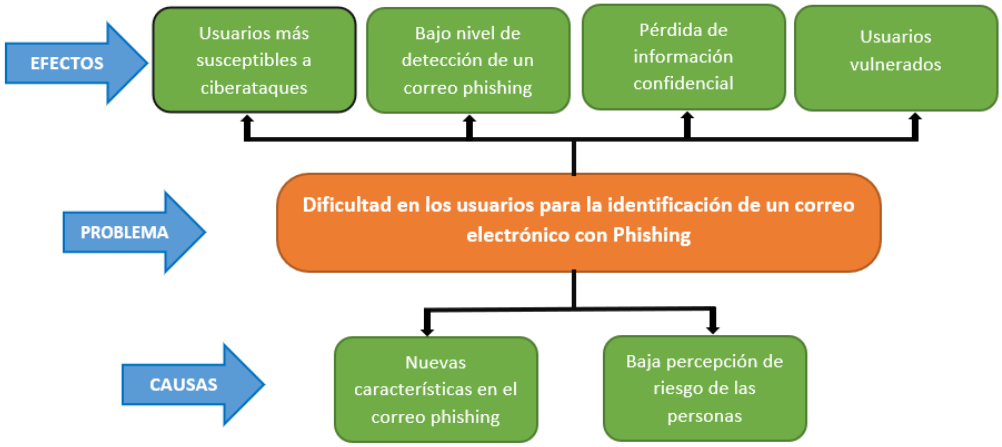
En el 2021, la investigación de Tessian (Rosenthal, 2022) descubrió que los empleados reciben un promedio de 14 correos electrónicos maliciosos por año. Algunas industrias se vieron particularmente afectadas, y los trabajadores minoristas recibieron un promedio de 49. La investigación de ESET de 2021 (ESET, 2021) encontró un aumento del 7,3 % en los ataques basados en correo electrónico entre mayo y agosto de 2021, la mayoría de los cuales formaban parte de campañas de Phishing. El informe de tendencias de amenazas de seguridad cibernética de 2021 de CISCO (Cisco, 2021) sugiere que al menos una persona hizo clic en un enlace de Phishing en alrededor del 86% de las organizaciones. Los datos de la empresa indican que el Phishing representa alrededor del 90% de las filtraciones de datos.

Así mismo, la investigación de IBM en el 2022 (IBM, 2022) confirma que el Phishing fue el principal vector de infección de 2021, y las marcas más imitadas en los kits de Phishing se encuentran entre las empresas más grandes y confiables: Microsoft, Apple y Google.

A continuación, en la Figura 1 se presenta el árbol de problemas del presente tema, en donde se ilustra el problema con sus respectivas causas y efectos.

Figura 1

Árbol de problemas



Nota. La Figura detalla las causas, problemas y efectos en el árbol de problema

Es por esta razón, que el presente trabajo de investigación propone una plataforma web para entrenamiento de ataques de Phishing mediante la combinación de seguridad y psicología cognitiva. Con el propósito de ayudar a los usuarios a tener una buena percepción de riesgo de estos ataques en correos electrónicos y coadyuvar a su capacidad de detectarlos a tiempo.

Formulación del Problema

¿Es factible desarrollar una plataforma web para realizar entrenamiento de ataques de Phishing que permita detallar la percepción de riesgo y la capacidad de detección de correos con Phishing de las personas?

Justificación

En el mundo actual, lo digital está totalmente inmerso en la sociedad. Esto conlleva a grandes retos, ya que la gente tiende adoptar esta forma de vida y todas sus nuevas tecnologías en un proceso de pandémico como fu el COVID19 (Carroll et al., 2022).

Las organizaciones y los usuarios a pesar de las salvaguardas técnicas que establecen ante los ataques cibernéticos, tales como ransomware, malware, Phishing, vishing, etc., son los mismos usuarios los que toman muchas decisiones críticas de seguridad. Sin embargo, los ataques de Phishing requieren una comprensión de los aspectos cognitivos humanos que son explotados por los delincuentes cibernéticos, ya que los métodos de defensa actuales no abordan adecuadamente el factor humano de esta amenaza, de tal forma que los atacantes mediante el correo electrónico logran victimizar a su objetivo. Es por esta razón que las empresas y la academia se motivan a la búsqueda de soluciones a través de la seguridad y psicología cognitiva.

Justificación Teórica

Primera parte: diseñar los correos electrónicos de Phishing en la plataforma web. Para el diseño se planea buscar las tácticas, temas, características y componentes de los correos electrónicos infectados con Phishing en repositorios de datos actuales, así mismo se busca en correos reales para tener un número significativo de 20 ejercicios que simulen correos con Phishing y correos legítimos, para un óptimo entrenamiento de los usuarios. Como fuente de información, se utilizará la base de datos que ofrece Confese (Confense, 2020), la misma que es un sitio gratuito ofrece ejemplos reales y actuales de correos electrónicos con Phishing con sus respectivas clasificación y descripción. Para la programación se plantea utilizar las herramientas de Java y Angular.

Segunda parte: Implementación de un formulario para medir la percepción de riesgo de los usuarios frente ataques de ingeniería Social tipo Phishing dentro del proceso de entrenamiento en la plataforma. En este sentido, se realizará una investigación bibliografía previa para determinar un formulario con directrices de medición para cada pregunta.

Tercera parte: entrenamiento de los usuarios en la plataforma web. Se pretende implementar seguridad cognitiva en el proceso de entrenamiento del usuario, en este sentido se desarrolla un algoritmo mediante teorías de juego con árboles de decisión que seleccione la dificultad de los ejercicios con respecto al resultado del score del usuario en cada una de los caminos asignados.

Justificación práctica

El proyecto está encaminado a las empresas, academia y sociedad en general del Ecuador que deseen realizar capacitaciones o entrenamiento a los usuarios permitiéndoles medir su nivel de percepción y así mismo aumentar la capacidad de detección de correos electrónicos de Phishing, de tal manera que se pueda prevenir la pérdida de información mediante este ataque.

Objetivos

Objetivo General

Desarrollar una plataforma web para entrenamiento de ataques de Phishing en correos electrónicos mediante la utilización de metodologías ágiles, al combinar seguridad y psicología cognitiva

Objetivos específicos

- Investigar las técnicas, métodos y herramientas actuales con seguridad y psicología cognitiva donde se involucra al factor humano para realizar detección de Phishing a través de la guía metodológica de Bárbara Kinchenham.
- Desarrollar el Back-End de la plataforma web mediante el framework Spring boot en el marco de la arquitectura orientada a microservicios y aplicación de las metodologías ágiles.

- Desarrollar el Front-End web de la plataforma, de manera que se cumplan los requerimientos funcionales del sistema.
- Desplegar la plataforma web donde se pueda explorar y recolectar datos sobre el comportamiento de los usuarios ante ataques de Phishing.
- Evaluar y realizar un análisis cognitivo de los datos obtenidos del comportamiento del usuario ante ataques de phishing e identificar los factores que influyen en la persona para tomar dicha elección.

Alcance

El presente proyecto comprende diseñar y desarrollar una plataforma web de entrenamiento de ataques tipo Phishing en correos electrónicos. Esta plataforma será desarrollada con el framework Spring Boot y Angular, para un adecuado manejo de las partes técnicas de la plataforma y por ende una óptima interacción de la plataforma con los usuarios. Los ejercicios simulados de Phishing que se presentarán serán caracterizados por las tácticas, temas relevantes de la actualidad y el tipo de URL. Por otro lado, se va a medir la percepción de riesgo de las personas al realizar el entrenamiento, para esto se implementará un cuestionario desarrollado por la experta en psicología. Para la seguridad cognitiva se realizará un algoritmo aplicando teorías de juego que permita a la plataforma mostrar los ejercicios con respecto a las respuestas del usuario por caminos.

Capítulo II

Marco Conceptual y Estado del Arte

Marco Conceptual

Seguridad de la Información

Al tener en cuenta el progreso tecnológico paralelo de los atacantes malintencionados y los beneficios del fraude, la seguridad de la información es un campo de investigación en continua evolución con interés práctico para el mundo empresarial (Spanos & Angelis, 2016).

Varios autores han definido la seguridad de la información de diferentes formas con diversos descriptores. Sin embargo, en todas las definiciones prevalecen tres descriptores clave: confidencialidad, integridad y disponibilidad (CIA). La seguridad de la información se ha convertido en una cuestión que ninguna empresa puede ignorar; por tanto, las cuestiones no técnicas deben recibir la misma atención que las técnicas (Amankwa et al., 2014).

Según (von Solms & van Niekerk, 2013) en la seguridad de la información, la referencia al factor humano generalmente se relaciona con el rol o roles de los humanos en el proceso de seguridad. Sin embargo, en la ciberseguridad este factor tiene una dimensión adicional al tratar a los humanos como posibles objetivos de los ciberataques e incluso participar sin saberlo en un ataque cibernético.

De igual manera un término significativo dentro de la seguridad de la información es la formación en seguridad de la información (TSI), la cual se define como todo lo que se lleva a cabo para garantizar que los empleados tengan conocimientos de la seguridad de la información y de las responsabilidades que esto conlleva, mediante el uso de métodos de instrucción práctica, como seminarios y talleres (Amankwa et al., 2014). Las organizaciones deben contar con programas de TSI para todos los empleados, ya que estos tienen funciones y responsabilidades en asegurar los activos de información de una organización.

Ataques de Ingeniería Social

Los ataques de Ingeniería social con el paso de los años se han convertido en uno de los más amenazantes del mundo digital que sufren las empresas, entidades financieras, instituciones educativas, entre otras, y más aún en una época de COVID-19 en la que se utiliza constantemente el Internet para actividades diarias, ya sea para el trabajo, educación, salud, etc.

Estos ataques tienen como objetivo engañar a las personas o empresas para que realicen acciones que beneficien a los atacantes o les proporcionen datos confidenciales, como el número de seguro social, los registros de salud y las contraseñas (Salahdine & Kaabouch, 2019).

La mayoría de las causas están relacionadas con el comportamiento humano, como la inocencia, la inconsciencia y la falta de entrenamiento o capacidad. Además, las redes sociales y el correo electrónico son las principales fuentes desde las que se producen los ataques. Phishing y Ransomware son los ataques más significativos a empresas y personas naturales (Fuertes et al., 2022).

Ataques de phishing por correo electrónico

El phishing es la combinación de ingeniería social y métodos técnicos para convencer al usuario de que revele sus datos personales, generalmente se lleva a cabo mediante la suplantación de identidad por correo electrónico o mensajería instantánea. Se dirige al usuario que no tiene conocimiento sobre ataques de ingeniería social y seguridad en Internet, como personas que no cuidan la privacidad de los detalles de sus cuentas como Facebook, Gmail, cuentas de bancos de crédito y otras cuentas financieras (Gupta et al., 2016).

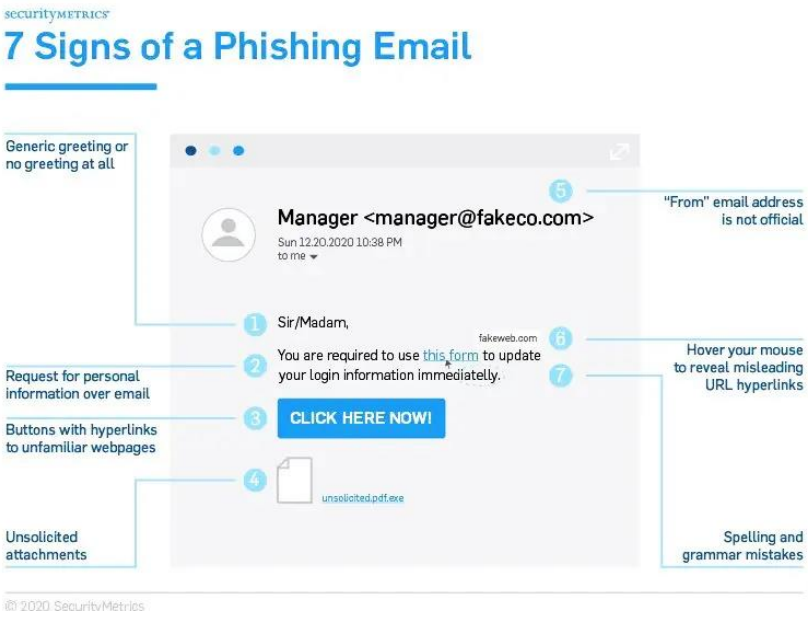
Los ataques de phishing por correo electrónico son una de las mayores amenazas de seguridad cibernética de nuestro tiempo y aumentan exponencialmente año tras año. De

manera alarmante, se ha visto que los ataques de correos electrónicos de phishing aumentaron casi un 700 % en comparación con el año pasado (Burke, 2021).

A menudo los phishers atacan a empresas e individuos a través de correos electrónicos diseñados para parecer que provienen de un banco legítimo, una agencia gubernamental o una organización, en estos, el remitente solicita a los destinatarios que hagan clic en un enlace que se redirige a una página donde corroboran datos personales, información de la cuenta, etc. En el estudio realizado por (Ellis, 2020) se indica que las solicitudes de información personal, saludos genéricos, ausencia de saludos, faltas de ortografía, direcciones de correo electrónico "de" no oficiales, páginas web desconocidas e hipervínculos engañosos son los indicadores más comunes de un ataque de phishing, como se observa en la Figura 2.

Figura 2

Indicadores de un ataque común de phishing por correo electrónico



Nota. El gráfico indica las señales de un correo electrónico de phishing. Tomado de (Ellis, 2020).

Para diferenciar un correo electrónico legítimo y un correo electrónico de Phishing es necesario comprender que las empresas legítimas:

- No solicitan su información confidencial por correo electrónico.
- Suelen llamar al usuario por el nombre.
- Tienen correos electrónicos de dominio.
- Saben cómo se escribe, no tienen mala gramática.
- No le obligan al usuario a visitar un sitio web.
- No envían archivos adjuntos no solicitados.
- Los enlaces coinciden con URL legítimas.

Por otra parte se pueden establecer defensas que ayuden a prevenir o mitigar este tipo de ataques, de acuerdo con (Chaudhry et al., 2016) para la educación de los usuarios las tecnologías adecuadas y la ingeniería de procesos, serían las alternativas:

- ***Educación del usuario:*** las habilidades analíticas del usuario al utilizar los canales de comunicación electrónicos tienen un lugar fundamental en el reconocimiento de los ataques de phishing, se hace un hincapié en la formación y la educación del usuario. Dado que los ataques de phishing normalmente se dirigen a varios usuarios de la misma o de diferentes organizaciones, compartir los conocimientos para alertar a otros de los ataques de phishing se convierte en una cuestión importante como el propio reconocimiento del ataque.
- ***Software/mejora tecnológica:*** En el mercado se comercializan varios programas informáticos contra los ciberataques como el spam, malware, ataque de denegación de servicios, etc., que afirman tener un alto índice de éxito en el filtrado y bloqueo de los mismos, no obstante, el entorno del phishing actualmente es complejo.

- ***Ingeniería de procesos:*** Los procesos empresariales deben diseñarse de forma que se mantengan los controles y equilibrios adecuados y que el juicio informado del usuario esté respaldado por el apoyo a nivel de proceso, múltiples controles en una cadena de mando distribuida, verificación en línea y fuera de línea, aplicación de la cadena de suministro preventiva, etc.

Tácticas de Phishing

La base de datos de Phishing (Confense, 2020) que otorga ejemplos reales de ataques de Phishing por correo electrónico mencionan que la mayoría de los ataques encajan en tres categorías:

Correos electrónicos de phishing con enlaces maliciosos: a menudo, un ataque de phishing es simplemente un correo electrónico con un enlace incrustado. Es así que, al hacer clic sin saberlo se activan malwares o el enlace se dirige a una página web que parece perfectamente legítima que está diseñada para recopilar la información.

Ataques de phishing con archivos adjuntos maliciosos: los phishers a menudo envían correos electrónicos con archivos adjuntos que contienen malware o mensajes que incitan al usuario hacer clic en enlaces. Muchas veces, usan tipos de documentos populares como Microsoft Word, Excel o incluso Adobe PDF y se aprovechan de la confianza que la gente deposita en las herramientas comerciales populares.

Compromiso de correo electrónico comercial (BEC): los correos electrónicos BEC, también conocidos como fraude de CEO, generalmente no usan malware, sino que simplemente intentan manipular al objetivo para que envíe dinero. Tradicionalmente, los ataques de phishing de BEC intentan que los empleados del departamento de finanzas autoricen transferencias bancarias, por ejemplo, a un "proveedor" o "socio".

Adicionalmente, esta base de datos clasifica los ejemplos reales de Phishing por las tácticas que actualmente utilizan los ataques en los correos electrónicos. A continuación se menciona unas de estas (Confense, 2020) :

- Enlace
- Adjunto HTML:
- Adjunto DOCX
- Archivo Adjunto EXE
- Archivo Adjunto PDF
- Adjunto ISO
- Adjunto XLS
- Archivo adjunto ZIP
- Adjunto XLSX
- Adjunto RAR
- BEC
- Adjunto TAR.LZ

Tipos URLs utilizadas en Phishing

No todos los usuarios de tecnología son iguales, algunos tienen más conocimientos sobre cuestiones de seguridad y otros se lo piensan más antes de hacer clic en un enlace sospechoso. Unos pueden recibir formación o capacitación en el trabajo, sin embargo, la mayoría de los usuarios de Internet no tienen conocimiento alguno.

Los phishers para engañar a sus víctimas utilizan una variedad de tipos de URLs (Localizador de recursos uniforme), es así que, en el estudio de (Pearson et al., 2017) mencionan cuatro tipos de discrepancias que se encuentran a menudo en las URL:

- ***El texto adicional***: puede describirse como una URL con demasiados o caracteres adicionales, por ejemplo wwww.google.com.
- ***Texto manipulado***: las URLs incluyen números, textos o caracteres especiales para engañar al usuario, por ejemplo www.goog1e.com, en la que se utiliza el número uno para sustituir la "L" minúscula de Google.
- ***Las combinaciones de manipulación***: hacen uso de múltiples tácticas para engañar al usuario, por ejemplo, www.google.corn. En este ejemplo, la "r" y la "n" se utilizan para formar la "m" de .com. Además, el tamaño de la letra de la "r" y la "n" se ha cambiado.
- ***La ofuscación***: describe el proceso de ocultar una URL maliciosa detrás de una URL legítima, por ejemplo www.google.com (hay una URL maliciosa escondida detrás de este hipervínculo que puede verse si se pasa el ratón por encima del enlace antes de hacer clic en él).

El phishing siempre se centra en los enlaces en los que se supone que debe hacer clic. Por otro lado, existen algunas formas de verificar si un enlace que alguien le envió es legítimo (McAfee, 2021) como lo son:

- El usuario debe pasar el cursor sobre el enlace en el correo electrónico para mostrar su URL. A menudo, las URLs de phishing contienen errores ortográficos, que es un signo común de phishing. Al pasar el cursor sobre el enlace, podrá ver una vista previa del enlace. Si la URL parece sospechosa, no se debe interactuar con ella y se debe elimina el mensaje por completo.
- El usuario debe hacer clic derecho en el enlace, copiar y pegar la URL en un procesador de textos. Esto permitirá examinar el enlace minuciosamente en

busca de errores gramaticales o de ortografía sin ser dirigido a la página web potencialmente maliciosa.

- Si la URL que se descubre no coincide con la entidad que supuestamente envió el mensaje, probablemente el usuario recibió un correo electrónico de phishing.

Seguridad cognitiva

La seguridad cognitiva se refiere a las prácticas, metodologías y esfuerzos realizados para defenderse de los intentos de ataques de ingeniería social. Sin embargo, la seguridad cognitiva, en contextos de seguridad cibernética, generalmente se refiere a la aplicación de tecnologías de inteligencia artificial y aprendizaje automático que se basan en la cognición humana para la detección de amenazas de seguridad.

((R. Andrade & Torres, 2018) la definen como “la capacidad de generar cognición para la toma de decisiones eficientes en tiempo real por parte del humano o de un sistema informático, a partir de la percepción de ciberseguridad que el sistema informático genera de su entorno y del conocimiento sobre sí mismo, mediante el análisis de cualquier tipo de información (estructurada o no estructurada) a través de técnicas de inteligencia artificial (data mining, machine learning, natural language processing y human-computer interaction) y de análisis de datos (bigdata, procesos estocásticos, teoría de juegos) de forma que simula el proceso de pensamiento para el aprendizaje continuo, la toma de decisiones y el análisis de seguridad”.

Por otro lado, para hacer frente a los desafíos de seguridad, se han propuesto nuevas arquitecturas de seguridad inspiradas en la cognición que enfatizan la gestión dinámica y autónoma de la confianza. Los sistemas de seguridad cognitiva aprovechan las capacidades informáticas y de detección de los dispositivos inteligentes para analizar datos de sensores sin

procesar y aplicar técnicas de aprendizaje automático para tomar decisiones de seguridad (Zheng et al., 2016).

Los esfuerzos de seguridad cognitiva en esta área incluyen enfoques no técnicos para hacer que las personas no sean vulnerables a la manipulación, así como soluciones técnicas diseñadas para detectar datos engañosos y desinformación y evitar su difusión.

Teoría de juegos con árboles de decisión

La teoría de los juegos es la base del análisis de las decisiones en condiciones de riesgo, conflicto o cooperación entre los participantes. El método de los juegos puede utilizarse para simular la relación estratégica entre dos o más jugadores, con el objetivo de encontrar la ideal recompensa para todos ellos (Martínez et al., 2022). Al aprender los conceptos y modelos de la teoría de juegos, los responsables de la toma de decisiones pueden mejorar su comprensión de los dilemas a los que pueden enfrentarse en diferentes situaciones, de tal manera que revuelve los problemas de forma más racional (Gibson, 2003).

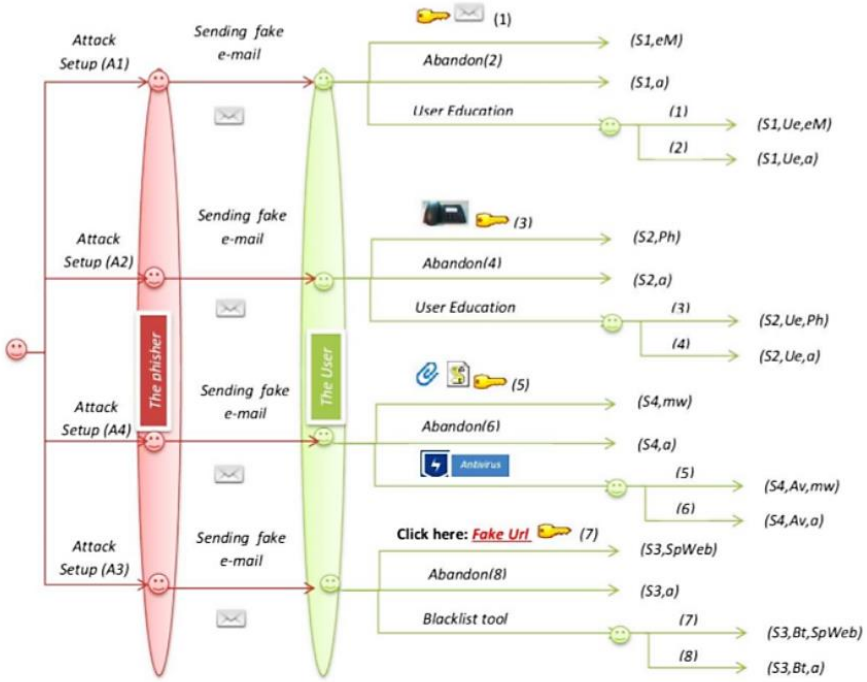
Por otro lado, de acuerdo con (Martínez et al., 2022) el árbol de decisión es un método de selección de la alternativa más adecuada en un proceso de decisión basado en varias opciones disponibles. Este método utiliza una estructura de árbol, ya que puede haber más de dos opciones disponibles, y las ramas representan los diferentes resultados y las decisiones asociadas que puede tener cada opción.

En la teoría de juegos, la forma extensiva es una forma de describir juegos mediante el uso de un árbol de juego (o árbol de decisión). Es simplemente un diagrama que detalla las decisiones que los jugadores toman en diferentes puntos en el tiempo (que corresponde a cada nodo). Los pagos finales del juego están representados en el extremo de cada rama (Policonomics, 2017) .

Hoy en día, la teoría de juegos ha cobrado un impulso significativo y sus aplicaciones se encuentran en casi todas las disciplinas principales, incluidas la economía, las ciencias políticas, la biología evolutiva, la psicología, la lógica y la informática. En el estudio de (Tchakounte et al., 2020) mencionan que la teoría de los juegos al involucrarse en el ámbito de la ciberseguridad, se aprovecha para luchar contra el phishing. Además, en su propuesta desarrollan un modelo teórico de juegos para anticipar las estrategias de Spear-Phishing en el correo electrónico, ver Figura 3.

Figura 3

Escenarios de interacción entre el atacante y el usuario en un ataque tipo Phishing.



Nota. Interacción de los escenarios y las estrategias dentro de un ataque Phishing. Tomada de (Tchakounte et al., 2020)

Psicología cognitiva

El procesamiento de la información en humanos se asemeja al de las computadoras, y se basa en transformar, almacenar y recuperar información de la memoria. Los modelos de procesamiento de información de procesos cognitivos como la memoria y la atención asumen que los procesos mentales siguen una secuencia clara.

La psicología cognitiva es el estudio científico de la mente como procesador de información. Se trata de la forma en que asimilamos la información del mundo exterior, cómo le damos sentido a esa información (McLeod, 2020).

Otra definición importante es la del diccionario médico (Merriam-Webster, s. f.) en la que la define como: “una rama de la psicología que se ocupa de los procesos mentales (como la percepción, el pensamiento, el aprendizaje y la memoria), especialmente con respecto a los eventos internos que ocurren entre la estimulación sensorial y la expresión abierta de la conducta.”

Por otro lado, existe una combinación muy acertada entre la psicología cognitiva y la ciberseguridad puesto que los psicólogos sociales pueden, a su vez, proporcionar a los expertos en ciberseguridad enfoques basados en pruebas sobre cómo predecir y, si es necesario, intentar mitigar incidentes de ciberseguridad. Así como ayudar en los desafíos metodológicos y éticos inherentes al estudio de algunos de los factores humanos de la ciberseguridad. Existen trabajos de investigación en los que adoptan estas dos partes como lo es el estudio de (Veksler et al., 2020) en el que realizaron modelos cognitivos para la ciberseguridad que fueron capaces de generar predicciones del comportamiento de atacantes y defensores, concluyen que los estudios y modelos de la cognición humana son muy valiosos para avanzar en la ciberseguridad. Del mismo modo, en el estudio de (Montañez et al., 2020) mencionan que una defensa adecuada contra los ataques cibernéticos de ingeniería social requiere una comprensión más

profunda de qué aspectos de la cognición humana son explotados por estos ataques cibernéticos, por qué los humanos son susceptibles a estos ataques cibernéticos y cómo se puede minimizar o al menos mitigar su daño. Los autores encontraron los siguientes hallazgos:

- Una alta carga de trabajo cognitivo, el estrés extremo, el bajo nivel mental, la falta de conocimiento del campo y/o la falta de experiencia previa hacen que uno sea más vulnerable a los ciberataques;
- La conciencia o el género por sí solos no reducen necesariamente la susceptibilidad de una persona a los ciberataques de ingeniería social;
- Los antecedentes culturales afectan la susceptibilidad de uno a los ciberataques de ingeniería social;
- Cuanto menos frecuentes sean los ciberataques de ingeniería social, mayor será la susceptibilidad a estos ataques.

Tener conocimiento y aplicar la psicología cognitiva a la ciberseguridad podría brindar una comprensión de estos procesos al permitir desarrollar estrategias de prevención y mitigación más informadas para abordar los crecientes desafíos que enfrentan las organizaciones dentro de la ciberseguridad (C3L Security, 2021).

Percepción de riesgo

La forma en que las personas ven los riesgos asociados a la seguridad de la información determina las decisiones que tomarán con respecto a las acciones que emprenderán (o no emprenderán) junto con las medidas de seguridad de riesgos que su organización particular haya establecido. La percepción del riesgo es un área de estudio interesante porque es una compleja combinación de factores sociales, culturales, económicos, psicológicos, financieros y política (Brooker, 1984).

Existen diferentes estudios que definen la percepción de riesgo desde las diferentes situaciones en las que se la puede encontrar, por ejemplo (Kinateder et al., 2015) la definen como un proceso psicológico que describe la evaluación subjetiva (consciente e inconsciente) (en oposición a la evaluación objetiva del riesgo) de la probabilidad de verse afectado por un evento indeseable inminente en una situación específica y una evaluación de la propia vulnerabilidad percibida y recursos de resistencia .

Así mismo, (Castillo, 2012) define la percepción de riesgo como "un proceso cognitivo que descansa en la información de cada persona acerca de diferentes cuestiones como contextos, otras personas, objetos, y que procesa de forma inmediata organizándose un juicio o valor. Podríamos añadir que ese juicio o valor condiciona su comportamiento". Mencionan que algunos de los factores que intervienen en su distribución serían los siguientes:

- Perceptivos.
- De historia personal/experiencias.
- Cantidad y calidad de la información.
- Creencias y actitudes.

Por otro lado, la percepción de riesgo en ciberseguridad se ve reflejada en el trabajo de investigación de (Albladi & Weir, 2020) ellos desarrollan un modelo novedoso para predecir la vulnerabilidad del usuario basado en varias perspectivas de las características del usuario, en sus resultados detallan que la percepción del riesgo no tiene una influencia directa en la vulnerabilidad de las personas, no obstante, encontraron que el riesgo percibido aumenta significativamente el nivel de competencia de las personas para hacer frente a los ataques de ingeniería social. En el mismo contexto (Albladi & Weir, 2018) describen que la percepción del riesgo incluye la gravedad de la amenaza y la probabilidad de la amenaza, mientras que la

competencia del usuario incluye la autoeficacia, la conciencia de privacidad, la conciencia de seguridad y la experiencia pasada.

No obstante, la presión del tiempo, la carga de trabajo y el uso de una "forma más rápida de trabajar" son algunos de los aspectos del factor humano que influyen en la participación en acciones de riesgo por parte de los empleados en las organizaciones. La falta de investigación sobre el comportamiento humano en la ciberseguridad y la seguridad de la información agrava aún más la incomprensión de la toma de decisiones humanas mientras se opera un sistema de información (Nobles, 2018).

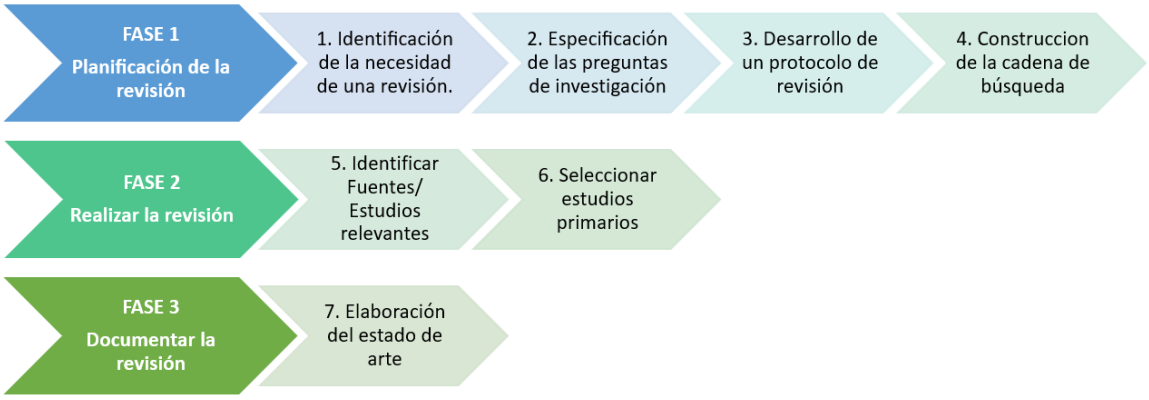
Estado del arte

Prototipos de entrenamiento de phishing con seguridad y psicología cognitiva

Para conocer el estado del arte de los prototipos de entrenamiento de phishing con seguridad y psicología cognitiva se realizó una revisión de literatura que está enfocada a los factores humanos en el tema de la percepción de riesgo de los usuarios frente a ataques de Ingeniería social, así como también las técnicas y herramientas con seguridad cognitiva utilizadas para la detección de Phishing en correos electrónicos, se la realizó mediante la metodología de Bárbara Kinchenham (Kitchenham & Brereton, 2013) . En la Figura 4 se detalla cada una de las fases.

Figura 4

Proceso de revisión de literatura científica



Nota. La figura detalla las fases de la metodología aplicada.

Planificación de la revisión

Identificación de la necesidad de una revisión

Para iniciar el proceso de búsqueda sistemática de literatura, en este literal se realizó una descripción del problema central del presente estudio de titulación y nace la necesidad de indagar la existencia de estudios de los que se pueda extraer conocimiento relevante y ayuden a alcanzar los objetivos planteados.

Especificación de las preguntas de investigación

Se plantea 3 preguntas de investigación para la revisión sistemática de literatura:

- RQ1. ¿Cuáles son las técnicas donde involucra el factor humano ante la detección de Phishing?
- RQ2. ¿Cuáles son las nuevas técnicas y herramientas de Seguridad Cognitiva en Phishing?
- RQ3. ¿Cuál es la aplicación de Psicología Cognitiva en Phishing?

Desarrollo de un protocolo de revisión

Criterios de inclusión y exclusión

Se excluyeron los artículos que no estuvieran escritos en inglés y que no estuvieran comprendidos entre 2016 y 2022. Este corte temporal sirvió para encontrar estudios importantes que determinan la percepción de riesgo de los usuarios frente ataques Phishing. Para ello, se aplicaron los siguientes criterios de inclusión:

- Artículos cuyo contenido presenten los métodos y herramientas actuales de seguridad y Psicología cognitiva donde se involucra al factor humano.
- Artículos cuyo contenido evalúe el rendimiento de prototipos, herramientas o aplicaciones.
- Artículos cuya revista de publicación o conferencias se encuentren en un cuartil Q3 o superior

Construcción de la cadena de búsqueda

Proceso de búsqueda

Las bases de datos científicas que se utilizarán en este proceso serán: ACM Digital Library (https://dl.acm.org/), IEEE Digital Library (https://ieeexplore.ieee.org/), Scopus (http://www.scopus.com), Springer (https://www.springer.com/), Google Scholar (https://scholar.google.com/).

Por otro lado, para obtener las palabras claves de nuestro proyecto se estableció los temas importantes y con relevancia al realizar una investigación previa se ha decidido que serán las siguientes: Phishing, human factors, risk perception, cognitive security and cognitive psychology, tools.

Ya identificadas las palabras claves, en este literal se procede a crear las posibles cadenas de búsqueda, en la que se encuentra las siguientes:

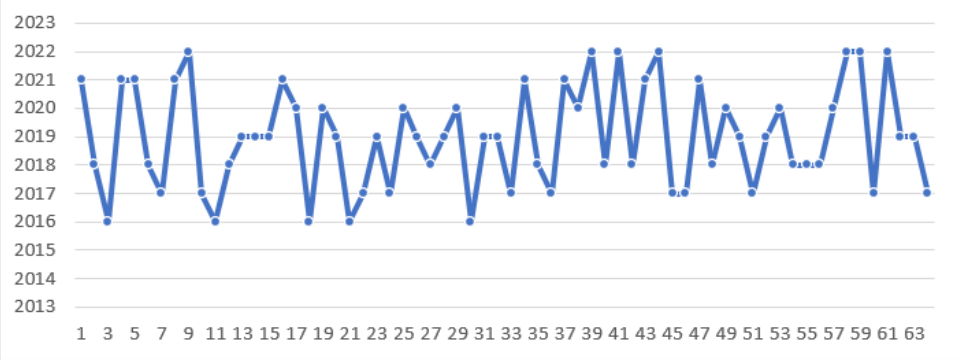
- “(Cognitive security AND phishing) OR human factors)”

- “(Cognitive security AND cognitive psychology) OR phishing)”
- “(Cognitive security AND phishing AND tools) AND human factors OR risk perception)”

Se obtiene como resultado 656 trabajos relacionados en conjunto en las bases científicas antes propuestas. En la Figura 5 se detalla los 63 artículos seleccionados y que están directamente relacionados con el tema durante el periodo de tiempo establecido.

Figura 5

Distribución de los artículos seleccionados en el intervalo de tiempo



Nota. La figura presenta los artículos encontrados y su año de publicación.

Estos estudios fueron cargados a la herramienta Rayyan (*Rayyan*, s. f.), la cual permite poseer un óptimo control de la revisión de literatura, al igual que un registro de los artículos incluidos, excluidos, duplicados, las revistas o conferencias a las que pertenecen, etc. Una parte interesante de Rayyan es que presenta un mapa con las temáticas de los trabajos encontrados, como se visualiza en la Figura 6.

Figura 6

Screenshot de Rayyan relacionada con los temas en la revisión de literatura

Nota. La figura presenta los términos que más se mencionan en los artículos seleccionados.

Realizar la revisión

Identificar fuentes o estudios relevantes

Cabe señalar los estudios que fueron publicados en revistas transcendentales, los cuales pertenecen a la siguiente distribución: SN Computer Science (Carroll et al., 2022), ACM Transactions on Social Computing (Greitzer et al., 2021), European Interdisciplinary Cybersecurity Conference (Kießling et al., 2021), Cognitive science (R. O. Andrade & Yoo, 2019), Computers in Human Behavior (Musuva et al., 2019a), IEEE Access (Alturki et al., 2020), Behavior Research Methods volume (Hakim et al., 2021).

Conforme a la RQ1., en los estudios encontrados los autores (Dixon et al., 2019) mencionan que los juegos educativos y las simulaciones son herramientas de enseñanza poderosas, pusieron a prueba a jugadores mediante ejemplos prácticos de tácticas de phishing en acción y una demostración de un juego educativo de ciberseguridad existente. En el mismo contexto, los investigadores (Kießling et al., 2021) diseñaron e implementaron un prototipo basado en un juego llamado Salt&Pepper, fue utilizado para mejorar los factores de impacto en

el comportamiento de seguridad de la información (ISB) basado en el factor motivación y en los sesgos cognitivos. De igual manera, (Wen et al., 2019) en su estudio presentan el juego What.Hack, que no solo enseña conceptos de phishing, sino que también simula ataques de phishing reales en un juego de rol para alentar al jugador a practicar la defensa.

Por otra parte, (Srinivasa Rao & Pais, 2017) desarrollaron una aplicación denominada FeedPhish que es capaz de detectar ataques de phishing basada en el comportamiento humano mientras se expone a un sitio web falso. Otra propuesta interesante es la de (Younis & Musbah, 2020), quienes proponen videos de animación para la formación de conciencia y parte de gamificación que va a poner a los usuarios en una prueba real para detectar ataques de phishing reales y falsos, estos están incrustados en juegos basados en desafíos.

Conforme a la RQ2., las nuevas técnicas y herramientas de Seguridad Cognitiva en Phishing, los autores (Salahdine & Kaabouch, 2019) detalla que los mecanismos de defensa basados en inteligencia artificial son las técnicas más efectivas para reducir el riesgo de ataques de ingeniería social. Otra alternativa la sugieren (Gupta et al., 2018) donde utilizan Big data con computación cognitiva.

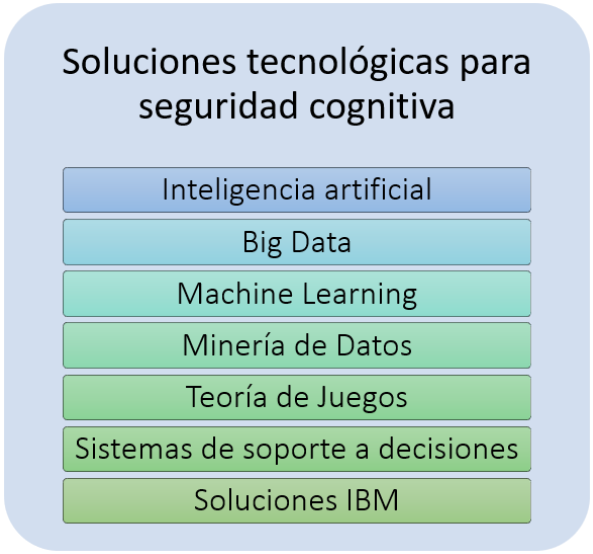
En el estudio de (Ortiz Garcés et al., 2019) mencionan que la aplicación de seguridad cognitiva propone el uso de big data, machine learning y análisis de datos para mejorar los tiempos de respuesta en la detección de ataques. Igualmente, en la investigación de (R. O. Andrade & Yoo, 2019) y en (R. Andrade et al., 2019) indican que la seguridad cognitiva podría mejorar las habilidades cognitivas de los analistas de seguridad se hace uso de soluciones tecnológicas como: big data, machine learning, support decision systems y data mining para generar estados de conciencia de ciberseguridad.

Cabe mencionar que también IBM ofrece una cartera integral de soluciones cognitivas, móviles, de nube y de seguridad relevantes para la investigación y la enseñanza académicas.

ofertas clave de IBM, con énfasis en las API cognitivas de Bluemix y Watson Analytics (Collins & Buttera, 2016). En la Figura 7 se presenta las técnicas que se puede aplicar en seguridad cognitiva según la literatura existente:

Figura 7

Algunas soluciones para aplicar seguridad cognitiva.



Nota. La figura presenta las técnicas para seguridad cognitiva detalladas en la literatura.

Conforme a RQ3. la aplicación de Psicología Cognitiva en Phishing, detallamos los factores cognitivos tratados en los artículos encontrados y las principales características de la investigación realizada ver en Tabla 1:

Tabla 1

Factores cognitivos que influyen en un ataque de Phishing

Cita	Título	Factores cognitivos tratados	Principales características
(Brinton Anderson et al., 2016)	How users perceive and respond to security messages: a NeuroIS research agenda and empirical study	Habitualidad, estrés, miedo e interferencia de la doble tarea.	Desarrollan un programa de investigación de NeuroIS para examinar cuatro factores neuronales clave relacionados con la forma en que los usuarios reciben y procesan los mensajes de seguridad.
(Williams & Li, 2017)	Simulating Human Detection of Phishing Websites: An Investigation into the Applicability of the ACT-R Cognitive Behaviour Architecture Model	La percepción y la atención, el conocimiento y la memoria, la resolución de problemas y la toma de decisiones, así como la confirmación motora de la decisión	Realizan un modelo informático de prueba de concepto para simular el comportamiento humano con respecto a la detección de sitios web de phishing basado en la arquitectura cognitiva ACT-R
(Nasser et al., 2020)	The Effects of Cue Utilization and Cognitive Load in the Detection of Phishing Emails	Utilización de pistas ayuda a reducir las demandas de la memoria de trabajo (es decir, la carga cognitiva)	Exploran el efecto de la utilización de pistas y la carga cognitiva en la detección de correos electrónicos de phishing. Un total de 50 estudiantes universitarios completaron: (1) una tarea de control de carriles y; (2) una tarea de detección de phishing
(Musuva et al., 2019b)	A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility	Susceptibilidad Género, Edad, Nivel de Educación, Rol, Años en Internet, Horas en Internet, Habilidad Informática, Carga de Correo Electrónico, Capacidad de Respuesta al Correo Electrónico, Uso de Servicios en Línea, victimización previa y Propensión al Riesgo.	El modelo propuesto se basa en el modelo de probabilidad de elaboración y se prueba empíricamente mediante la utilización de datos de 192 casos.
(Alshaikh & Adamson, 2021)	From awareness to influence: toward a model for improving employees' security behaviour	Influencia del cumplimiento, empleados cumplen la política de la empresa para obtener recompensas o evitar castigos	El estudio adoptó la teoría del apego psicológico de Kelman

Cita	Título	Factores cognitivos tratados	Principales características
(Albladi & Weir, 2018)	User characteristics that influence judgment of social engineering attacks in social networks	Cuatro perspectivas: sociopsicológica, habitual, socioemocional y perceptual.	Realizan un experimento donde envían un correo electrónico de invitación a los expertos seleccionados pidiéndoles que participaran en el estudio.
(Oliveira et al., 2017)	Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing	Tipo de influencia, el ámbito personal y la edad.	Se realizó un estudio de 21 días con 158 participantes (usuarios de Internet más jóvenes y mayores)
(Alturki et al., 2020)	Factors Influencing Players' Susceptibility to Social Engineering in Social Gaming Networks	La percepción de la gravedad de la amenaza, las barreras percibidas, los beneficios percibidos, la autoeficacia, la competencia y la cooperación	El modelo desarrollado en este estudio se basa en el modelo de creencias sobre la salud y la teoría de la cooperación y la competencia.
(Cho et al., 2016)	Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis	La confianza, el riesgo percibido y el desempeño de las decisiones	El modelo matemático desarrollado se puede aplicar para predecir qué perfiles de personalidad en una organización están más expuestos a la ingeniería social
(Carroll et al., 2022)	How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society	Credibilidad, Persuasión, Consistencia y la Escasez ejercen un claro efecto positivo sobre el número de clics generados	Emplearon mediciones cuantitativas de los desencadenantes de la vulnerabilidad cognitiva en los correos electrónicos de phishing para predecir el grado de éxito de un ataque
(Pearson et al., 2017)	"To click or not to click is the question": Fraudulent URL identification accuracy in a community sample	Alta carga de trabajo cognitivo, un alto grado de estrés, un bajo grado de vigilancia atencional, la falta de conocimiento del dominio y/o la falta de experiencia pasada. Los antecedentes culturales	Un marco extendido de funciones cognitivas humanas para adaptarse a los ciberataques de ingeniería social
(Wash & Cooper, 2018)	Who Provides Phishing Training?: Facts, Stories, and People Like Me	Mecanismos de confianza y desconfianza interpersonal	Presentan un estudio realizado en 249 participantes diseñado para averiguar cómo interpretan los correos electrónicos de phishing y decidían si confiar o no en ellos.

2. Selección de estudios primarios

Al realizar la selección de los trabajos de investigación se aplica los siguientes criterios de inclusión:

- ✓ Idioma: inglés
- ✓ Año: 2017-2022
- ✓ Tipo de publicación: Revistas y conferencias

En base a los criterios antes mencionados, y el criterio de los investigadores, se optaron por 7 estudios primarios, los cuales contribuyen a sustentar una base para realizar el estudio del arte, los cuales se describen en la Tabla 2.

Tabla 2

Estudios Primarios

Código	Título	Cita
EP1	Detecting Phishing Websites using Automation of Human Behavior	Routhu Srinivasa Rao and Alwyn R. Pais. (2017).
EP2	How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society	Carroll F., Adejobi J.A. & Montasari R. (2022).
EP3	"To click or not to click is the question": Fraudulent URL identification accuracy in a community sample	Pearson E., Bethel C. L., Jarosz A. F. and Berman M. E. (2017)
EP4	Engaging Users with Educational Games: The Case of Phishing	Matt Dixon, Nalin Asanka Gamagedara Arachchilage, and James Nicholson. (2019).
EP5	What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game	Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. (2019).

EP6	Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility	Greitzer F. L., Li Wanru, Laskey K. B., Lee J. and PURL J. (2021)

Documentar la revisión

3. Elaboración del estado del arte

EP1 (Routhu Srinivasa Rao and Alwyn R. Pais. (2017)): Detecting Phishing Websites using Automation of Human Behavior

En el presente estudio proponen una técnica para detectar ataques de phishing basada en el comportamiento humano mientras se expone a un sitio web falso. Desarrollaron una aplicación denominada FeedPhish, implementada en la plataforma Java. Para lo cual introducen valores falsos en la página de inicio, si la página web inicia sesión correctamente, se clasifica como phishing; de lo contrario, lo somete a un filtrado heurístico adicional. Todo el trabajo se divide en tres módulos que realizan el proceso de filtrado en cada nivel, estos filtros son: LoginCheck, FeedFakeCredentials y HeuristicsCheck. Los resultados de la experimentación muestran que su aplicación ha logrado una tasa de precisión general del 96,38%.

EP2 (Carroll F., Adejobi J.A. & Montasari R. (2022)): How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society

El éxito de los ataques de phishing más recientes depende de cuán convincente y, a menudo, cuán familiar o identificable sea un escenario de correo electrónico. Los investigadores indican que "el miedo a la COVID-19 influye en el éxito de las estafas de phishing temáticas específicas de la COVID-19, mientras que la ansiedad, el estrés y la asunción de riesgos influyen en el éxito de las estafas de phishing comunes y temáticas de la COVID-19". El documento evidencia un estudio que presentó a los participantes de la prueba cinco categorías diferentes

de correos electrónicos (se incluye phishing y no phishing). Los hallazgos presentan que, a los participantes, en general, les resultó difícil detectar los ataques de correo electrónico de phishing modernos. También desarrollaron un cuestionario mediante el uso del software de encuestas de Qualtrics para investigar la percepción de las personas sobre la detección de ataques de correo electrónico de phishing. Los investigadores descubrieron que las personas no tenían confianza, estaban preocupadas y, a menudo, insatisfechas con las tecnologías actuales disponibles para protegerse contra los correos electrónicos de phishing.

EP3 (Pearson E., Bethel C. L., Jarosz A. F. and Berman M. E. (2017)): "To click or not to click is the question": Fraudulent URL identification accuracy in a community sample

Es difícil defenderse de la explotación de los sesgos cognitivos humanos en respuesta a los ataques de phishing. El propósito de este estudio fue determinar si los humanos podían discriminar localizadores uniformes de recursos (URL) fraudulentos o enlaces de URLs legítimas sin la ayuda de hardware o software específico. Se utilizó la táctica del juego de roles para minimizar los riesgos de los participantes. Los correos electrónicos se diseñaron para que se parecieran a situaciones de la vida real. El documento puso de manifiesto que durante la tarea principal de un usuario es "consultar el correo electrónico", le resulta difícil descifrar los correos electrónicos fraudulentos de los auténticos. Los resultados de la fase de juego de rol de este estudio indicaron que los participantes tuvieron la mayor dificultad con las URLs de texto adicional.

EP4 (Matt Dixon, Nalin Asanka Gamagedara Arachchilage, and James Nicholson. (2019)): Engaging Users with Educational Games: The Case of Phishing

En este documento detallan que los juegos educativos y las simulaciones son herramientas de enseñanza versátiles y poderosas, pusieron a prueba a jugadores mediante ejemplos prácticos de tácticas de phishing en acción y una demostración de un juego educativo

de ciberseguridad existente. Como resultados mencionan que al tratarse de un juego educativo el tema y los resultados de aprendizaje del juego deben ser consistentes para crear una experiencia fluida en la que el jugador aprende y se pone a prueba a través del juego.

EP5 (Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. (2019)): What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game

En el presente trabajo de investigación presentan el juego What.Hack, que no solo enseña conceptos de phishing, sino que también simula ataques de phishing reales en un juego de rol para alentar al jugador a practicar la defensa. Integraron el conocimiento conceptual en un juego de procesamiento de correo electrónico y dejaron que el jugador interprete qué tipos de URL son peligrosos, mientras que las otras dos condiciones sólo se centran en el conocimiento conceptual, como la mecánica de las URL. Los resultados de su estudio demuestran que What.Hack fue capaz de mejorar la capacidad de los jugadores para identificar las amenazas entrantes en un 36,7%, mientras que un grupo de control que jugó a un juego diferente no consiguió una mejora estadísticamente significativa. What.Hack ofrece un buen punto de partida para el desarrollo de otras experiencias similares basadas en juegos en el campo de la ciberseguridad.

EP6 (Greitzer F. L., Li Wanru, Laskey K. B., Lee J. and PURL J. (2021)): Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility

En el documento informan sobre un experimento de phishing simulado dirigido a 6938 profesores y personal de la Universidad George Mason. En la campaña de phishing de tres semanas emplearon tres tipos de vulnerabilidades de phishing, examinó datos demográficos de auditoría de monitoreo de redes/estaciones de trabajo vinculadas, y una variedad de factores conductuales y psicológicos medidos a través de encuestas previas y posteriores a la campaña.

Características del estado del arte

En los estudios encontrados detallan diferentes técnicas o métodos para realizar una detección de phishing mediante la utilización de una aplicación o software, implementado en los mismos inteligencia artificial, aprendizaje automático, juego de roles, entre otros. Dentro de los trabajos primarios existe el desarrollo de juegos educativos utilizados para realizar campañas de capacitación sobre phishing y detallan las vulnerabilidades de las personas y los factores humanos que en algunos casos influyen para que sea una víctima.

La mayoría de los estudios concuerdan que un factor primordial en la seguridad informática es el ser humano, pese a las implementaciones de software o de herramientas que detectan ataques cibernéticos ya sea en empresas, organizaciones o universidades. Los ciberataques han aumentado con el pasar de los años y más aún en una época de pandemia en la que las personas tuvieron que adaptarse al teletrabajo, al uso constante de Internet y del correo electrónico. Además, que los phishers cada día crean nuevas formas para engañar a sus víctimas aprovechándose de las vulnerabilidades psicológicas.

Estos problemas son los que llevan a proponer el desarrollo de la plataforma para el entrenamiento de Phishing con ejercicios simulados mediante la aplicación de seguridad cognitiva y la detección de la percepción de riesgo del usuario.

Capítulo III

Marco Metodológico

Metodología aplicada al desarrollo del trabajo de investigación

El enfoque de este estudio es la creación de un producto que aporte con el entrenamiento de los usuarios al momento de detectar un ataque tipo Phishing en correos electrónicos. La metodología que se adapta y que se aplicará es la metodología Ciencia del diseño (Design Science), que es la ciencia que procura consolidar conocimientos sobre el diseño y desarrollo de soluciones para mejorar sistemas existentes, resolver problemas y crear nuevos artefactos.

A través de la plataforma web propuesta se realizará un entrenamiento sobre ataques de tipo Phishing, mediante el cual se tomarán datos de los usuarios y de las respuestas que den a cada uno de los ejercicios planteados. En una primera instancia será para obtener la información necesaria y realizar una clasificación de los ejercicios, la cual ayudará en el proceso de desarrollo del algoritmo mediante la aplicación de teoría de juegos con árboles de decisión. Y en una segunda instancia será para conocer la percepción de riesgo mediante el cuestionario aplicado dentro de la plataforma y analizar los caminos por los cuales los usuarios se dirigieron a partir de su scrore.

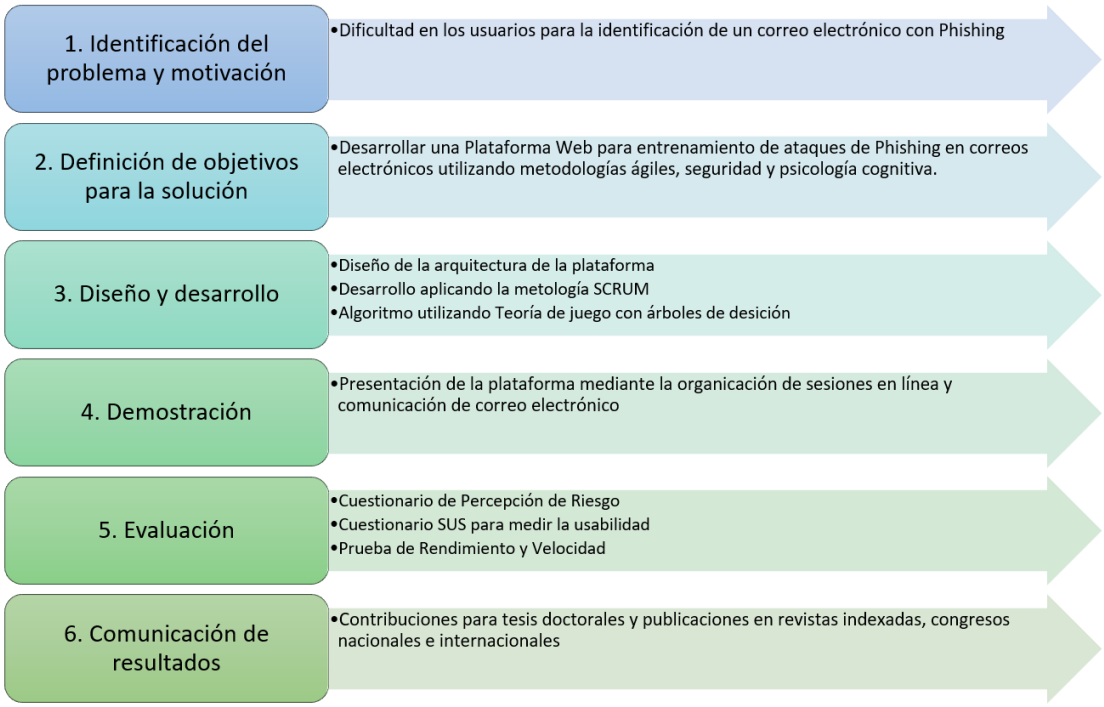
DSR (Design Science Research)

DRS es una metodología la cual se define como "un paradigma de resolución de problemas que busca mejorar el conocimiento mediante la creación de artefactos innovadores" (vom Brocke et al., 2020). La literatura identifica 6 etapas típicas del proyecto DSR: identificación y justificación del problema, definición de los objetivos de la solución, diseño y desarrollo del artefacto, demostración, evaluación, seguida de la comunicación de los resultados (Alexei, 2022).

Es así que el presente trabajo de investigación se realiza a medida de cada una de estas fases como podemos observar en la Figura 8.

Figura 8

Etapas del DSR aplicadas en el presente trabajo de investigación



Nota. En la figura se detalla los procedimientos aplicados en el desarrollo del proyecto dentro de la metodología

Metodología de desarrollo

De acuerdo al tiempo y a la forma de desarrollo dentro del presente estudio se va aplicar una metodología ágil ya que brinda muchos beneficios entre ellos: la satisfacción del cliente que es la máxima prioridad, demostrada a través de la entrega continua y el valor agregado.

La metodología ágil es un enfoque centrado en las personas y en los resultados para el desarrollo de software que respeta que cambie rápidamente. Se centra en la planificación

adaptativa, la autoorganización y los plazos de entrega breves. Es flexible y busca mejoras continuas en la calidad, más aún, con el uso de herramientas como Scrum y eXtreme Programming (Altvater, 2017). La metodología escogida es Scrum ya que se adapta al plan de desarrollo que se va implementar.

Scrum

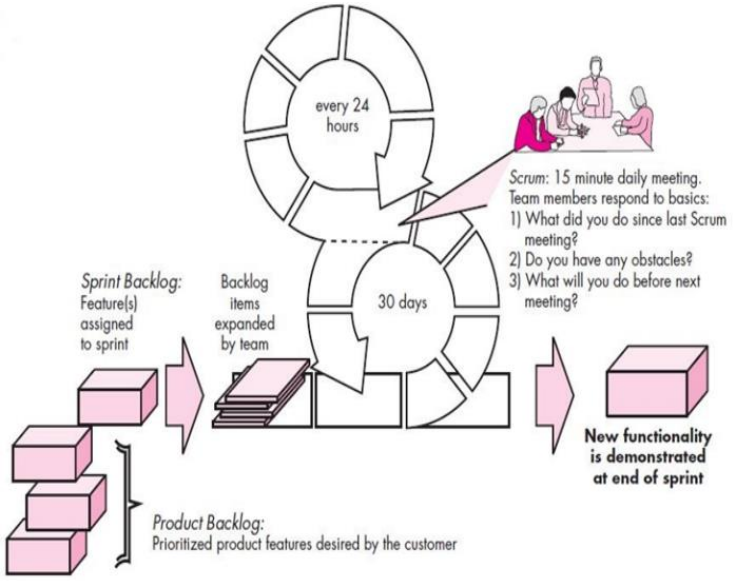
Scrum es un enfoque de gestión de proyectos iterativo e incremental que proporciona un marco sencillo de "inspeccionar y adaptar". En Scrum, el software se entrega en incrementos llamados "Sprints" (normalmente iteraciones de 2-4 semanas) (Hossain et al., 2009).

Del mismo modo, (Sutherland et al., 2007) describen Scrum como un "proceso de desarrollo de software ágil diseñado para añadir energía, enfoque, claridad y transparencia a los equipos de proyecto que desarrollan sistemas de software". Los procesos de Scrum se adhieren a los principios del enfoque ágil. Scrum es conocido por sus importantes procesos de software que lo distinguen de otros enfoques ágiles como XP, el desarrollo de software, procesos ágiles unificados, etc., como se puede visualizar en la Figura 9. Scrum incluye (Faniran et al., 2017) :

- **Backlogs:** lista de requisitos funcionales en una escala de preferencia, que puede cambiar durante el desarrollo;
- **Sprints**: unidades de trabajo necesarias para lograr un requisito en el backlog con un marco de tiempo (normalmente 30 días);
- **Reuniones de Scrum**: reuniones breves (normalmente de 15 minutos) reuniones entre los miembros del equipo en las que participa un Scrum Master que coordina el equipo.
- **Demostraciones**: incrementos de software entregados al cliente para su evaluación, que incluye funcionalidades solicitadas para ser entregadas dentro de un plazo establecido.

Figura 9

Flujo del proceso Scrum en la plataforma



Nota. La figura presenta el desarrollo de la metodología Scrum. Tomada de (Faniran et al., 2017)

Roles de Scrum

A diferencia de los métodos clásicos de gestión de proyectos, Scrum no tiene ni necesita un gestor de producto, un gestor de tareas o un jefe de equipo. Un equipo Scrum tiene una composición ligeramente diferente a la de un proyecto tradicional en cascada, con tres roles específicos: Propietario del producto, Scrum Master, y Equipo de desarrollo. Estos tres roles son coetáneos y todos ellos tienen ciertas responsabilidades (Sachdeva, 2016):

- **Product Owner**: es responsable de la visión del producto, la recopilación y la priorización de los requisitos y el control sobre el presupuesto.
- **Scrum Master**: se encarga de los problemas, se responsabiliza de que las reglas de Scrum se sigan adecuadamente y también entrena al equipo.

- **Equipo de Scrum**: es un grupo de personas autoorganizadas, responsables de la creación y la calidad del producto. Y como los equipos de Scrum son interfuncionales, el equipo de desarrollo incluye a probadores, diseñadores e ingenieros de operaciones, además de los desarrolladores.

Así mismo, existen algunos más de Stakeholders, que sirven de observadores o consejeros.

Artefactos de Scrum

Son información que el equipo de Scrum y las partes interesadas utilizan para detallar el producto en desarrollo, las acciones necesarias para producirlo y las acciones realizadas en el proyecto (Atlassian, s. f.). En el estudio realizado por (Sachdeva, 2016) se mencionan los siguientes artefactos:

- **Backlog del producto:** enumera los requisitos para el producto que se está desarrollado en formato de historia de usuario. Cada elemento en el Backlog del Producto tiene una descripción, una prioridad y una estimación del esfuerzo necesario para completarlo. Lo gestiona el propietario del producto.
- **Plan de lanzamiento:** describe el objetivo de la versión, los elementos de mayor prioridad en el Product Backlog, los principales riesgos, y las características generales y funcionalidad que contendrá la versión. También establece una fecha de entrega y un coste probable, al que se supone que nada cambie.
- **Sprint Backlog**: es un resultado de la Reunión de Planificación del Sprint. Consiste en las tareas estimadas y asignadas. Poseído y modificado sólo por el equipo.
- **Gráficos de Burn-down:** durante un sprint, los artefactos visuales como los tableros de tareas y los gráficos de burn down, visibles tanto para el equipo como para los espectadores, actúan como poderosos motivadores.

Capítulo IV

Desarrollo de la plataforma web de entrenamiento de Phishing

Descripción del sistema

Los ejemplos de ataques de Phishing reales proporcionan información muy útil que ayuda a los equipos de seguridad a identificar de forma óptima los métodos y tácticas de los atacantes. Las estrategias de los atacantes cambian rápidamente, es por esto que los ejemplos de Phishing del mundo real son un componente central de la seguridad integral ya que revelan las últimas maniobras de los actores de la amenaza en el momento en que se lanzan.

Una alternativa a este tipo de ataques en las empresas, organizaciones, instituciones es realizar capacitaciones o entrenamiento a sus trabajadores y conocer su capacidad de detección. Es por esta razón que la plataforma web desarrollada contiene como ejercicios correos electrónicos simulados de Phishing y legítimos, y la persona que finalice el entrenamiento va a conocer su nivel de detección y su nivel de percepción de riesgo ante este ciberataque. Así mismo, tiene una retroalimentación de cada uno de los ejercicios que se le mostraron en el proceso y un puntaje de Score.

En la Tabla 3 se detallan los procesos que forman parte de la plataforma de entrenamiento. Cabe destacar que el presente estudio es una segunda fase ya que la primera se ve plasmada en el artículo denominado “Una plataforma web de formación para mejorar las habilidades cognitivas para la detección de ataques de Phishing” (Cazares et al., 2022).

Tabla 3

Procesos de la plataforma de entrenamiento

Proceso	Descripción
Registro de los usuarios	El usuario al iniciar el entrenamiento tiene un formulario donde va registrar su nombre y apellido, correo electrónico, los años de edad, debe seleccionar si es profesional o estudiante, así mismo su género, carrera y los años de experiencia en ciberseguridad. El objetivo de este proceso es tener un registro específico de cada uno de los participantes en la base de datos.
Visualización de los ejercicios de cada usuario	En este proceso, internamente se le asignan al usuario ejercicios mediante el algoritmo implementado, estos ejercicios se almacenan en el documento de cada usuario creado en la base de datos.
Registro del tiempo de respuesta	Por cada ejercicio existe un cronómetro interno que controla el tiempo del usuario en dar la respuesta. Al final en la vista de resultados, el usuario visualiza el tiempo en segundos que se tardó por ejercicio y un tiempo total y promedio en el entrenamiento. Todos estos datos se agregan al documento del usuario en la base de datos.
Registro de eventos clic y focus en los enlaces de cada ejercicio.	Los ejercicios contendrán enlaces los cuales registramos los eventos que el usuario puede accionar, estos suceden mientras que el usuario interacciona con un botón o enlace y este se agrega al documento del usuario en la base de datos.
Registro de las respuestas del usuario en cada ejercicio	El usuario tiene dos opciones de respuesta en cada ejercicio, Phishing o Legítimo. Estas respuestas son registradas por cada ejercicio y guardadas respectivamente en la base. En la vista de resultados estos datos se ven reflejados y también una retroalimentación de los mismos.
Registro del comentario sobre la respuesta escogida	El usuario escoge una respuesta dentro del ejercicio se le despliega una ventana emergente en la que él debe escribir la o las razones por las que escogió esa respuesta. Estos datos también se guardan en la base de datos para un futuro análisis.
Registro de las respuestas del cuestionario de percepción de riesgo	El usuario tiene que seleccionar su respuesta en cada una de las preguntas del cuestionario de percepción de riesgo que se le presenta luego del 4 ejercicio en el proceso de entrenamiento. Estas respuestas sirven para sacar el nivel de percepción de riesgo del usuario frente a este ataque.

Cálculo y Visualización del Score del usuario	A medida que el usuario contesta los ejercicios, estos se le presentan en relación a las respuestas anteriores, ya sean ejercicios fáciles, intermedios o difíciles, cada uno de estos tiene un respectivo puntaje con el que se le asigna al score.
Registro y visualización del nivel de detección del usuario	Al terminar todo el proceso de entrenamiento al usuario se le presenta una vista con todos los resultados obtenidos en los ejercicios. El nivel de detección se le calcula con respecto a los aciertos que tuvo y este puede ser malo bueno y excelente.

Limitaciones de la plataforma

La plataforma web para el entrenamiento de Phishing ayuda a los usuarios a saber su nivel de detección de estos ataques en correos electrónicos, de igual forma a conocer su nivel de percepción de riesgo. Así mismo, con la retroalimentación de los ejercicios el usuario puede aprender algunas de las características que debe tomar en cuenta al momento de detectar un ataque Phishing. El score motiva a seguir preparándose y capacitándose en este tema para evitar de alguna manera ser vulnerado por los ciber atacantes. Sin embargo, el prototipo cuenta con algunas restricciones como son:

- La plataforma está orientada específicamente a ser utilizada en un computador por las dimensiones de los ejercicios y el focus que se captura.
- El proceso de validación del cuestionario de percepción de riesgo necesita una población amplia para alcanzar la validez y los niveles de confiabilidad, cabe mencionar que este proceso está en desarrollo, es decir, es un primer pilotaje de este instrumento para detectar el nivel de percepción de los usuarios frente ataques de tipo Phishing.

Personal Involucrado

Dentro del proceso del desarrollo de la Plataforma web de entrenamiento de Phishing, se encuentran involucrados profesionales del ámbito de la ciberseguridad y de la psicología, quienes aportaron con conocimientos y directrices necesarias para lograr cada uno de los

objetivos. Del mismo modo su participación ayudó para validar el funcionamiento de la aplicación web. A continuación, en la Tabla 4 se detalla los integrantes del equipo con su respectivo rol.

Tabla 4

Personal involucrado en el desarrollo del estudio propuesto

Nombre	Campo Profesional	Rol	Información del contacto
María Fernanda Cazares	Psicóloga clínica	Experta en Psicología	mariaferpsicolclinica@gmail.com
Walter Marcelo Fuertes	Doctor (PhD) en Ingeniería Informática y de Telecomunicación	Director del proyecto, experto en Ciberseguridad	wmfuertes@espe.edu.ec
Darío Ismael Valarezo	Estudiante de la carrera de Ingeniería en Tecnologías de la Información	Diseñador y programador	divalarezo@espe.edu.ec
Diana Anabel Arévalo	Estudiante de la carrera de Ingeniería en Tecnologías de la Información	Diseñadora y programadora	daarevalo3@espe.edu.ec

Perspectiva del prototipo

El diseño y desarrollo del presente estudio tendrá como resultado una plataforma web de entrenamiento de ataques de Phishing en correos electrónicos, mediante la utilización de seguridad y psicología cognitiva, para esto se utilizará las siguientes tecnologías: a) Java como lenguaje de programación mediante el uso del Framework Spring Boot para implementar los microservicios en el Back-End de la plataforma web; b) Angular como framework de JavaScript para el desarrollo del Front-End, es decir las vistas del prototipo ; c) MongoDB Atlas como servicio de base de datos de múltiples nubes, donde se creará un cluster para almacenar la información necesaria del proceso de entrenamiento de los usuarios. Es así, que al combinar

estas tecnologías se tendrá un producto final en producción y cumplirá con los requerimientos establecidos.

Funciones del Producto

En la Tabla 5 se describen las funciones generales que el usuario desarrolla dentro de la plataforma web y por ende se puede decir que son los casos de uso que están implementados en la misma.

Tabla 5

Funciones generales de la plataforma de entrenamiento de Phishing

Proceso	Funciones
Registrarse	Permite al usuario registrarse al empezar el entrenamiento. Se le presenta un formulario donde se le pide ingresar algunos datos.
Ver ayuda	Admite al usuario que al estar que al momento de realizar los ejercicios pueda presionar el botón de ayuda, el cual despliega una ventana emergente con algunos tips sobre la detección de un ataque de Phishing en correos electrónicos. Esta ayuda es general.
Seleccionar respuesta de Ejercicio	Admite que el usuario seleccione una de las dos respuestas que tiene cada ejercicio, es decir Phishing o Legítimo.
Escribir las razones del porqué de su respuesta	Proporciona al usuario el poder escribir la o las razones por las que escogió la respuesta sobre el ejercicio. Esto sucede en cada uno de los ejercicios.
Seleccionar respuestas en el cuestionario de percepción de riesgo	Permite al usuario seleccionar en cada pregunta del cuestionario una respuesta. Este cuestionario solo se le presenta una sola vez.
Ver resultados del entrenamiento	Proporciona al usuario que al final del entrenamiento pueda visualizar los resultados que obtuvo en todo el proceso, como también le presenta una retroalimentación de cada uno de los ejercicios que realizó.

Determinar las siguientes preguntas con relación al Score	Permite al sistema determinar qué ejercicios le muestra al usuario con referencia a las respuestas anteriores, esto se ve reflejado en el score que le aparece al usuario con la puntuación asignada por cada ejercicio acertado.

Tipos de los usuarios

La plataforma web de Phishing la podrá utilizar cualquier usuario que desee entrenarse o capacitarse en este tipo de ataques, únicamente se requiere tener un manejo básico de aplicaciones web. Igualmente, para la validación del proyecto se han seleccionado dos grupos de usuarios objetivos, en este caso son los estudiantes universitarios y profesionales. Por otro lado, para el manejo interno de la plataforma se necesita de un administrador que tenga acceso al cluster de la base de datos y del código almacenado en un repositorio de Github. Sin embrago, se necesitará de un profesional en ciberseguridad y de un profesional en psicología por los conceptos que se aplican a la plataforma. En la Tabla 6 se detallan los tipos de usuarios que forman parte de la plataforma con su respectiva descripción y capacidad técnica.

Tabla 6

Tipos de usuarios de la plataforma de entrenamiento

Usuario	**Descripción**	**Capacidad técnica**
Profesional	Es el usuario que tenga una carrera profesional en cualquier rama, no obstante, necesariamente se necesitan profesionales en ciberseguridad, ya que con sus respuestas podemos validar la calidad y dificultad de los ejercicios propuestos en la plataforma.	Conocimientos básicos en ataques de ingeniería social tipo Phishing.
Estudiante	Es el usuario que cursa actualmente sus estudios de pregrado, este puede	No se necesita tener conocimientos previos en ciberataques y no es necesario

	pertenecer a cualquier carrera. Las respuestas de estos usuarios permitirán realizar un proceso de clasificación de los ejercicios con respecto a la cantidad de errores y aciertos que hayan tenido en una primera fase.	que tenga conceptos de tecnología avanzados.
Psicólogo clínico	Es el usuario que aporta con los conocimientos de psicología cognitiva dentro de la plataforma, es decir, quien contribuye con el cuestionario de la percepción de riesgo y el análisis del respectivo resultado.	Conocimientos básicos de ataques Phishing.
Profesional en Ciberseguridad	Es el usuario que aporta con los conocimientos en ataques de Phishing en correos electrónicos y quien válida que los tipos de ejercicios, la táctica y las características de los mismos.	Este usuario necesita conocimientos técnicos y principalmente conocimientos en ciberseguridad.
Administrador	Es el usuario encargado internamente de monitorear la base de datos y los servidores donde se encuentra desplegada la plataforma web.	Necesita tener un conocimiento de configuraciones de servidores en la nube, conceptos de programación en Java y Angular. Así mismo de manejo del Cluster de MongoDB Atlas

Requerimientos específicos

Con el propósito de establecer los requerimientos específicos se realizaron reuniones con los interesados del producto final de este proyecto, es decir con los expertos en las áreas que se implementaron como lo es la psicología y la ciberseguridad. Para esto se detalla a continuación los requerimientos funcionales y no funcionales que se cumplieron en el desarrollo del presente estudio. Además, su identificación permitió una correcta planificación en diseño y desarrollo del mismo.

Requerimientos Funcionales

A continuación, en la Tabla 7 se detalla cada uno de los requerimientos funcionales con su respectivo nombre, propósito, entrada, salida y la prioridad que se asignó.

Tabla 7

Requerimientos Funcionales de la plataforma de entrenamiento

Código requerimiento	**RF01**
Nombre	**Visualización de inicio al test y concepto de Phishing**
Propósito	Mostrar una descripción de la plataforma y concepto de Phishing
Descripción	Mientras que el usuario ingresa a la página web, se le presentará una pantalla de inicio donde estará una pequeña descripción de lo que podrá realizar junto a un botón para comenzar el test, aparte se visualizará el concepto de Phishing.
Entrada	Clic en el botón comenzar
Salida	Redirección a la página de registro de usuario
Prioridad	Baja

Código requerimiento	**RF02**
Nombre	**Registro de usuario**
Propósito	Obtener registro de cada usuario que realizará el test.
Descripción	El usuario debe registrar sus datos tales como su nombre y apellido, correo electrónico, los años de edad, debe seleccionar si es profesional o estudiante, al igual que su género, carrera y los años de experiencia en ciberseguridad. Para guardar el registro deberá pulsar el botón siguiente o tiene la opción de volver al inicio.
Entrada	Clic en el botón siguiente
Salida	Redirección a la página de indicaciones
Prioridad	Alta

Código requerimiento	**RF03**
Nombre	**Visualización de indicaciones**
Propósito	Mostrar indicaciones sobre qué debe hacer en cada ejercicio.
Descripción	Al usuario se le presentan las indicaciones que deberá tener en cuenta una vez que empiece el test, para seguir deberá pulsar el botón empezar.
Entrada	Clic en el botón empezar
Salida	Redirección al test
Prioridad	Baja

Código requerimiento	**RF04**
Nombre	**Visualización de ejercicios (simulación de contenido de correo electrónico)**
Propósito	Mostrar los ejercicios uno por uno
Descripción	Al usuario se le presenta un ejercicio (correo electrónico) el cual deberá analizar para determinar si es legítimo o Phishing. Implementación de visualización de ejercicios.
Entrada	Registro de usuario
Salida	Visualización de ejercicio
Prioridad	Alta

Código requerimiento	**RF05**
Nombre	**Registro en segundo plano de eventos clic y focus en los enlaces en cada ejercicio**
Propósito	Registrar las pulsaciones y movimiento entre los enlaces en cada ejercicio.
Descripción	Guardado de los eventos activados de clic y focus que contienen los enlaces o botones en cada ejercicio. Se implementará en RF04
Entrada	Clic o focus en enlaces o botones
Salida	Registro de los eventos en la base de datos
Prioridad	Alta

Código requerimiento	**RF06**
Nombre	**Registro de tiempo en cada ejercicio**
Propósito	Registrar el tiempo de cada ejercicio
Descripción	Se implementará un cronómetro interno que registrará el tiempo de respuesta de cada ejercicio por parte del usuario.
Entrada	Inicio de ejercicio
Salida	Guardado de tiempo en la base de datos
Prioridad	Alta

Código requerimiento	**RF07**
Nombre	**Registro de las respuestas del usuario en cada ejercicio**
Propósito	Registrar la respuesta del usuario ante el ejercicio.
Descripción	El usuario deberá responder al ejercicio entre Legitimo o Phishing. Cada respuesta se guardará en la base de datos.
Entrada	Clic en el botón Legítimo o Phishing
Salida	RF08
Prioridad	Media

Código requerimiento	**RF08**
Nombre	**Registro del comentario sobre la respuesta escogida**
Propósito	Registrar el comentario de cada ejercicio
Descripción	Una vez que el usuario respondió al ejercicio en RF07, se le presentará un modal en pantalla donde podrá ingresar un comentario de manera obligatoria para después pulsar el botón guardar.
Entrada	RF07
Salida	Visualización de ejercicio, cuestionario o resultados
Prioridad	Media

Código requerimiento	**RF09**

Nombre	**Visualización y registro de cuestionarios.**
Propósito	Mostrar cuestionario para que el usuario responda
Descripción	Antes de llegar al ejercicio 4, se le mostrará el cuestionario que el usuario deberá responder de manera obligatoria. Las respuestas del cuestionario se guardarán en la base de datos y seguidamente se le presentan los demás ejercicios.
Entrada	Preguntas del cuestionario
Salida	Registro de respuestas y redireccionamiento a los ejercicios.
Prioridad	Media

Código requerimiento	**RF010**
Nombre	**Cálculo y Visualización del Score del usuario**
Propósito	Calcular y visualizar score en cada ejercicio
Descripción	Se calculará el score que se obtiene por cada respuesta que el usuario escoge. Este score comienza en cero y aumenta a medida que responde cada uno de los ejercicios. En cada ejercicio se visualizará el score que tiene hasta el momento.
Entrada	Respuesta del usuario
Salida	Aumento de score si la respuesta es correcta.
Prioridad	Alta

Código requerimiento	**RF011**
Nombre	**Registro y visualización del nivel de detección del usuario**
Propósito	Se registra y visualiza el nivel de detección.
Descripción	Al finalizar el test, se calculará y registrará el nivel de detección del usuario antes ataques Phishing. Posterior a los resultados se visualizará el puntaje del nivel de detección.
Entrada	Datos de detección.
Salida	Visualización y registro de nivel de detección.
Prioridad	Media

Código requerimiento	**RF012**
Nombre	**Visualización de resultados y retroalimentación.**
Propósito	Mostrar los resultados del test
Descripción	Al finalizar el test, al usuario se le mostrará los resultados finales, se mostrará el tiempo total y promedio, score final, resultados de los ejercicios, gráfico de nivel de percepción y retroalimentación de los ejercicios.
Entrada	Test finalizado
Salida	Resultados del test
Prioridad	Media

Requerimientos no funcionales

Los requerimientos no funcionales establecidos se encuentran detallados en la Tabla 8.

Tabla 8

Requerimientos no funcionales de la plataforma de entrenamiento

Código requerimiento	**RNF01**
Nombre	**Robustez**
Descripción	La página debe funcionar con fluidez y debe responder bien al guardado de datos en segundo plano.
Prioridad	Alta

Código requerimiento	**RNF02**
Nombre	**Confidencialidad**
Descripción	El sistema debe guardar la información de manera segura para fines investigativos.
Prioridad	Alta

Código requerimiento	**RNF03**

Nombre	**Disponibilidad**
Descripción	El sistema debe de estar disponible en cualquier momento para el acceso y realización del test por parte de los usuarios
Prioridad	Alta

Código requerimiento	**RNF04**
Nombre	**Usabilidad**
Descripción	El sistema debe ser fácil y efectivo de usar para los usuarios que requieran realizar el test.
Prioridad	Media

Descripción de las herramientas

La Plataforma web se desarrolló dentro de una infraestructura de microservicios, para lo cual se utilizó las siguientes herramientas, para la parte Back-End y Front-End.

Java

Aunque se usa principalmente para aplicaciones basadas en Internet, Java es un lenguaje simple, eficiente y de propósito general. Java se diseñó originalmente para aplicaciones de red integradas que se ejecutan en múltiples plataformas. Es un lenguaje portátil, orientado a objetos e interpretado, es extremadamente portátil, es decir, se ejecutará de manera idéntica en cualquier computadora, independientemente de las características del hardware o del sistema operativo, siempre que tenga un intérprete de Java (Austerlitz, 2003).

Java es un lenguaje de programación orientado a objetos, es uno de los tres más utilizados en los últimos tiempos gracias al amplio soporte con el que cuenta, así como también con la gran variedad de clases y colecciones. Además, es uno de los lenguajes más robustos y utilizados en el mundo del desarrollo de software multiplataforma, permite a los

desarrolladores crear aplicaciones o sistemas de información locales, ambientes web e incluso aplicaciones para móviles, con lo que se puede decir que se consolida como uno de los mejores lenguajes de programación en la actualidad (Beltrán, 2016) .

Un ejemplo de uso de este lenguaje de programación es el estudio realizado por (Srinivasa Rao & Pais, 2017) donde desarrollan una aplicación denominada FeedPhish que detecta ataques de Phishing basados en el comportamiento humano mientras se expone a un sitio web falso y mencionan que está implementada en la plataforma Java.

Framework Spring Boot

El marco de trabajo Spring Boot es un subproyecto bajo el proyecto Spring y es actualmente el marco de trabajo de desarrollo a nivel empresarial más popular de Java (Miao et al., 2020). Está basado en Java de código abierto que se utiliza para crear un microservicio.

Se utiliza para crear aplicaciones Spring independientes y listas para producción, proporciona una buena plataforma para que los desarrolladores de Java desarrollen una aplicación Spring independiente y de grado de producción que puede ejecutar. Así mismo, facilita la creación de aplicaciones basadas en Spring independientes y de grado de producción que puede "simplemente ejecutar" (Spring, 2020).

Ventajas

Spring Boot ofrece las siguientes ventajas a sus desarrolladores:

- Fácil de entender y desarrollar aplicaciones.
- Aumenta la productividad.
- Reduce el tiempo de desarrollo.
- Es una buena opción para crear aplicaciones basadas en microservicios.

- Proporciona un amplio soporte a diferentes tecnologías como: bases de datos relaciones y no relacionales, almacenamiento en caché, mensajería, procesamiento por lotes y más.

Microservicios

El estilo arquitectónico de microservicios es un enfoque para desarrollar una aplicación única como un conjunto de pequeños servicios, cada uno de los cuales se ejecuta en su propio proceso y se comunica con mecanismos ligeros, a menudo una API de recursos HTTP. Estos servicios se construyen en torno a las capacidades empresariales y se pueden desplegar de forma independiente mediante una maquinaria de despliegue totalmente automatizada. Hay un mínimo de gestión centralizada de estos servicios, que pueden estar escritos en diferentes lenguajes de programación y utilizar diferentes tecnologías de almacenamiento de datos (Zimmermann, 2017) (Lewis & Fowler, 2014). En el estudio realizado por (Bushong et al., 2021) mencionan que el diseño de microservicios ofrece muchas ventajas para las aplicaciones empresariales, incluida una mayor escalabilidad y tiempos de implementación más rápidos. La independencia de los microservicios entre sí en el desarrollo y la implementación proporciona estas ventajas.

Existe una variedad de ventajas al utilizar microservicios, entre las que se puede mencionar:

- Lenguaje de programación y tecnología independientes.
- Mejora de la escalabilidad, agilidad y tiempo de comercialización.
- Alta mantenibilidad e implementación automatizada.
- Migración y actualización efectivas.
- Confiabilidad y riesgos de seguridad reducidos.
- Costo y tiempo de desarrollo optimizados.

Angular

El marco de desarrollo web Angular, respaldado por Google, es una plataforma de desarrollo, construida sobre Type Script (Angular, s. f.). Angular facilita a los programadores el uso de dependencias y un marco basado en componentes para crear aplicaciones web escalables. Además, una colección de bibliotecas bien integradas que cubren una amplia variedad de funciones, incluido el enrutamiento, la gestión de formularios, la comunicación cliente-servidor y más (Sterling, 2019).

Visual Studio Code

Visual Studio Code es un editor de texto gratuito de código abierto de Microsoft. Está disponible para Windows, Linux y macOS. Aunque el editor es relativamente liviano, incluye algunas características poderosas que han convertido a VS Code en una de las herramientas de entorno de desarrollo más populares en los últimos tiempos (Zohair, s. f.). Además, tiene un editor de código de alta productividad que, una vez que se combina con servicios de lenguaje de programación, le brinda el poder de un IDE y la velocidad de un editor de texto (Visual Studio Code, 2022).

MongoDB Atlas

La evolución de diferentes modelos de datos NoSQL para administrar gran volumen y variedad de datos ha ayudado a facilitar el manejo de muchas aplicaciones poderosas como Facebook, Instagram, WhatsApp, etc. Existen proveedores que proporcionan modelos de datos NoSQL como instalación de servicios en la nube. Así mismo, MongoDB es uno de los modelos populares de datos NoSQL orientados a documentos (Samanta & Chaki, 2021).

MongoDB Atlas es una oferta alojada de MongoDB como servicio, que es fácil de configurar, operar y escalar en la nube. Al igual que muchas tiendas NoSQL, MongoDB Atlas

permite a los usuarios aceptar posibles incoherencias temporales entre las réplicas, a cambio de una latencia más baja y una mayor disponibilidad durante las peticiones (Huang et al., 2019).

Microsoft Azure

Microsoft Azure es una marca global para los servicios de computación en la nube de Microsoft, abarca una amplia gama de servicios que sigue en crecimiento y, a menudo forman los elementos fundamentales de la informática en la nube (Copeland et al., 2015).

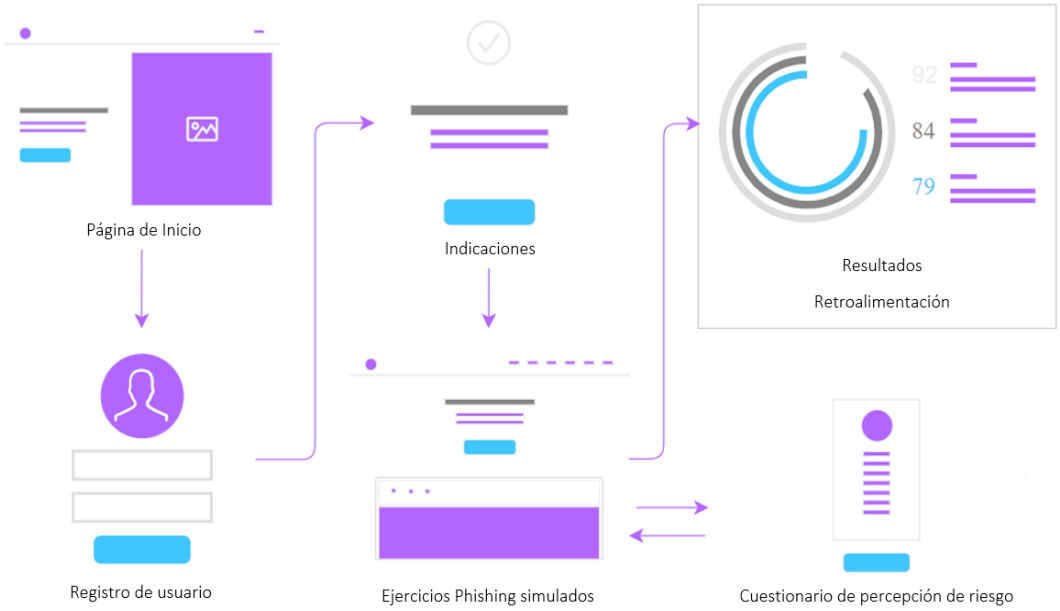
Con el servicio de App Service que ofrece esta plataforma se puede crear, implementar y escalar rápidamente aplicaciones web y API según sus términos. Se puede trabajar con .NET, .NET Core, Node.js, Java, Python o PHP en contenedores o ejecutándose en Windows o Linux. Cuenta con servicio completamente administrado con mantenimiento de infraestructura incorporado, parches de seguridad y escalabilidad (Microsoft Azure, s. f.).

Diseño de la plataforma web

Cabe recalcar que el diseño de la plataforma sigue una estructura similar a la realizada en la anterior fase, es así que la plataforma está plasmada en el siguiente esquema, ver Figura 10.

Figura 10

Diagrama de funcionamiento de la plataforma de entrenamiento



Nota. En la figura se presenta cada una de las iteraciones que debe realizar el usuario dentro de la plataforma de entrenamiento.

Para empezar, se describe el diseño de la base de datos en la que se basa el desarrollo, seguidamente el diagrama de casos de uso y el diseño de la arquitectura de la plataforma web.

Diseño de la Base de Datos

Para tener un adecuado control de las interacciones de cada uno de los usuarios dentro del entrenamiento de la plataforma se vio conveniente utilizar una base de datos no relacional, ya que estas son utilizadas en la creación de aplicaciones, tiendas online, desarrollo de juegos, administración de sistemas que tienen gran volumen de datos, etc. Y en este caso utilizamos el servicio de MongoDB Atlas, donde se creó un cluster específicamente para almacenar los datos recolectados. Además, que este tipo de base datos ofrece alta disponibilidad, incorporación de

cambios durante el proceso de desarrollo, todo lo almacena en colecciones, las cuales son un conjunto de documentos que en este caso serían cada uno de los usuarios que, a su vez, tienen una estructura JSON e internamente, poseen claves que funcionan como campos y ofrecen una alta capacidad de almacenamiento. A continuación, se mencionan algunas de las variables que se recolectaron:

- Tiempo de respuesta en cada ejercicio
- Tasa de acierto y error
- Latencia de respuesta (tiempo que tarda en dar respuesta)
- Interacción del usuario (Información de ayuda)
- Razones por las que toma la decisión

En la Figura 11 se observa la estructura JSON o modelo de datos no relacional del presente prototipo.

Figura 11

Esquema de base de datos de la plataforma web


```
{
  "anioExperiencia": 0,
  "apellido": "string",
  "carrera": "string",
  "cuestionario": [
    {
      "pregunta": "string",
      "puntuacion": 0,
      "respuesta": "string"
    }
  ],
  "direccion": "string",
  "edad": 0,
  "ejercicios": [
    {
      "click": [
        [
          "string"
        ]
      ],
      "comentario": "string",
      "focus": [
        [
          "string"
        ]
      ],
      "respuesta": "string",
      "tiempo": 0,
      "tipo": "string"
    }
  ],
  "email": "string",
  "fechaInicio": "2022-08-03T01:04:14.931Z",
  "genero": "string",
  "id": "string",
  "key": "string",
  "nombre": "string",
  "ordenEjercicios": [
    0
  ],
  "profesion": "string",
  "resultados": {
    "tasaError": 0,
    "tasaExito": 0,
    "tiempoPromedio": 0,
    "tiempoTotal": 0
  }
}
```


Nota. En la figura se visualiza el esquema JSON de los datos que se guardan de cada usuario.

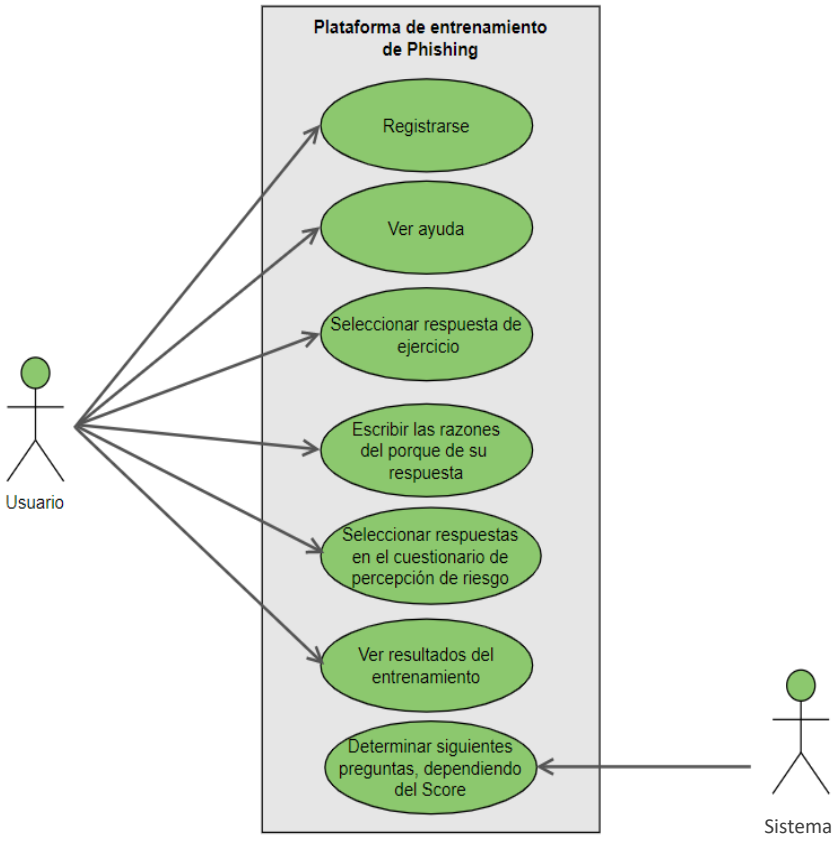
Diagrama de caso de uso

Un caso de uso se puede decir que es una metodología utilizada en el análisis de sistemas para identificar, aclarar y organizar los requisitos del sistema. Del mismo modo en UML, los diagramas de casos de uso modelan el comportamiento de un sistema y ayudan a capturar los requisitos del sistema. Los diagramas de casos de uso describen las funciones de alto nivel y el alcance de un sistema, también identifican las interacciones entre el sistema y sus actores. Los casos de uso y los actores en estos diagramas describen lo que hace el sistema y cómo lo usan, pero no cómo funciona internamente el sistema (IBM Docs, 2021).

En la Figura 12 se visualiza el desarrollo del caso de uso para la presente plataforma con las funcionalidades de los actores dentro del sistema.

Figura 12

Diagrama de casos de uso de la plataforma de entrenamiento de Phishing



Nota. En la figura se visualiza el diagrama con los actores y los casos de uso dentro de la plataforma.

En la sección de descripción de las funciones del producto se detalló cada uno de los casos de uso que tiene el presente diagrama.

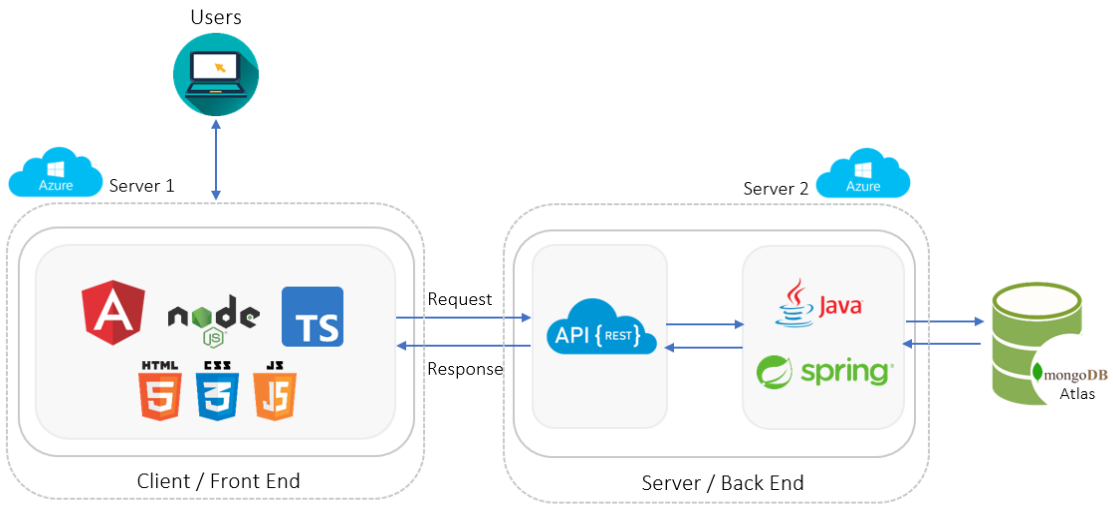
Diseño de la Arquitectura

Tener un diagrama de arquitectura es fundamental porque permite compartir la visión con el equipo, colaborar con ellos, repetir el diseño y crear la versión final óptima que cumpla con los requisitos para el uso comercial (Google Cloud, s. f.).

La arquitectura diseñada para la construcción de la plataforma web consta de tres niveles, estos son: Cliente, que corresponde a Angular con Node JS y TypeSprint; el segundo nivel es la lógica de negocio que representa al servidor de aplicaciones, corresponde a Java con el framework Spring Boot para el uso de Api REST, y el último nivel representa el modelo de la base de datos, que se encuentra en un cluster de MongoDB Altas. Adicionalmente, cabe recalcar que, para el despliegue de la plataforma la parte de Front End y Back End se encuentran alojados en servidores separados dentro de la plataforma de Microsoft Azure. Ya descrito, en la Figura 13 se visualiza la arquitectura trazada para el desarrollo de la plataforma web.

Figura 13

Diagrama de Arquitectura de la plataforma web de entrenamiento de Phishing



Nota. En la figura se visualiza la arquitectura con las herramientas utilizadas.

Diseño del cuestionario de percepción de riesgo

El cuestionario de percepción de riesgo se implementó a partir de un proceso realizado por la experta en el tema de Psicología cognitiva. De acuerdo con (Brewer et al., 2007) hay una relación muy estrecha entre percepción de riesgo y comportamiento.

La percepción de riesgo, (Brewer et al., 2007) detalla que es un constructo con 3 dimensiones:

- **Dimensión 1- Probabilidad percibida**: es la probabilidad de que uno se vea perjudicado por el peligro
- **Dimensión 2- Susceptibilidad percibida**: es la vulnerabilidad constitucional de un individuo a un peligro; y
- **Dimensión 3- Gravedad percibida**: es la magnitud del daño que causaría un peligro.

Es así que en la Tabla 9 se detalla el conjunto de preguntas establecidas dentro de las tres dimensiones:

Tabla 9

Cuestionario de percepción de riesgo

Nro. Pregunta	Pregunta	Dimensión
1	¿Me preocupan los ataques informáticos?	1
2	¿Estoy en peligro por los ciberataques?	2
3	¿Los ciberataques son un riesgo real?	3
4	¿Puede ocurrir un ciberataque?	1
5	¿En caso de un ciberataque puedo perder dinero?	3
6	¿Tengo temor de que en un ciberataque accedan a mi información personal?	3

7	¿Me siento inseguro por los ciberataques?	2

Los puntajes establecidos para cada respuesta son los siguientes:

- Siempre = 4 puntos;
- Casi siempre = 3 puntos;
- A veces = 2 puntos;
- Casi nunca = 1 puntos;
- Nunca = 0 puntos**.**

Ya establecidos los puntajes de las respuestas del cuestionario de percepción de riesgo, para calcular se hace un promedio entre el puntaje de las tres dimensiones. Así mismo, para establecer el nivel de percepción del usuario, se fijó los siguientes rangos:

- 7 - 10 puntos: Percepción de Riesgo ALTA
- 4 - 6 puntos: Percepción de Riesgo MEDIA
- 3 - 0 puntos: Percepción de Riesgo BAJA

Desarrollo de la Plataforma web

Para la planificación, desarrollo y prueba del prototipo correspondiente, se utilizó la metodología de desarrollo ágil Scrum, la cual determinó el orden en el que se desarrolló cada una de las tareas correspondientes a los requisitos del cliente que en este caso son los expertos mencionados.

Planificación mediante la metodología Scrum

Dentro de la metodología Scrum se inició con la asignación del Product Backlog que se visualiza en la Tabla 10, en donde se define las funcionalidades con respecto a los requerimientos detallados anteriormente. Además, se describe un código, la funcionalidad y la

estimación del tiempo de desarrollo en días. Cada funcionalidad tiene un grupo de tareas que se ejecutaron en el tiempo establecido dentro de cada iteración denominada Sprint. Del mismo modo cuentan con una descripción dentro del Sprint Backlog.

Tabla 10

Product Backlog Inicial de la plataforma de entrenamiento

Código	Funcionalidad	Estimación en días
RF01	Visualización de inicio al test y concepto de Phishing	4
RF02	Registro de usuario	7
RF03	Visualización de indicaciones	3
RF04	Visualización de ejercicios (simulación de contenido de correo electrónico)	14
RF05	Registro en segundo plano de eventos clic y focus en los enlaces en cada ejercicio	4
RF06	Registro de tiempo en cada ejercicio	4
RF07	Registro de las respuestas del usuario en cada ejercicio	4
RF08	Registro del comentario sobre la respuesta escogida	4
RF09	Visualización y registro de cuestionario de percepción de riesgo	7
RF010	Cálculo y Visualización del Score del usuario	7
RF011	Registro y visualización del nivel de detección del usuario	5
RF012	Visualización de resultados y retroalimentación.	14

Primera Iteración

Para la primera iteración de Sprint se desarrollaron los requisitos funcionales especificados en la Tabla 11, la cual tendrá una duración estimada de 28 días. Estas funcionalidades corresponden al inicio del proyecto el cual será la base para las siguientes iteraciones.

Tabla 11

Descripción de las funcionalidades del Primer Sprint

Código	Funcionalidad	Estimación en días
RF01	Visualización de inicio al test y concepto de Phishing	4
RF02	Registro de usuario	7
RF03	Visualización de indicaciones	3
RF04	Visualización de ejercicios (simulación de contenido de correo electrónico)	14

Sprint Backlog Primera Iteración

En esta primera iteración se delegan tareas para el desarrollo descritas en la Tabla 11, las cuales están vinculadas a los requisitos funcionales que se cumplieron en el primer sprint, adicionalmente, se especificó la fecha de finalización de cada tarea con respecto a la estimación de tiempo presentada en la Tabla 12.

Tabla 12

Spring Backlog correspondiente al primer Sprint.

Nro.	Tarea	Fecha de entrega	Responsable
1	Creación de repositorios en Github.	02/05/2022	Darío Valarezo
2	Creación y configuración de proyectos en Java y Angular.	02/05/2022	Darío Valarezo
3	Subida de proyectos a repositorios de Github.	02/05/2022	Darío Valarezo
4	Realización de prototipo para la página de inicio.	03/05/2022	Diana Arévalo
5	Desarrollo de la vista inicio en Angular.	04/05/2022	Darío Valarezo
6	Prueba de funcionamiento a la vista inicio.	05/05/2022	Darío Valarezo
7	Realización de prototipo para la página de registro.	06/05/2022	Diana Arévalo
8	Creación de modelo para el registro del perfil de cada usuario.	06/05/2022	Diana Arévalo
9	Creación e implementación de la lógica de negocio para el registro.	07/05/2022	Darío Valarezo
10	Creación de End Point para el acceso y/o modificación de datos para el registro.	08/05/2022	Darío Valarezo
11	Prueba de funcionamiento de End Point.	09/05/2022	Diana Arévalo
12	Desarrollo de la vista registro en Angular.	11/05/2022	Darío Valarezo
13	Prueba de funcionamiento de la vista registro.	12/05/2022	Diana Arévalo
14	Realización de prototipo para la página de indicaciones.	13/05/2022	Diana Arévalo
15	Desarrollo y prueba de la vista indicaciones en Angular.	15/05/2022	Diana Arévalo

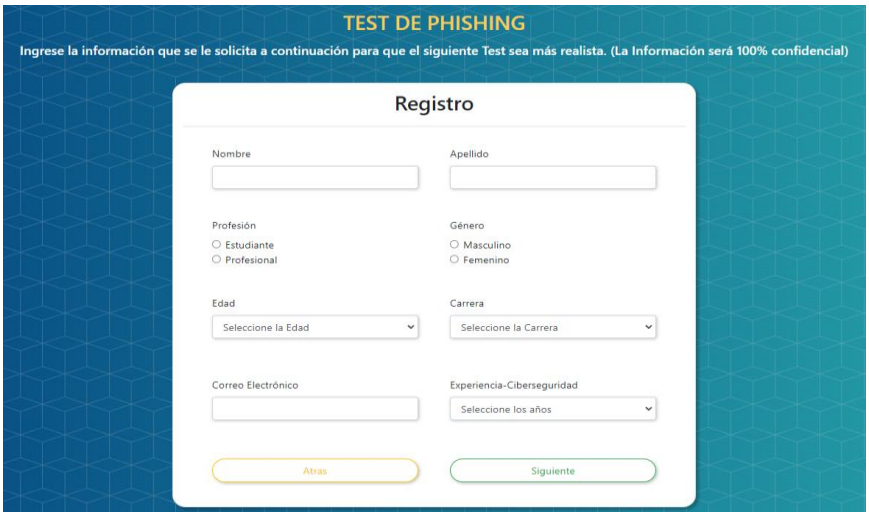
16	Realización de prototipo para la vista play.	16/05/2022	Diana Arévalo
17	Realización de prototipo de 20 ejercicios para la vista play.	17/05/2022	Diana Arévalo y Darío Valarezo
18	Desarrollo de la vista play en Angular.	21/05/2022	Darío Valarezo
19	Implementación de 20 ejercicios en la vista play.	22/05/2022	Darío Valarezo
20	Desarrollo e implementación de un algoritmo para mostrar ejercicios adaptados a las respuestas.	26/05/2022	Diana Arévalo y Darío Valarezo
21	Prueba de funcionamiento al algoritmo implementado.	27/05/2022	Diana Arévalo y Darío Valarezo
23	Implementación de lógica para la identificación de cada ejercicio.	28/05/2022	Diana Arévalo
24	Prueba de funcionamiento de la vista play.	29/05/2022	Diana Arévalo

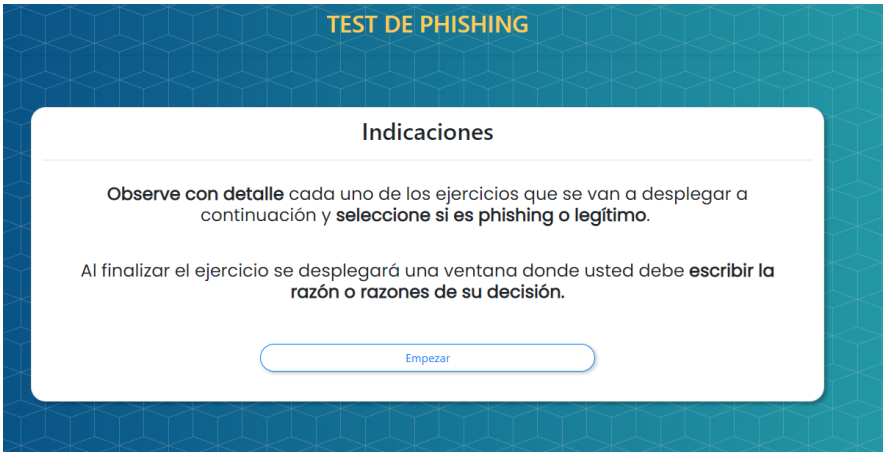
Demostración de la Primer Iteración

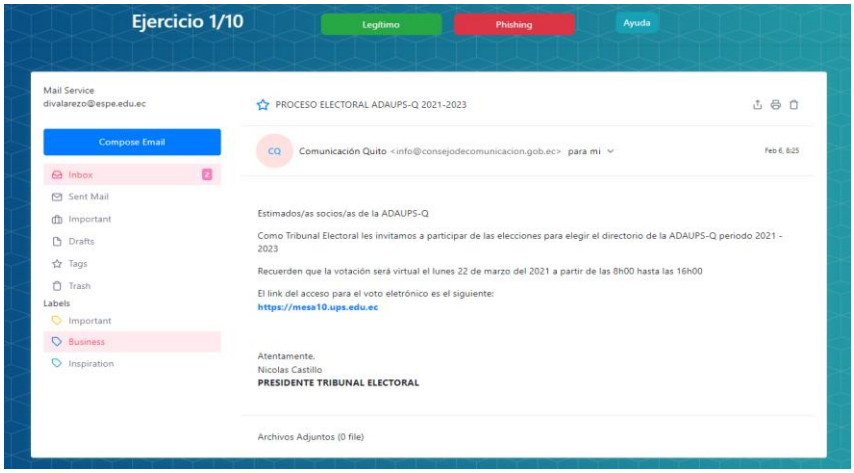
Se presenta a continuación los resultados pertenecientes a la primera iteración, así como la implementación de la visualización de inicio al test y concepto de Phishing, registro de usuario, visualización de indicaciones y la visualización de ejercicios (simulación de contenido de correo electrónico). Esta demostración de las vistas se la visualiza en la Figura 14 y del funcionamiento de las API REST se visualiza en la Figura 15. Posteriormente, en la Tabla 13 se detalla la táctica, el tema, el tipo de URL y las características de cada uno de los 20 ejercicios propuestos.

Figura 14

Demostración Iteración 1



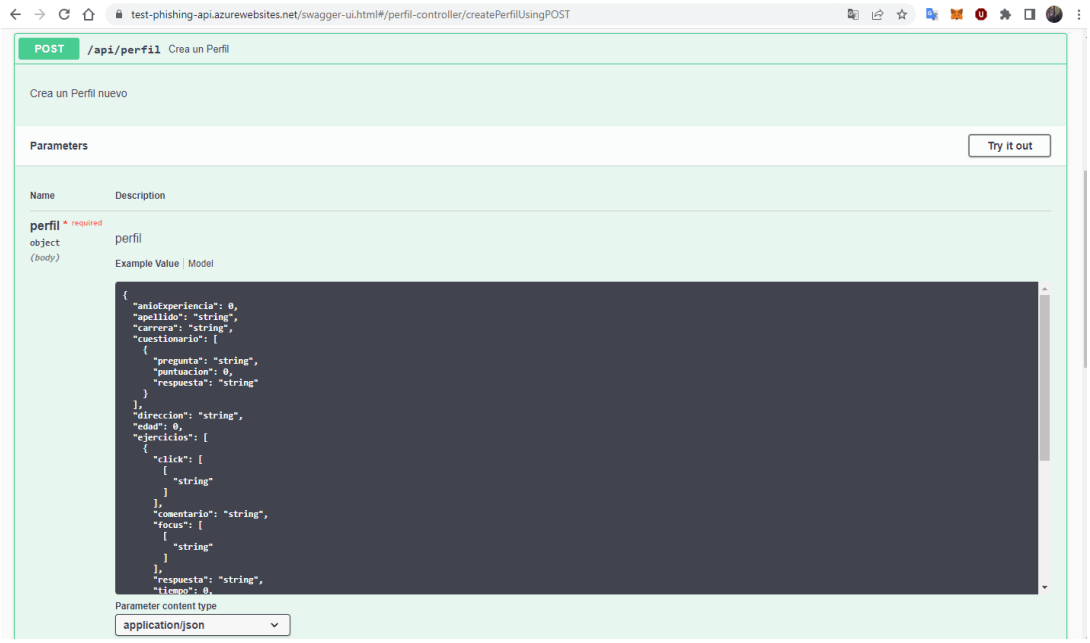


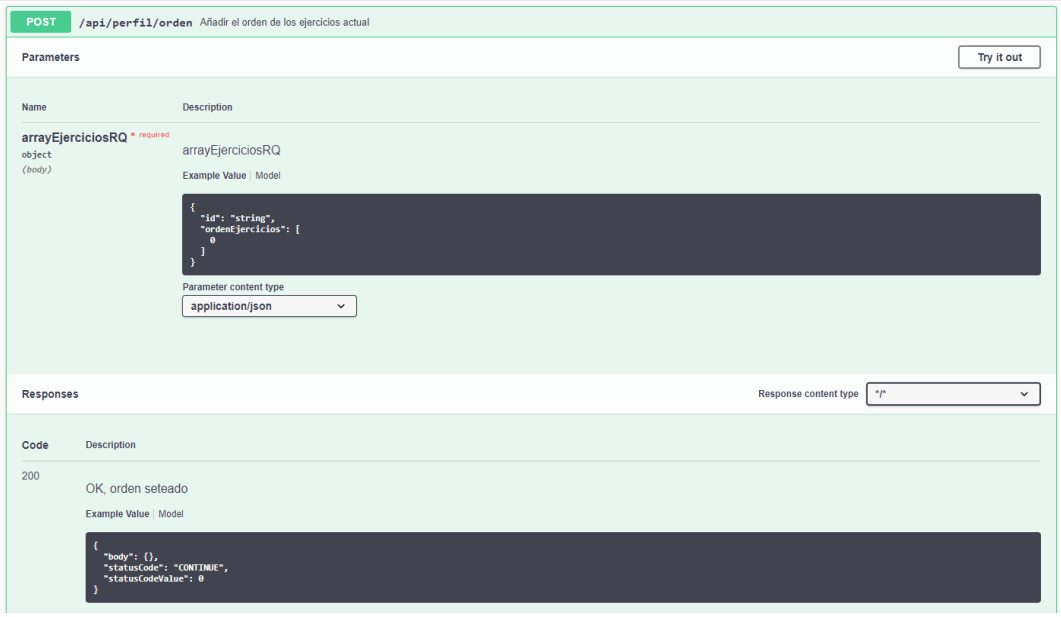


Nota. Estas figuras presentan la vista de inicio, de registro, indicaciones y el ejercicio

Figura 15

Documentación de la API REST





Nota. En estas figuras se presenta la documentación de la API REST implementada

Tabla 13

Planteamiento de los 20 ejercicios de ataques de Phishing por correo electrónico

Nro. EJERCICIO	TEMA	TIPO DE EJERCICIO	TÁCTICA	TIPO DE URL	Características
1	Coronavirus	Phishing	Adjunto .zip	Ofuscación. La URL del archivo .pdf se dirige a una URL desconocida que es "CoronaVirus_Safety.pdf.zip", es decir mientras que se descarga el adjunto en realidad se descarga un archivo comprimido que pretende secuestrar nuestra información.	Saludo y contenido genérico, Contenido persuasivo, tema de interés actual
2	Notificación, Documentación	Phishing	Adjunto .docx	Ofuscación y Texto adicional. La URL a donde se dirige el archivo adjunto en este caso es la siguiente: https://driver.google.com/danna.johonson.docx.exe , la palabra correcta es "drive" y no "driver" la URL correcta empezaría con https://drive.google.com . Además, la URL va dirigida a un archivo ejecutable .exe y no a un documento como el mensaje quiere dar a conocer.	Comunicado institucional usa correo personal, texto corto y preciso, en un ámbito laboral podría causar confusión y credibilidad
3	Suplantación de marca	Phishing	Enlace	Ofuscación y Texto adicional. La URL a la que se dirige el mensaje de CAMBIAR CONTRASEÑA es la siguiente:	Google no envía links para cambio de claves, el saludo es muy informal, el contenido es persuasivo, correo electrónico

				https://wwww.myaccount.google.com-segurity setting-mt.segurity.org/signon/ en este caso se tiene cuatro “w” en el subdominio de la dirección y se dirige a una URL desconocida.	no pertenece al de soporte de Google
4	Notificación	Phishing	Enlace	Ofuscación y Texto Adicional. La URL se esconde detrás del enlace Ver Foto https://wwww.driver.google.com.download-photo.system.net/ft1537PD el enlace se dirige a una URL que tiene un texto adicional, tiene cuatro w en el subdominio del enlace, por lo tanto, no se dirige a un enlace propio de Google Drive. Por otro lado la palabra correcta del dominio es “drive”.	Correo llama la atención del usuario, es corto y preciso, puede causar sospecha, correo de personas desconocidas, Enlace del adjunto es sospechoso, dominio de la foto es raro
5	Oferta de Empleo, Notificación	Phishing	Adjunto .exe	Texto manipulado y Ofuscación. La URL que se presenta no corresponde a una URL original https://www.dropbox/documento_aceptacion.pdf ya que le falta en la dirección la extensión (.com). Así mismo, mientras se posiciona sobre el enlace se visualiza una dirección diferente https://www.dropbox-com.syst.biz/documento_aceptacion.pdf.exe . En el enlace original sería https://www.dropbox.com/ ,	Dominio del Adjunto no es Dropbox, Comunicado institucional usa correo personal, Saludo cordial, Caso real en caso de estar en proceso de búsqueda de trabajo la persona podría ser víctima

				adicionalmente el destino final de la URL es un archivo ejecutable .exe.	
6	Financiero, Suplantación de marca	Phishing	Enlace	Ofuscación, Texto adicional. La URL a la que se dirige es la siguiente: https://www.bancopichincha.com/Verificacion?cliente43524jkr4ish a simple vista se diría que es correcta la dirección. No obstante, mientras se posicione sobre ella la verdadera dirección a la que se dirige es : https://www.bancopichinca.com/cssVerificacion?pagemane=v_cliente43524jkr4ish en la que el dominio no corresponde a la del Banco.	No hay coincidencia de los dominios del correo con el del enlace, contenido llama la atención del usuario, saludo general
7	Financiero, Entrega	Phishing	Enlace	Ofuscación y Texto adicional. La URL que se presenta en el mensaje “Seguros Internacionales”. No obstante al posicionarse sobre el mismo, a la verdadera dirección que se envía es a la siguiente https://seguro-internacional.commonnet/0/deposito/registro.php , donde posiblemente sea un formulario para que el usuario llene con datos importantes	Comunicado institucional usa correo personal, Hace referencia a un retiro de dinero, capta la atención del usuario, el correo de entrada no pertenece al remitente.
8	Notificación	Legítimo	Enlace	Correcta. Esta URL va dirigida a un dominio correcto y la misma URL es la que aparece mientras se	Email proviene de un correo institucional, saludo cordial y formal

				posiciona sobre el enlace al que pide acceder https://mesa10.ups.edu.ec/.	
9	Notificación	Legítimo	Enlace	Correcta. La URL presentada pertenece al dominio de GitHub. Así mismo al colocarse sobre el enlace, la URL a la que se dirige es la misma https://github.blog/2020-12-15-token-authentication-requirements-for-git-operations/	Dominios si pertenecen a GitHub, Caso real
10	Financiero, Notificación	Legítimo		No tiene URL	Correo de notificación del banco, con dominio del mismo, saludo cordial y Formal, Contenido con información concreta
11	Notificación, Marca	Phishing	Enlace	Los enlaces a los que se direcciona con enlaces propios de la plataforma de LinkedIn, en el enlace “Descubre las novedades” se redirecciona a la siguiente dirección https://www.linkedin.com/comm/feed/?midToken=AQEPN7hXTR_l4w por lo que es una dirección correcta	El mensaje solo notifica al usuario, es concreto, no le pide llenar datos, y es una notificación real ya que el dominio del correo de donde proviene el mensaje corresponde al de la empresa
12	Suplantación de marca, Notificación	Phishing	Adjunto .php	Texto adicional. La URL que se presenta no corresponde a ningún enlace seguro proveniente de Amazon o sus dominios oficiales, Amazon tiene la siguiente URL https://www.amazon.com/ la	El correo electrónico notifica que se ganará un premio al contestar una encuesta. Sin embargo, la URL que se adjunta no corresponde a los dominios oficiales. Le muestra

				extensión y el dominio de la URL que muestra el ejercicio son incorrectos, la URL donde se dirige posiblemente sea un formulario para pedir datos personales http://www.b20-amazon.top/amazon/encuesta.php?_t=25468002663	el conteo de minutos restantes para delimitar el accionar y presionar al usuario.
13	Suplantación de marca	Phishing	Enlace	Ofuscación y Texto adicional. La URL que se presenta no corresponde a ningún enlace seguro proveniente de Amazon o sus dominios oficiales, la URL original de Amazon es https://www.amazon.com/ y la que se visualiza en el ejercicio no tiene similitud	La URL no está registrada en los dominios oficiales de la marca comercial, utiliza texto persuasivo para engañar al usuario
14	Coronavirus	Legítimo	Enlace	La URL es correcta, al posicionarse sobre el enlace que se visualiza, este se redirige a esa misma dirección. Así mismo es un enlace correcto de Google forms	El mensaje proviene de un correo electrónico institucional, en este caso del gobierno, el contenido es claro, no pretende pedir información personal
15	Financiero, notificación	Legítimo		No tiene URL	Correo de notificación de ingreso de banca web de una entidad financiera, presenta datos importantes para el usuario, no le pide ingresar a ningún enlace, el mensaje es concreto y preciso

16	Notificación, Entrega	Legítimo		No tiene URL	Correo de notificación de marca comercial, Saludo cordial, Contenido con información de pedido de compra, no pide al usuario un accionar solo notifica
17	Financiero, Notificación	Legítimo		En el botón “Quiero pagar” se redirige a un enlace correcto de la entidad financiera https://click.email.pichincha.com/?qs=735c53834d80f89f5b53f1c3adff0e1e0b43012ae89b9ee4f6f9a2e47321b9de340a93c4b892f1ef228781ef713519978ab43d1cab8774fb y en el mismo contexto en el botón “Pagar en Banca Web” se redirige al Login de la banca Web propia del banco https://click.email.pichincha.com/?qs=782c2cb9bb74da5bf066f3c9bcf33824308458b50cf813e806d211b909ebf12c08ad0d94bbf79b2051934278f6165274036b2719e8adebff	Correo electrónico correcto con dominio del banco, no pide información personal, el contenido directo, URL correctas
18	Notificación, Factura	Legítimo	Archivo adjunto	Los archivos adjuntos no se redireccionan a enlaces distintos, son archivos propios de un formato de factura electrónica.	Correo de notificación de recepción de factura de compra, Saludo cordial y Formal, Contenido con información concreta, el correo electrónico es institucional
19	Notificación	Legítimo	Enlace	Los enlaces son correctos, propios de Udemy https://www.udemy.com/es/, por	Correo electrónico es de una empresa de cursos online, el contenido informativo, no

				ejemplo, el curso de Python, su URL tiene el dominio correcto.	pide accionar ni presiona al usuario
20	Financiero, Notificación	Phishing	Enlace	Texto manipulado. La URL que se presenta no es la que pertenece a la entidad financiera, https://www.bancoguayaquil.com/Extra?Download-html ya que el dominio se muestra es guayaquil con “i l” mayúscula mientras que sería guayaquil con “L”	Correo de notificación del banco, pide al usuario realizar una acción al presionar la URL para lograr un descuento, el contenido es persuasivo, asunto del correo llama la atención del usuario

Segunda Iteración

Para el segundo Sprint se sigue el proceso a partir de las funcionalidades implementadas en la primera iteración, estas se visualizan en la Tabla 14. El tiempo establecido para la finalización de este Sprint es de 23 días. A continuación, se detalla las funcionalidades correspondientes a esta iteración.

Tabla 14

Funcionalidades correspondiente al segundo Sprint

Código	Funcionalidad	Estimación en días
RF05	Registro en segundo plano de eventos clic y focus en los enlaces de cada ejercicio.	4
RF06	Registro de tiempo de cada ejercicio.	4
RF07	Registro de las respuestas del usuario en cada ejercicio.	4
RF08	Registro del comentario sobre la respuesta escogida.	4
RF09	Visualización y registro de cuestionario de percepción de riesgo.	7

Sprint Backlog Segunda Iteración

En esta iteración se delegan nuevamente las tareas para el desarrollo descritas en la Tabla 14, con lo que se cumplió con los siguientes requisitos funcionales que se establecieron para cumplir en este sprint, adicionalmente, se especifica la fecha de finalización de cada tarea con respecto a la estimación de tiempo descrito en la Tabla 15.

Tabla 15

Sprint Backlog correspondiente al segundo Sprint.

Nro.	Tarea	Fecha de entrega	Responsable
1	Desarrollo de EndPoint para el registro de respuestas.	31/05/2022	Darío Valarezo
2	Implementación de eventos en TypeScript.	31/05/2022	Darío Valarezo
3	Registrar eventos en la base de datos	01/06/2022	Darío Valarezo
4	Prueba de funcionamiento de registro de eventos	02/06/2022	Darío Valarezo
5	Desarrollo e implementación de cronómetro	05/06/2022	Diana Arévalo
6	Prueba de funcionamiento de registro de tiempo por pregunta	06/06/2022	Darío Valarezo
7	Desarrollo e implementación de funcionalidad y registro de las respuestas del usuario en cada ejercicio	09/06/2022	Darío Valarezo
8	Prueba de funcionamiento de registro de respuestas	10/06/2022	Diana Arévalo
9	Desarrollo e implementación de funcionalidad y registro de los comentarios del usuario en cada ejercicio	13/06/2022	Diana Arévalo
10	Prueba de funcionamiento de registro de comentario	14/06/2022	Darío Valarezo
11	Realización de prototipo para la vista cuestionario	15/06/2022	Darío Valarezo
12	Diseño de las preguntas y respuestas para el cuestionario	16/06/2022	Diana Arévalo
13	Creación de EndPoint para el registro de las preguntas y respuestas del cuestionario.	18/06/2022	Darío Valarezo

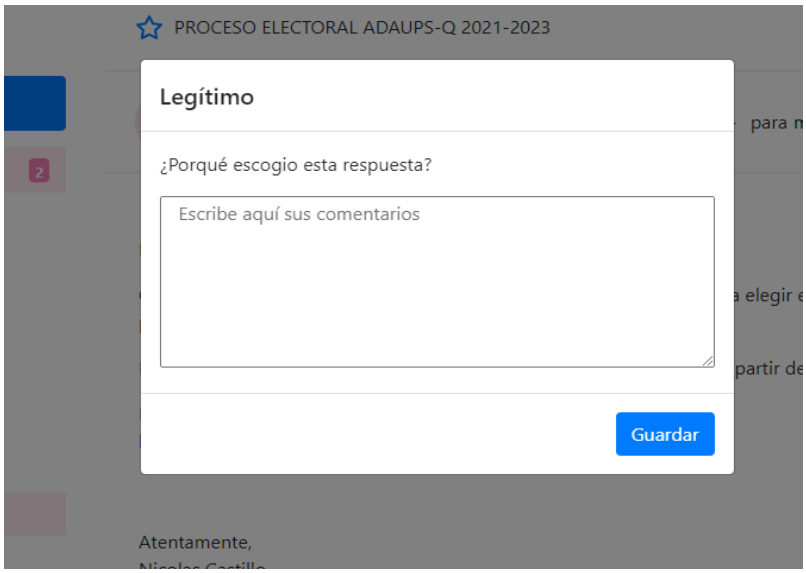
14	Desarrollo de la vista del cuestionario	20/06/2022	Diana Arévalo
15	Prueba de funcionamiento del registro de las preguntas y respuestas del cuestionario.	21/06/2022	Diana Arévalo

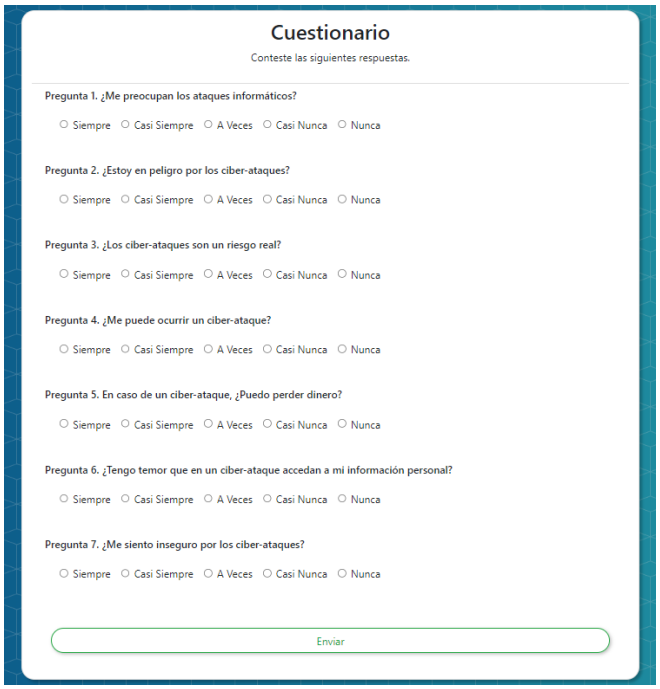
Demostración de la Segunda Iteración

A continuación, se presentan los resultados pertenecientes a la segunda iteración, así como el Registro en segundo plano de eventos clic y focus en los enlaces de cada ejercicio, el registro de tiempo en cada ejercicio, el registro de las respuestas del usuario en cada ejercicio, el registro del comentario sobre la respuesta escogida, la visualización y registro de cuestionarios, esta demostración se visualiza en la Figura 16. Así mismo, en la Figura 17 y 18 se presentan las respectivas demostraciones del funcionamiento del EndPoint para añadir el detalle de los ejercicios y el EndPoint para añadir el cuestionario de percepción de riesgo.

Figura 16

Demostración Iteración 2

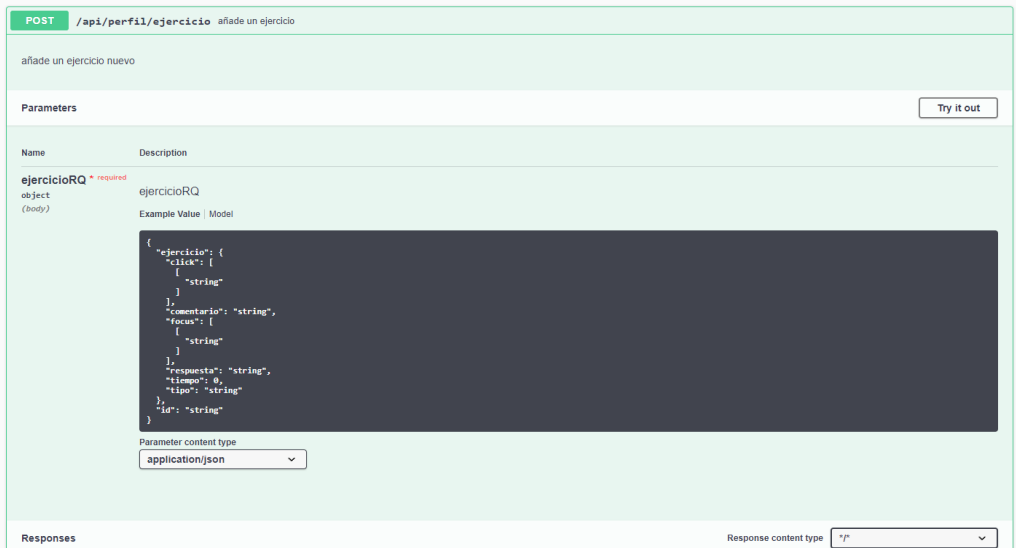




Nota. En estas figuras se visualizan la vista del comentario y la del cuestionario de percepción de riesgo

Figura 17

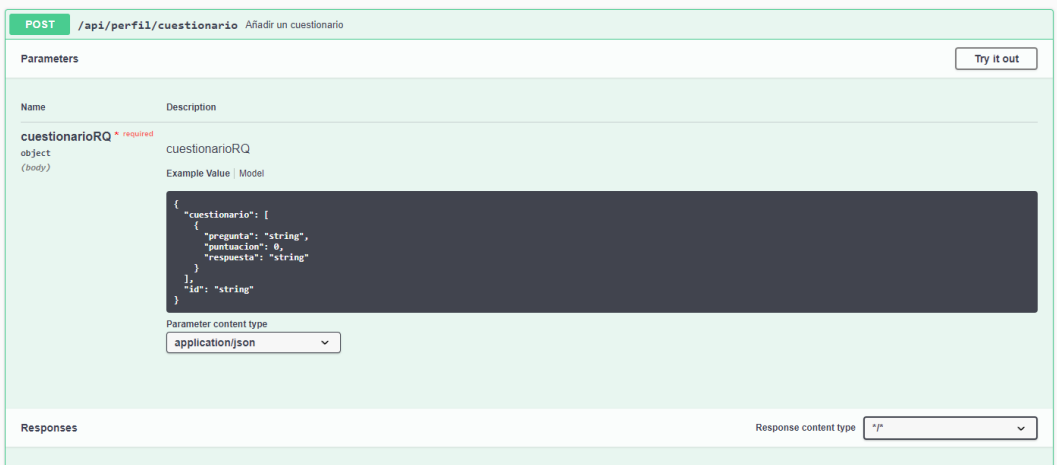
EndPoint para añadir los detalles del ejercicio



Nota. La figura indica el método POST para añadir un ejercicio en la plataforma

Figura 18

EndPoint para añadir las preguntas y respuestas del cuestionario



Nota. La figura indica el método POST para el cuestionario a la plataforma

Tercera Iteración

Para esta tercera y última iteración se cumplió en su totalidad con el desarrollo e implementación de las funcionalidades establecidas, teniendo como resultado el funcionamiento de la plataforma de entrenamiento, para esta interacción se establecido una estimación de 26 días. Por ello en la Tabla 16 se detalla las funcionalidades para la presente iteración.

Tabla 16

Funcionalidades correspondiente al tercer Sprint

Código	Funcionalidad	Estimación en días
RF010	Cálculo y visualización del Score del usuario	7
RF011	Registro y visualización del nivel de detección del usuario	5
RF012	Visualización de resultados y retroalimentación.	14

Sprint Backlog Tercera Iteración

Para cumplir esta última iteración se asignaron 12 tareas con la fecha máxima de entrega, las mismas que completaron el proceso de desarrollo y entrega del producto, ver Tabla 17. En la Figura 19 se visualizan las tareas para finalizar el tercer Sprint.

Tabla 17

Spring Backlog correspondiente al tercer Sprint.

Nro.	Tarea	Fecha de entrega	Responsable
1	Desarrollo e implementación de la lógica para el cálculo del score.	26/06/2022	Darío Valarezo
2	Visualización de score en cada ejercicio	27/06/2022	Darío Valarezo
3	Prueba de funcionamiento de cálculo y visualización del score.	28/06/2022	Darío Valarezo
4	Desarrollo de EndPoint para el registro del nivel de detección.	30/06/2022	Darío Valarezo
5	Desarrollo e implementación de la lógica para el cálculo del nivel de percepción.	02/07/2022	Diana Arévalo
6	Prueba de funcionamiento de registro del nivel de percepción.	03/07/2022	Darío Valarezo
7	Desarrollo de EndPoint para el registro de resultados del test.	08/07/2022	Darío Valarezo
8	Realización de prototipo para la vista de resultados.	09/07/2022	Diana Arévalo
9	Desarrollo e implementación de retroalimentación.	13/07/2022	Diana Arévalo

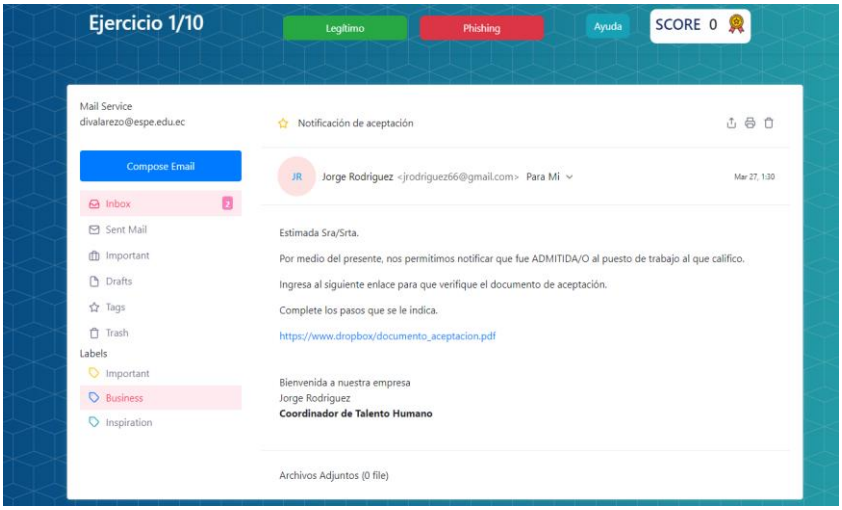
10	Desarrollo e implementación de resultados de los ejercicios.	17/07/2022	Darío Valarezo
11	Desarrollo e implementación de gráficos de nivel de percepción.	21/07/2022	Darío Valarezo
12	Prueba de funcionamiento de la vista de registro	22/07/2022	Diana Arévalo

Demostración de la Tercera Iteración

Para finalizar este proceso en la Figura 19 se presentan los resultados obtenidos en esta iteración, con lo que se cumple de esta manera las funcionalidades y requisitos dentro de la plataforma, es decir se cumple con: el cálculo y visualización del Score del usuario, el registro y visualización del nivel de detección del usuario, la visualización de resultados y retroalimentación.

Figura 19

Demostración Iteración 3



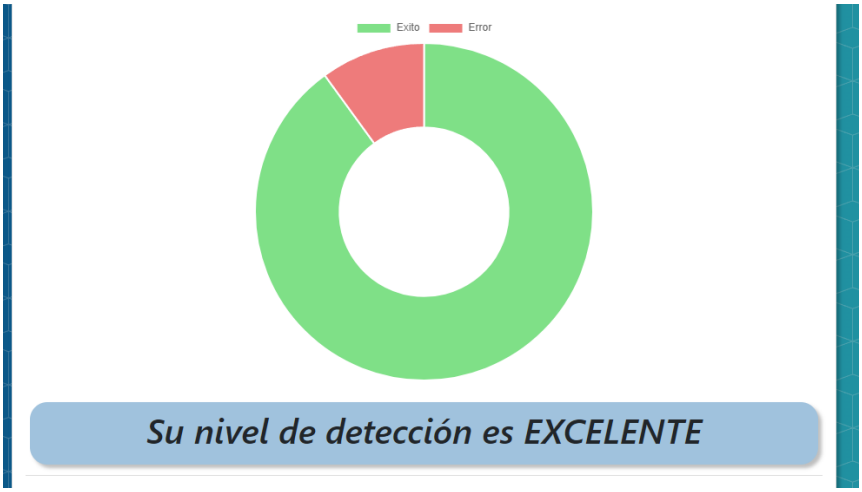
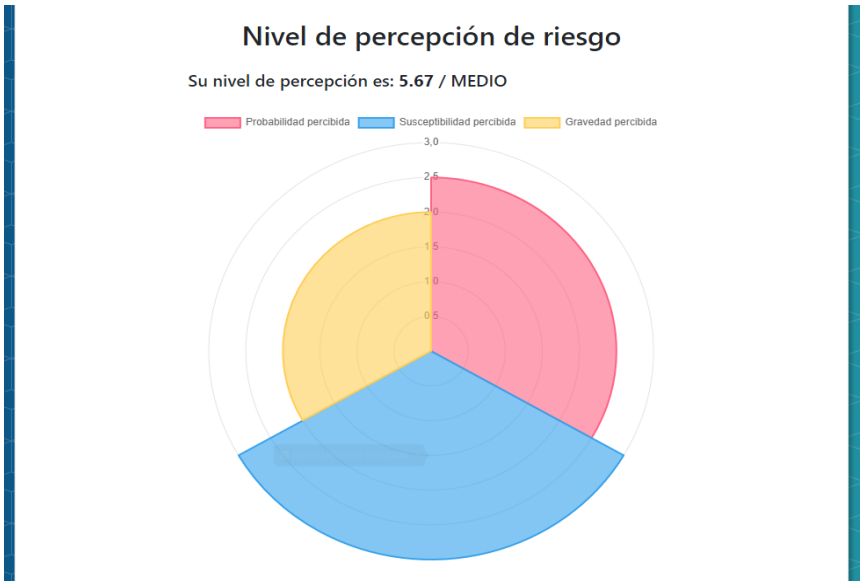
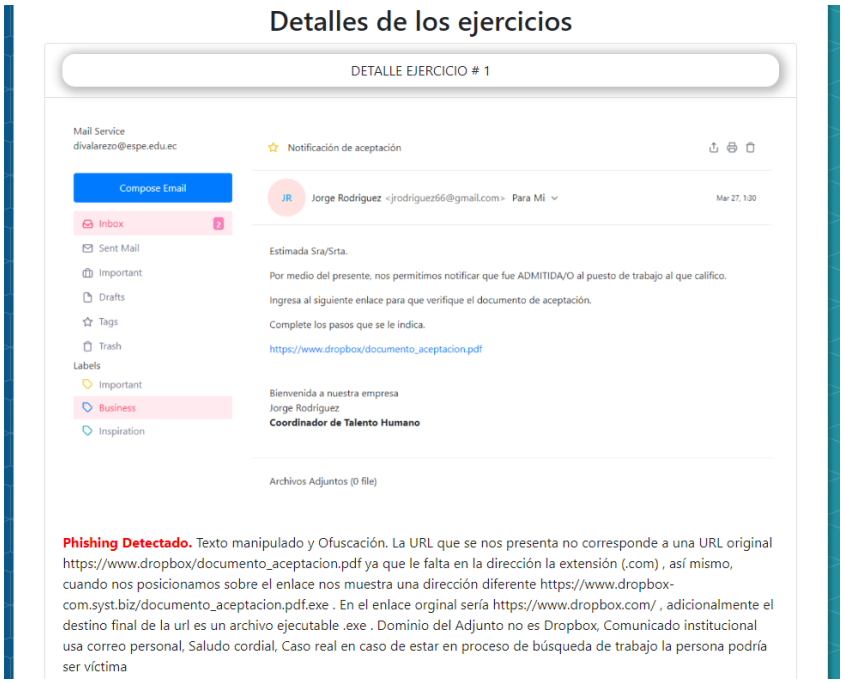


Tabla de Resultados

Ejercicio #	Tipo	Su respuesta	Estado	Tiempo (s)
1	Phishing	Phishing	**Correcto**	381.69
2	Legítimo	Legítimo	**Correcto**	1.53
3	Legítimo	Legítimo	**Correcto**	1.8
4	Phishing	Phishing	**Correcto**	1.46
5	Legítimo	Legítimo	**Correcto**	1.72
6	Legítimo	Legítimo	**Correcto**	1.67
7	Legítimo	Legítimo	**Correcto**	1.92
8	Legítimo	Legítimo	**Correcto**	1.34
9	Phishing	Phishing	**Correcto**	8.29
10	Legítimo	Phishing	**Incorrecto**	2.26





Nota. En las Figuras se despliegan la vista de los resultados y la retroalimentación del entrenamiento dentro de la plataforma de cada usuario

Desarrollo del algoritmo mediante Teoría de juegos con árbol de decisión

La teoría de juegos es capaz de modelar las interacciones que implican a diferentes actores o jugadores, mientras se busca las recompensas resultantes de las acciones óptimas.

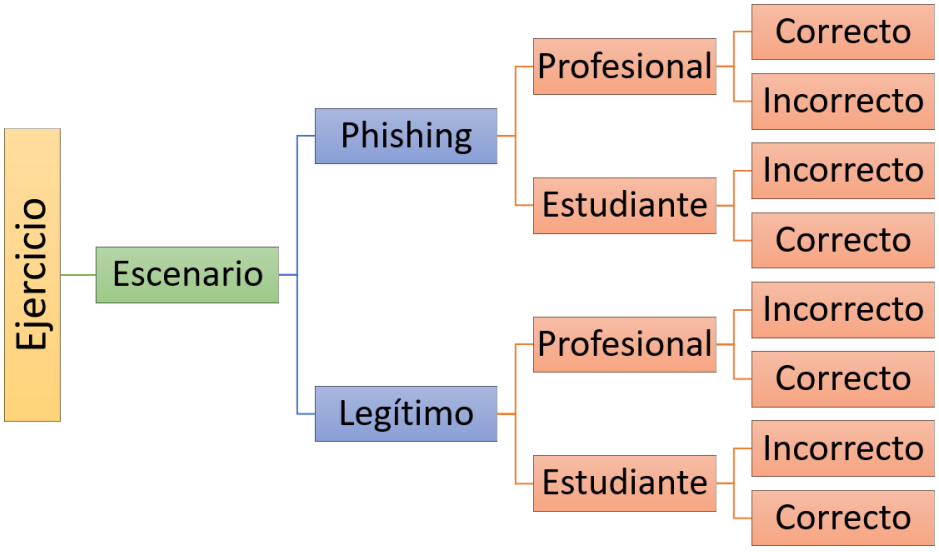
Con la utilización de la teoría de juegos es relevante definir las interacciones estratégicas entre un defensor (es decir, la víctima potencial) y un atacante durante las diferentes etapas de comunicación. Al final, la teoría de juegos proporciona estrategias del defensor para engañar a los atacantes (Tchakounte et al., 2020).

Al ajustar la variación de las técnicas de ataque durante intercambios entre ambos jugadores se modela el presente algoritmo donde el usuario es la víctima exponencial y cada uno de los ejercicios especialmente los de Phishing simula el ataque. Mientras que el usuario falle la detección estaría expuesta relativamente a un ataque de Phishing y cuando acierte la respuesta correcta, es premiado con aumento de puntaje en el score. El escenario es un motivador y cada ejercicio se encuentra dentro de uno o más escenarios, es decir, en el escenario, el atacante cambia sus estrategias a lo largo del tiempo mientras que la víctima (profesional o estudiante) se comporta de forma diferente en función de su nivel de conocimiento. Así mismo, las estrategias son utilizadas para diseñar cada uno de los ejercicios en sus dos categorías: correos electrónicos Phishing y correos electrónicos legítimos. Cabe recalcar que los ejercicios propuestos son simulados y no afectan a la integridad de los jugadores.

Para el desarrollo del algoritmo el primer paso fue definir los escenarios en los que se encontraron los ejercicios propuestos, seguidamente se clasificó estos ejercicios en fáciles, intermedios y difíciles, asignando un puntaje a cada uno de estos niveles, ya que esta es la base del algoritmo. Por último, se tiene la implementación del mismo en la plataforma web. En la Figura 20 se presenta el diseño del árbol de decisión con teorías de juego.

Figura 20

Interacción entre la plataforma web y el jugador en los escenarios



Nota. La Figura muestra el árbol de decisión para cada escenario establecido.

Definición de escenarios

Los escenarios se definieron en relación a los temas de los ejercicios propuestos. Los atacantes construyen correos electrónicos falsos en los que aplican distintas tácticas y los envían a sus víctimas que en este caso son los usuarios o jugadores dentro de la plataforma de entrenamiento. A continuación, se detalla cada uno de los seis escenarios que se tiene establecidos:

ESCENARIO 1

Dentro del tema FINANCIERO es necesario tomar en cuenta:

Escenario de ejercicio Legítimo:

- La entidad no envía enlaces externos
- Archivos de reporte solo manejan formatos .pdf

Escenario de ejercicio Phishing:

- URL con enlace externo, la URL está mal escrita
- Archivo adjunto HTML

ESCENARIO 2

Dentro del tema SUPLANTACIÓN DE MARCA es necesario tomar en cuenta:

Escenario de ejercicio Legítimo:

- La empresa o marca no pide confirmaciones de pagos, anticipos de pagos etc.
- Archivos de reporte solo manejan formatos .pdf
- Archivos de facturas solo manejan en casos especiales formatos .xml

Escenario de ejercicio Phishing:

- URL con enlace externo, la URL está mal escrita
- Correos del destinatario no coinciden con direcciones legítimas de la marca o empresa
- Archivo adjunto HTML o de distinta extensión diferente a formatos establecidos.

ESCENARIO 3

Dentro del tema NOTIFICACIÓN es necesario tomar en cuenta:

Escenario de ejercicio Legítimo:

- Las empresas envían notificaciones mediante los correos electrónicos institucionales
- URL va dirigida a un dominio correcto de la institución
- Archivos adjuntos son en formatos conocido como .pdf, .png
- No se necesita ingresar algún enlace para solicitar información.

Escenario de ejercicio Phishing:

- URL con enlace externo, la URL con texto manipulado
- Falta ortográfica en el texto del contenido del correo electrónico

- El asunto del correo presenta una alerta
- El correo solicita realizar alguna acción para entregar información

ESCENARIO 4

Dentro del tema CORONAVIRUS es necesario tomar en cuenta:

Escenario de ejercicio Legítimo:

- Solo empresas de salud pública e instituciones informan y envían correos con información sobre el coronavirus
- Archivos adjuntos son de formatos .pdf, .png
- Contenido directo y preciso, sin faltas ortográficas.

Escenario de ejercicio Phishing:

- Contexto de correo en idioma inglés, contenido genérico y persuasivo, tema de interés actual
- Asunto del correo con contenido alarmante
- La URL presenta ofuscación, texto adicional o texto manipulado.

ESCENARIO 5

Dentro del tema OFERTA DE EMPLEO es necesario tomar en cuenta:

Escenario de ejercicio Legítimo:

- Las empresas mandan información sobre ofertas de trabajos refiriéndose al propietario del correo.
- La estructura de los enlaces es legítima.
- Archivos adjuntos son de formatos .pdf, .png
- Contenido directo y preciso, sin faltas ortográficas.

Escenario de ejercicio Phishing:

- Contexto de correo en idioma inglés, contenido genérico y persuasivo, captación de dinero.
- Asunto del correo con contenido alarmante
- La URL presenta ofuscación, texto adicional o texto manipulado.

ESCENARIO 6

Dentro del tema ORDEN DE COMPRA / ENTREGA O FACTURA es necesario tomar en cuenta:

Escenario de ejercicio Legítimo:

- El contenido del correo electrónico sugiere la verificación de compra sin pedir datos personales, datos sensibles de tarjeta de banco.
- Archivos adjuntos son de formatos .pdf, .png
- Contenido directo y preciso, sin faltas ortográficas.

Escenario de ejercicio Phishing:

- Contexto de correo en idioma inglés, contenido genérico y persuasivo, captación de dinero.
- La URL presenta ofuscación, texto adicional o texto manipulado.

Clasificación de ejercicios

Para una adecuada retroalimentación del algoritmo se procedió a una primera recolección de datos, la cual ayudó a tener la información necesaria para conocer qué ejercicios fueron en los que más se equivocaron y acertaron los usuarios. Es así que, para este proceso de clasificación de los ejercicios en fáciles, intermedios y difíciles se centró en la Escala de Likert de dificultad, que es una escala de calificación utilizada para cuestionar a una persona qué tan de acuerdo o en desacuerdo está con una afirmación. Así mismo, es ideal para medir las

reacciones, actitudes y comportamiento de un individuo (QuestionPro, 2016). Cabe recalcar que se realizó un pilotaje con 30 participantes, estos realizaron el entrenamiento en la plataforma y a partir de sus errores y aciertos se procedió a analizar, establecer rangos y determinar la dificultad de cada ejercicio. Los ejercicios con menos aciertos se clasificaron como difíciles, seguidos de los intermedios, y los ejercicios con un mayor número de aciertos se los clasificó en el rango de fáciles. En la Tabla 18 se detalla la dificultad con el número de ejercicios correspondientes a cada categoría.

Tabla 18

Clasificación de los ejercicios

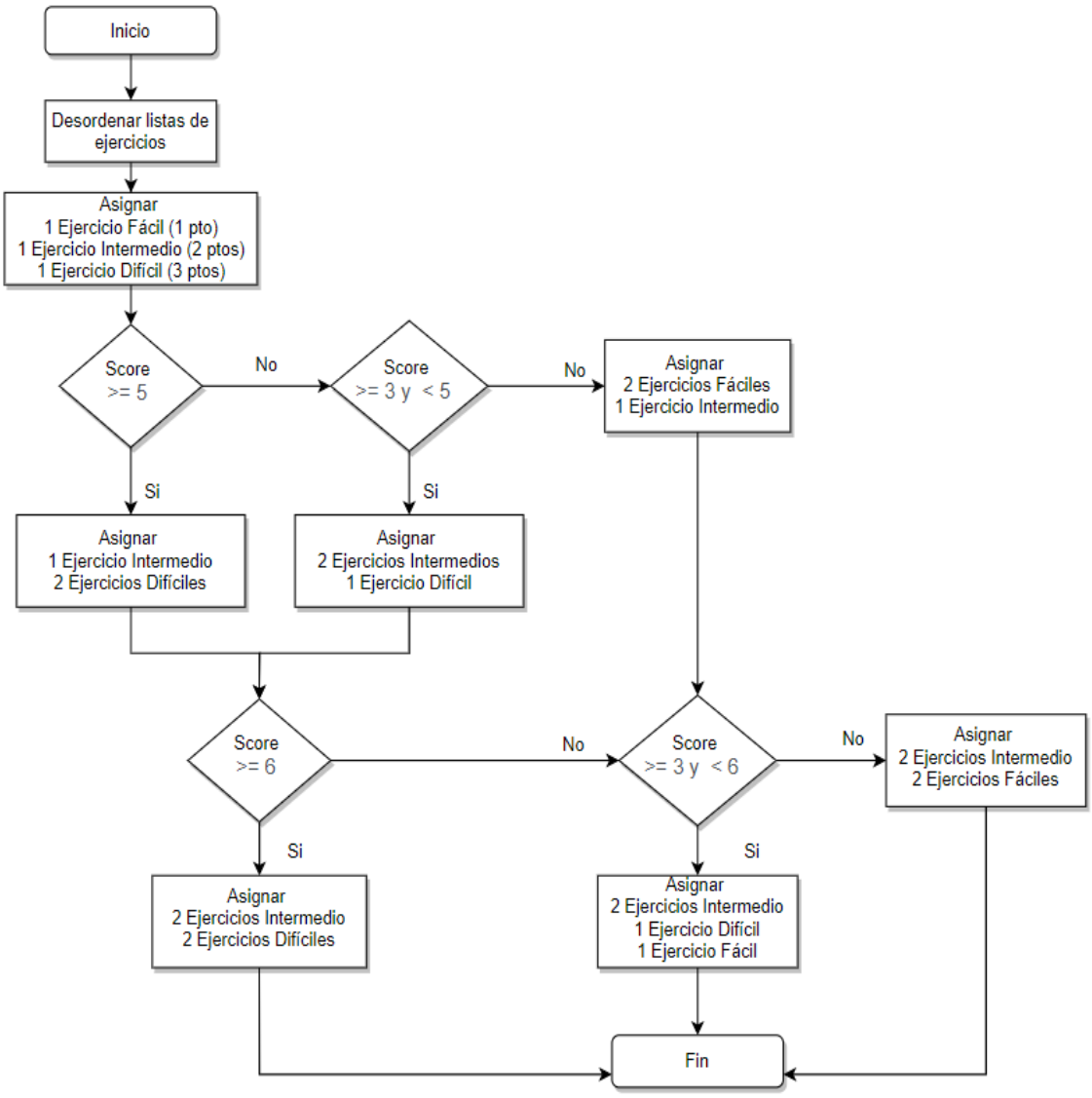
Puntaje Asignado	**Dificultad**	**Nro. de Ejercicios**
3 puntos	Difícil	Ejercicio 2 Ejercicio 11 Ejercicio 14 Ejercicio 18 Ejercicio 19
2 puntos	Intermedio	Ejercicio 1 Ejercicio 3 Ejercicio 9 Ejercicio 10 Ejercicio 17
1 punto	Fácil	Ejercicio 4 Ejercicio 5 Ejercicio 6 Ejercicio 7 Ejercicio 8 Ejercicio 12 Ejercicio 13 Ejercicio 15 Ejercicio 16 Ejercicio 20

Desarrollo del algoritmo mediante teoría de juegos con árboles de decisión

En efecto, la víctima potencial es el objetivo de los ataques que intentan atraerla en diferentes etapas. El ataque puede tener éxito a su primer envío de correo electrónico y si no lo consigue lo vuelve a intentar hasta alcanzar el objetivo. De este modo se diseñó el algoritmo, al iniciar el entrenamiento al usuario o jugador se le asigna tres ejercicios aleatorios de cada una de las dificultades establecidas, es decir, un ejercicio fácil con una equivalencia de 1 punto, un intermedio que equivale a 2 puntos y un difícil equivale a 3 puntos, a partir de estas respuestas y del score o puntación acumulada se le asignan los siguientes ejercicios hasta completar un número de 10 ejercicios, que son los que debe cumplir el jugador para terminar con el entrenamiento. Cabe recalcar que la puntuación máxima que el usuario puede obtener es de 24 puntos que corresponde al nivel establecido como difícil y una puntuación menor pertenece a un nivel intermedio o fácil. Todo este proceso se detalla en el siguiente diagrama de flujo. En la Figura 21 se especifica el funcionamiento del algoritmo en la plataforma:

Figura 21

Diagrama de flujo del algoritmo implementado



Nota. La figura exhibe el proceso a seguir del algoritmo implementado con lógica de teorías de juego en la plataforma para la selección de ejercicios con relación al score obtenido.

Capítulo V

Pruebas y análisis de resultados

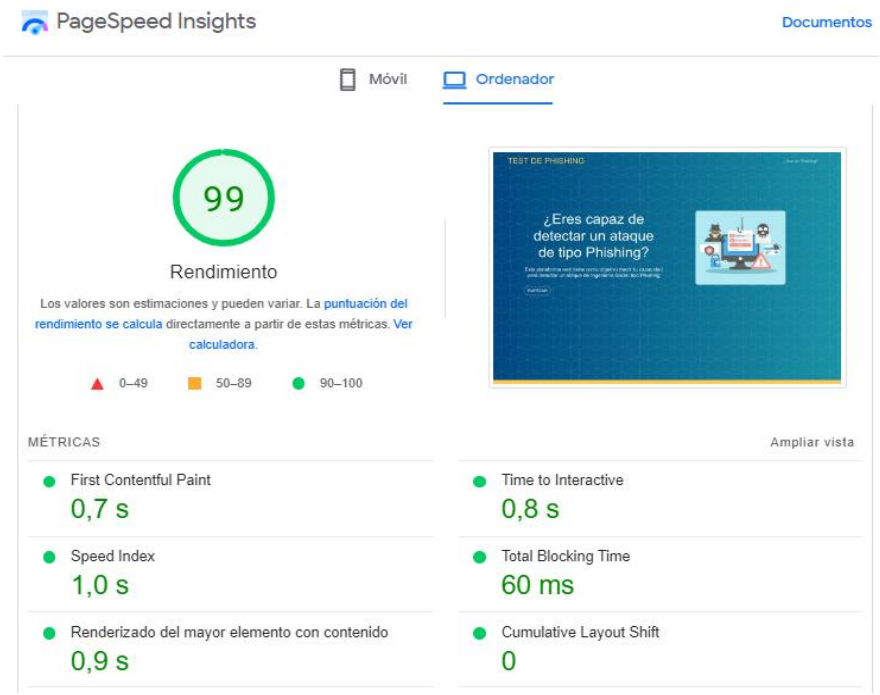
Luego de haber concluido con el desarrollo de la plataforma web de entrenamiento y de la implementación del algoritmo, se realizaron las pruebas correspondientes con el fin de cumplir con todos los requerimientos establecidos. Es así que se ejecutaron pruebas de rendimiento, velocidad y de usabilidad de la plataforma conforme a la norma ISO 25010 (ISO 25010, s. f.), como se presenta a continuación.

Prueba de Rendimiento

Para probar el rendimiento de la plataforma de entrenamiento se utilizó la herramienta PageSpeed Insights (PSI) (PageSpeed, s. f.), la cual informa sobre el performance de una página en dispositivos móviles y de escritorio. Además, brinda sugerencias sobre cómo se puede mejorar esa página, ya que proporciona datos de laboratorio y de campo sobre una página. Los datos de laboratorio son útiles para depurar problemas de rendimiento, puesto que se recopilan en un entorno controlado. Los datos de campo son útiles para capturar la verdadera experiencia del usuario en el mundo real (PageSpeed, s. f.). A continuación, en la Figura 22 se presentan los resultados de rendimiento de la plataforma mediante la herramienta PSI en el ordenador, donde se obtuvo un valor de 99 %. Este resultado refleja que su rendimiento es bueno ya que se encuentra dentro del rango de 90 a 100, el índice de velocidad es de 1,0 segundos y el renderizado del mayor elemento con contenido es de 0,9 segundos. Cabe recalcar que la herramienta hace la prueba en un escritorio emulado.

Figura 22

Rendimiento de la plataforma de entrenamiento



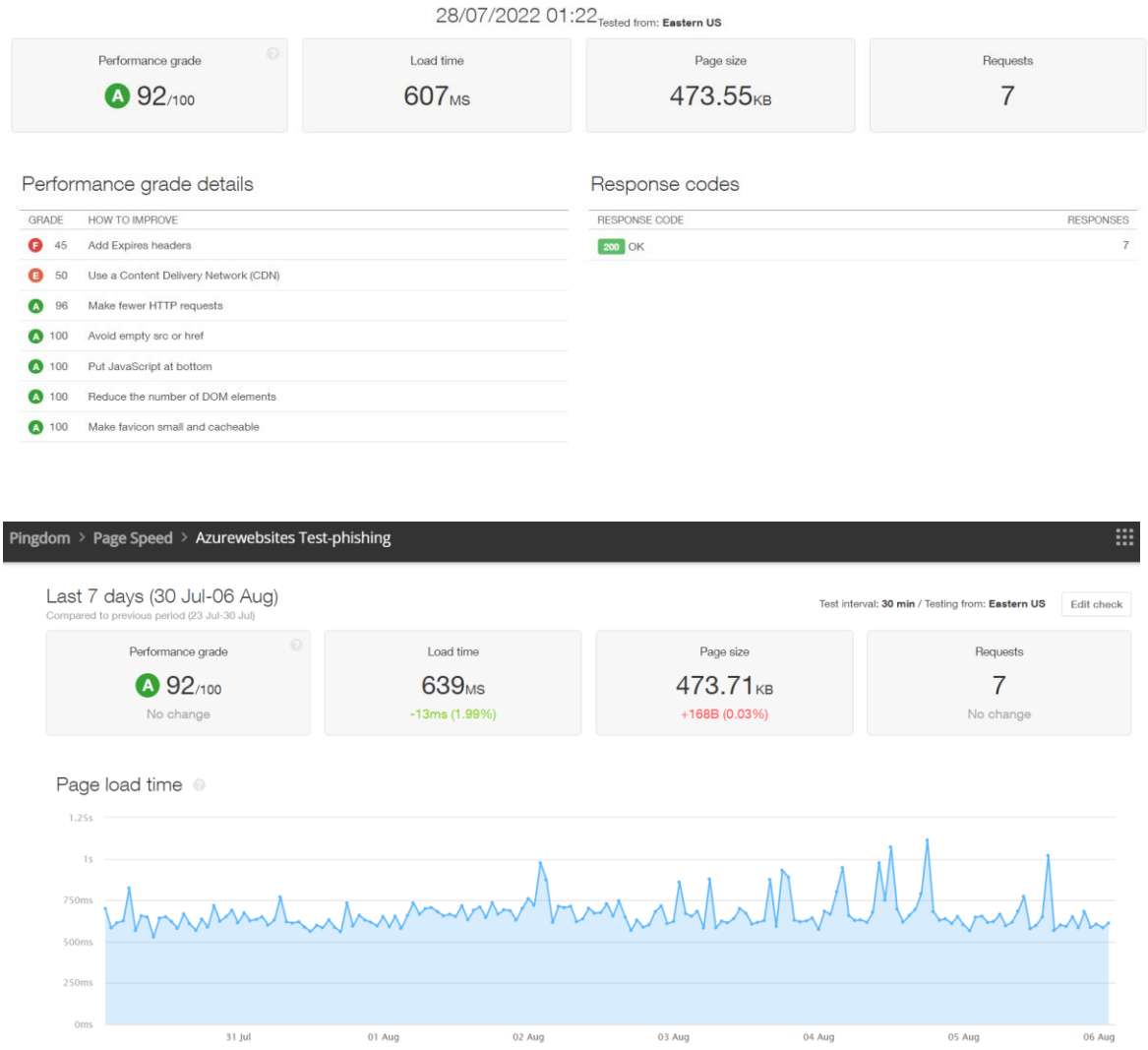
Nota. En la Figura se visualiza la descripción de los indicadores de medición con las que se obtiene el rendimiento dentro de la herramienta PSI.

Prueba de Velocidad

Para evaluar la velocidad de la plataforma de entrenamiento se utilizó la herramienta Pingdom (Pingdom, s. f.), la cual es un recurso integral que facilita la supervisión de una página o sitio web. Así mismo, ofrece la posibilidad de obtener visibilidad de cómo los usuarios finales reales interactúan con su sitio web y cómo lo experimentan (Pingdom, s. f.). En la Figura 23 se expone el resultado de la prueba de velocidad mediante el ingreso del enlace respectivo de la plataforma en Pingdom. El performance obtenido es de 92 sobre 100, se logró un tiempo de carga de 607 milisegundos durante 7 días, esto verifica la rapidez con la que los usuarios pueden acceder sin ningún inconveniente y esto es favorable en sentido de usabilidad.

Figura 23

Prueba de velocidad de la plataforma web en Pingdom



Nota. Los gráficos indican el monitoreo de la plataforma durante 7 días en la herramienta de Pingdom

Prueba de Usabilidad

Una de las pruebas significativas para saber cómo los usuarios interactúan con la plataforma web es la prueba de usabilidad. Para ello se tomó en consideración lo que menciona la norma ISO 25010, la que define a la Usabilidad como la “Capacidad del producto software

para ser entendido, aprendido, usado y resultar atractivo para el usuario, donde se usa bajo determinadas condiciones”(ISO 25010, s. f.). Esta característica se subdivide a su vez en:

- Capacidad para reconocer su adecuación.
- Capacidad de aprendizaje.
- Capacidad para ser usado.
- Protección contra errores de usuario.
- Estética de la interfaz de usuario.
- Accesibilidad.

De acuerdo con el estudio presentado por (Sharfina & Santoso, 2016), se indica que un aspecto clave del desarrollo de productos, es evaluar la usabilidad. Es así que, dentro de los métodos de evaluación más utilizados está la Escala de Usabilidad del Sistema en sus siglas en inglés System Usability Scale (SUS).

El SUS es una herramienta independiente de la tecnología que consta de diez preguntas con cinco respuestas para cada pregunta que van desde "totalmente de acuerdo" hasta "totalmente en desacuerdo" (Klug, 2017). Los diez ítems establecidos de la escala se los visualiza en la Tabla 19:

Tabla 19

Cuestionario de usabilidad SUS

Nro.	Pregunta	Completamente en desacuerdo				Completamente de acuerdo
1	Creo que me gustaría utilizar este sistema frecuentemente	1	2	3	4	5
2	El sistema me resultó difícil de usar.	1	2	3	4	5
3	Creo que el sistema es bastante fácil de utilizar.	1	2	3	4	5

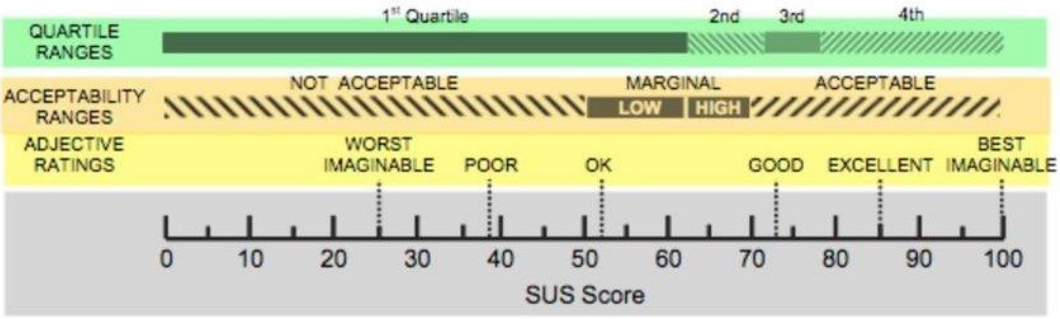
4	Creo que necesitaría el soporte de un técnico para poder utilizar este sistema.	1	2	3	4	5
5	Creo que las diferentes funciones del sistema se encuentran muy bien integradas.	1	2	3	4	5
6	Opino que hubo demasiada inconsistencia en el sistema.	1	2	3	4	5
7	Imagino que la mayoría de las personas aprendería a utilizar el sistema rápidamente.	1	2	3	4	5
8	Me sentí algo incómodo al utilizar este sistema.	1	2	3	4	5
9	Me sentí muy seguro al utilizar este sistema.	1	2	3	4	5
10	Necesito aprender muchas otras cosas antes de poder utilizar correctamente el sistema.	1	2	3	4	5

Cabe recalcar que el cuestionario SUS fue aplicado a cada uno de los usuarios que realizaron el entrenamiento en la plataforma, con el fin de conocer la usabilidad de la misma. Este establece que, de las diez preguntas, cinco son positivas (1, 3, 5, 7 y 9) y cinco son negativas (2, 4, 6, 8 y 10).

Ya recolectados los datos, el siguiente paso es realizar la ponderación de la puntuación del SUS. En la Figura 24 se observa la ponderación de la puntuación del SUS señalada, esta se divide en cinco opciones de evaluación como son Excelente, Bueno, OK, Malo y Pésimo. Aquí están los detalles:

Figura 24

Escala SUS



Nota. La figura indica las escalas de medición de SUS. Tomada de (Franco et al., 2019)

Al realizar los cálculos correspondientes de una población de 59 usuarios entre ellos estudiantes y profesionales, se adoptaron los lineamientos de medición del cuestionario. En la Tabla 20 se detalla el cálculo realizado para la obtención del porcentaje de usabilidad. Como se observa que la plataforma de entrenamiento obtuvo una usabilidad del 85,12 % lo que significa que está dentro de la escala aceptable y tiende a ser de buena a excelente. Cabe enfatizar que se puede mejorar en los aspectos en los que se tiene una puntuación baja.

Tabla 20

Cálculos para obtener el porcentaje de usabilidad SUS

Nro. Pregunta	Promedio de Preguntas impares	Promedio de preguntas pares
1	4,58	
2		1,61
3	4,46	
4		1,66
5	4,32	
6		1,63
7	4,53	
8		1,56
9	4,27	
10		1,64
SUMA	22,15	8,10

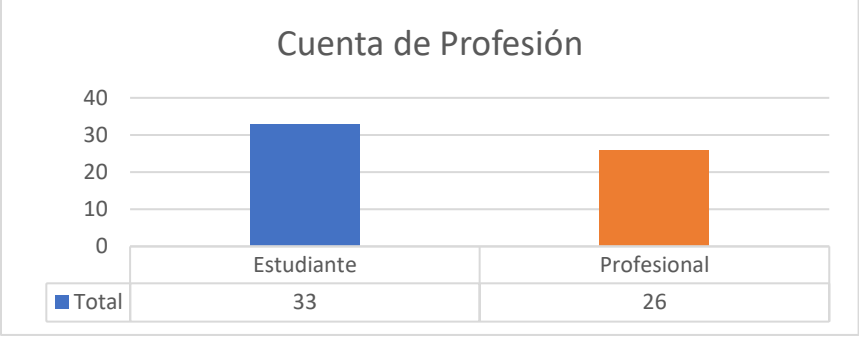
Cálculos SUS	22,15 – 5 = 17,15	25 - 8,10 =16,898
	Sumar los dos resultados y multiplicar por 2,5	
	Porcentaje de Usabilidad SUS	**85,12**

Resultados

Como parte de los resultados obtenidos del grupo de 59 usuarios, entre ellos estudiantes y profesionales, como se observa en la Figura 25, quienes realizaron el entrenamiento se tiene los siguientes análisis:

Figura 25

Número de Usuarios que realizaron el entrenamiento



Nota. En la figura se detalla el número de estudiantes y profesionales en el pilotaje de toma de datos.

Caminos de los usuarios en la plataforma

Para responder al objetivo específico cuatro, los caminos establecidos en el algoritmo se asignaron en el transcurso del entrenamiento por los usuarios al escoger de forma correcta o incorrecta la respuesta. Es así que en la Tabla 21 se detalla los caminos que recorrieron los profesionales, en donde se observa que la mayoría contestaron bien los tres primeros ejercicios, por lo tanto, el camino a seguir fue el difícil, posterior se observa que en algunos casos los

profesionales volvieron a tener ejercicios difíciles que corresponden al camino dos. Sin embargo, hay casos donde las respuestas no fueron correctas y el algoritmo asignó ejercicios intermedios o fáciles para el segundo camino. Todo este proceso fue determinante para obtener el score final, donde en algunos escenarios el resultado fue el máximo puntaje que equivale a 24 puntos.

Tabla 21

Detalle de caminos según el score obtenido por los profesionales

Profesión	Score1	Camino1	Score2	Camino2	Score3	Suma - Score Final
Profesional	6	Difícil	8	Difícil	10	24
Profesional	6	Difícil	8	Difícil	5	19
Profesional	5	Difícil	8	Difícil	10	23
Profesional	6	Difícil	6	Difícil	10	22
Profesional	4	Intermedio	2	Fácil	4	10
Profesional	1	Fácil	3	Intermedio	3	7
Profesional	4	Intermedio	7	Difícil	10	21
Profesional	6	Difícil	0	Fácil	6	12
Profesional	6	Difícil	8	Difícil	10	24
Profesional	6	Difícil	5	Intermedio	8	19
Profesional	6	Difícil	5	Intermedio	5	16
Profesional	1	Fácil	1	Fácil	3	5
Profesional	6	Difícil	5	Intermedio	8	19
Profesional	6	Difícil	6	Difícil	7	19
Profesional	6	Difícil	5	Intermedio	8	19
Profesional	6	Difícil	8	Difícil	10	24
Profesional	6	Difícil	5	Intermedio	8	19
Profesional	6	Difícil	2	Fácil	6	14
Profesional	6	Difícil	8	Difícil	10	24
Profesional	6	Difícil	8	Difícil	3	17
Profesional	6	Difícil	3	Intermedio	3	12
Profesional	6	Difícil	6	Difícil	7	19
Profesional	6	Difícil	5	Intermedio	8	19
Profesional	4	Intermedio	7	Difícil	10	21
Profesional	6	Difícil	8	Difícil	10	24
Profesional	6	Difícil	5	Intermedio	3	14

En la Tabla 22 se detalla los caminos que recorrieron los estudiantes, se puede observar que sus respuestas van entre 3 y 6 puntos, es decir, el camino que siguieron es el difícil y el intermedio. Posterior se observa que se mantiene el mismo nivel en el segundo camino. Sin embargo, hay casos en los que los estudiantes mejoraron su detección y el algoritmo les asignó un nivel superior que corresponde al difícil, caso contrario su puntuación disminuyó y fueron asignados a un nivel inferior o fácil.

Tabla 22

Detalle de caminos según el score obtenido por los profesionales

Profesión	Score1	Camino1	Score2	Camino2	Score3	Suma - Score Final
Estudiante	6	Difícil	2	Fácil	5	13
Estudiante	3	Intermedio	5	Intermedio	3	11
Estudiante	3	Intermedio	7	Difícil	10	20
Estudiante	6	Difícil	8	Difícil	0	14
Estudiante	3	Intermedio	5	Intermedio	6	14
Estudiante	6	Difícil	8	Difícil	7	21
Estudiante	3	Intermedio	4	Intermedio	8	15
Estudiante	3	Intermedio	7	Difícil	7	17
Estudiante	3	Intermedio	7	Difícil	7	17
Estudiante	3	Intermedio	4	Intermedio	5	12
Estudiante	6	Difícil	8	Difícil	5	19
Estudiante	4	Intermedio	4	Intermedio	8	16
Estudiante	5	Difícil	2	Fácil	2	9
Estudiante	1	Fácil	4	Intermedio	5	10
Estudiante	6	Difícil	5	Intermedio	6	17
Estudiante	3	Intermedio	4	Intermedio	5	12
Estudiante	6	Difícil	8	Difícil	6	20
Estudiante	6	Difícil	8	Difícil	10	24
Estudiante	3	Intermedio	2	Fácil	6	11
Estudiante	5	Difícil	2	Fácil	6	13
Estudiante	2	Fácil	2	Fácil	6	10
Estudiante	2	Fácil	4	Intermedio	6	12
Estudiante	6	Difícil	8	Difícil	8	22
Estudiante	3	Intermedio	0	Fácil	4	7
Estudiante	6	Difícil	0	Fácil	3	9
Estudiante	6	Difícil	8	Difícil	10	24

Estudiante	4	Intermedio	7	Difícil	5	16
Estudiante	1	Fácil	4	Intermedio	3	8
Estudiante	6	Difícil	6	Difícil	7	19
Estudiante	6	Difícil	5	Intermedio	5	16
Estudiante	6	Difícil	8	Difícil	5	19
Estudiante	3	Intermedio	5	Intermedio	4	12
Estudiante	3	Intermedio	4	Intermedio	5	12

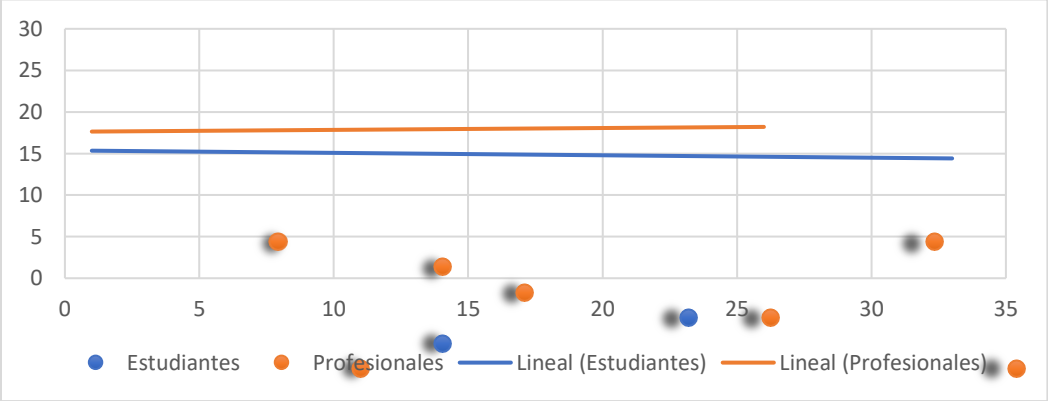
Promedio del score final de los usuarios

En el siguiente diagrama de dispersión (ver Figura 26) se observa que el puntaje de los profesionales se mantiene en un promedio de 17 – 18 puntos, que se corrobora con su tendencia lineal, es decir su detección fue buena o excelente. Sin embargo, existen 2 datos atípicos, en el universo de la muestra de los profesionales (7 y 5 puntos en el score final). Lo que representa un 7,69% de valores inconsistentes.

Por otro lado, se tiene la dispersión de los puntajes de los estudiantes, como se observa en la Figura 26, estos se mantienen en un promedio de 14 – 15 puntos, es decir que su nivel de detección es intermedio y mantienen la tendencia lineal.

Figura 26

Diagrama de dispersión del score final de los usuarios



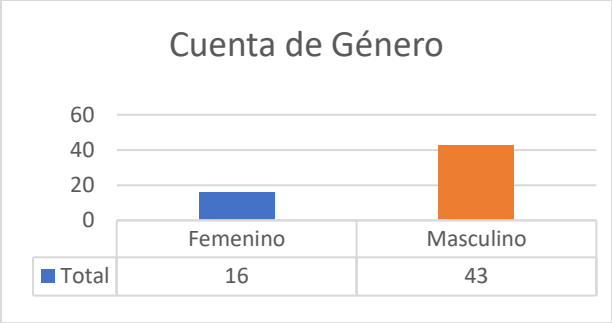
Nota. En la figura se visualiza la dispersión de los datos de profesionales y estudiantes.

Nivel de detección de Phishing por género

Con respecto al quinto objetivo específico, se realizó el análisis respectivo de los factores humanos como son la edad y el género. La recolección de datos se realizó a 59 personas, desglosadas de la siguiente manera: 16 (27,12%) mujeres y 43 (72,88 %) hombres, como se observa en la Figura 27.

Figura 27

Cantidad de usuarios por género

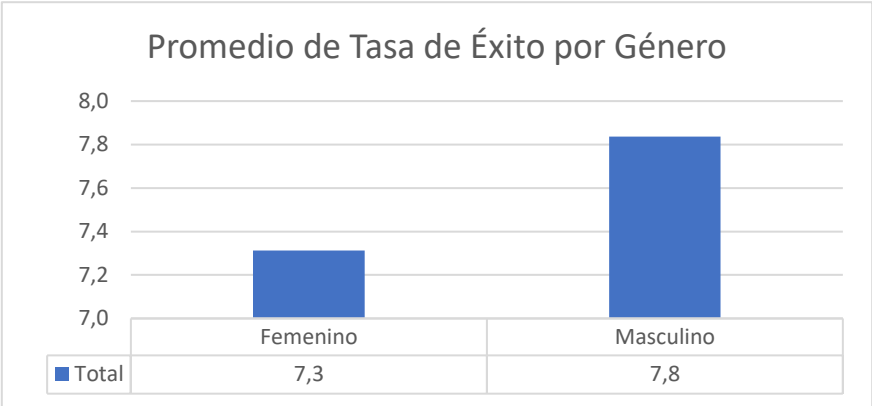


Nota. Esta figura detalla el número de usuarios en género masculino y femenino

En la Figura 28 se observa que, en el género femenino no existe un nivel bajo de detección de Phishing al realizar el entrenamiento en la plataforma, mientras que en el género masculino existe un nivel bajo con un promedio de 4 aciertos. Adicionalmente, el porcentaje de aciertos del género masculino es mayor que el del género femenino.

Figura 28

Niveles de detección de Phishing por género



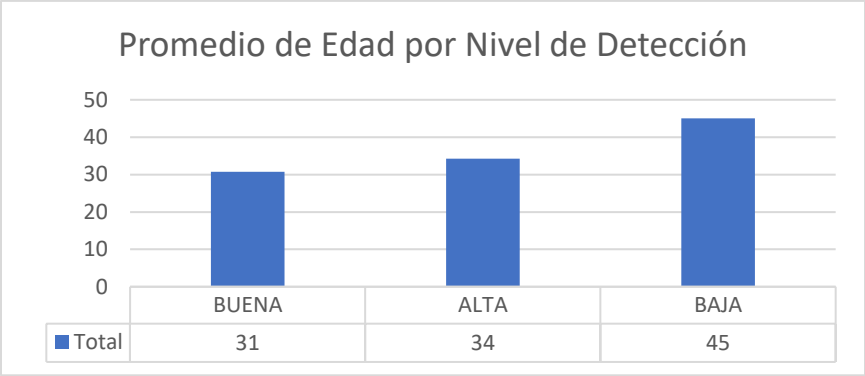
Nota. En la figura se detalla los promedios por género en cada nivel de detección

Nivel de detección de Phishing por edad

A continuación, en la Figura 29 se detalla que el promedio de edad de los usuarios que respondieron correctamente y obtuvieron un alto nivel de detección están entre los 34 años, mientras que en un nivel intermedio o bueno está en un promedio de 31 años, y en un nivel bajo de detección se dio en un promedio de edad de 45 años. Lo que se observa es que el nivel de aciertos es inversamente proporcional a la edad, es decir, a mayor edad la cantidad de ciertos disminuye y viceversa.

Figura 29

Niveles de detección de Phishing por edad



Nota. En la figura se visualiza el promedio de las edades con un nivel de detección alto, medio y bajo.

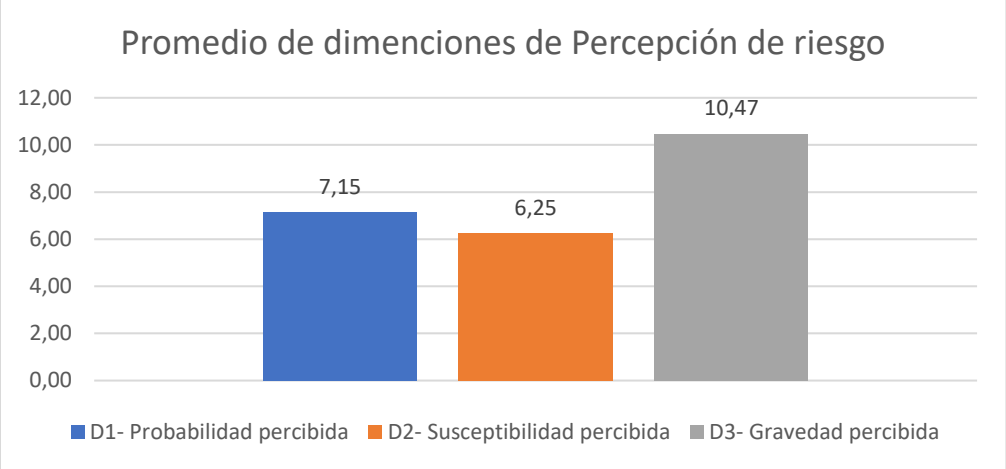
Nivel de Percepción de riesgo por cada dimensión

Dentro del aspecto de la psicología cognitiva se procedió a recolectar datos de la percepción de riesgo mediante el cuestionario establecido, con el que se obtuvo los siguientes resultados en cada dimensión, como se observa en la Figura 30. Cabe recalcar que para las dos primeras dimensiones se estableció un rango de nivel de percepción que corresponde a un nivel alto para el promedio mayor o igual a 6, para un nivel medio un promedio de 4 hasta 6 y para un nivel bajo de 0 hasta 4. Sin embargo, para la dimensión tres el promedio para el nivel alto es mayor o igual a 8, para un nivel medio de 5 hasta 8, y para un nivel bajo menores que 5.

Al comparar las tres dimensiones, es decir, la Probabilidad percibida, Susceptibilidad percibida y Gravedad percibida, se concluyó que sus promedios están en el nivel alto, por lo tanto, la mayoría de los 59 usuarios que realizaron el entrenamiento tienen un alto nivel de percepción de riesgo.

Figura 30

Promedio de las tres dimensiones de percepción de riesgo



Nota. En la figura se visualiza el promedio de cada dimensión por nivel de percepción

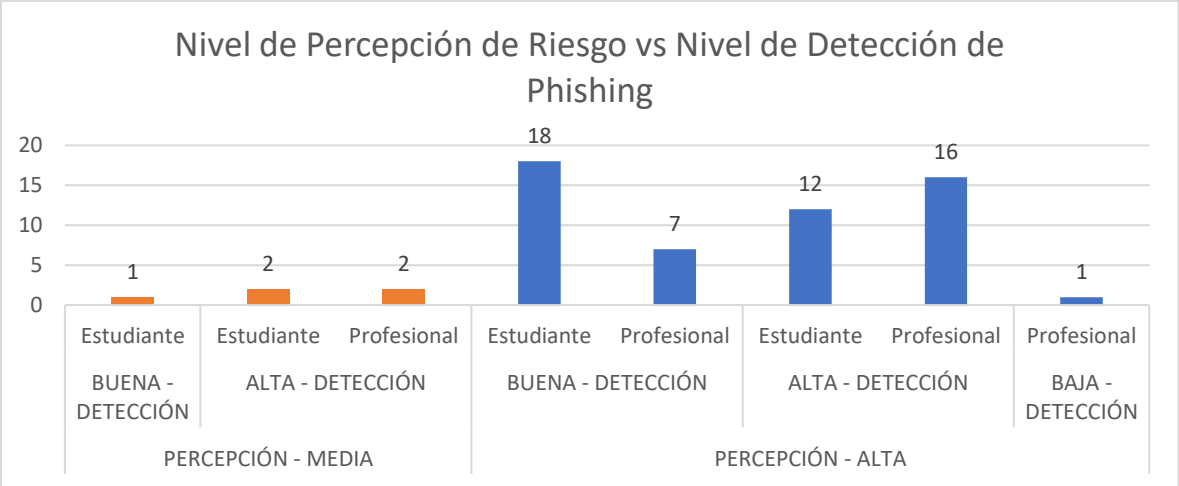
Comparativa entre el nivel de percepción de riesgo con el nivel de detección de Phishing

En la Figura 31 se visualiza que: un estudiante tiene una buena detección de Phishing y una percepción de riesgo media y a su vez, un profesional tiene una baja detección al realizar el entrenamiento, sin embargo, tiene una alta percepción de riesgo. Estos datos se los puede considerar atípicos, ya que no puede ser que un profesional tenga una alta percepción de ciberataques y en contraste una baja puntuación en el entrenamiento.

Un dato significativo es que, 18 estudiantes y 7 profesionales tienen una buena detección de Phishing en el entrenamiento y una alta percepción de riesgo. Así mismo, en el caso exitoso, 16 profesionales y 12 estudiantes tienen una alta detección en el entrenamiento y a su vez tienen una alta percepción de riesgo. Con estos datos se concluyó que el 88,46% (23 profesionales) y 75,75% (25 estudiantes) tienen una percepción de riesgo alta y un promedio elevado de detección de Phishing.

Figura 31

Nivel de percepción de riesgo en comparativa con el nivel de detección



Nota. En esta figura se detalla el nivel de percepción de riesgo vs el nivel de detección de Phishing en la plataforma de entrenamiento.

Análisis de los comentarios de los usuarios al seleccionar la respuesta

Los usuarios al seleccionar la respuesta de cada uno de los ejercicios en el entrenamiento escribieron la o las razones del porqué de su decisión. Al tener estos comentarios, se generó una nube con las palabras más significativas, mediante la utilización de la herramienta en línea Wordart (Word Art, s. f.), la cual contiene múltiples configuraciones para la generación de gráficos con las palabras con más concurrencia en una oración. Además, esta herramienta permite editar la fuente y estilo, así como también la edición de palabras para suprimir pronombres repetitivos.

Es así que en la Figura 32 se muestra una representación visual con las palabras que usualmente el usuario asoció para establecer su respuesta, ya sea Phishing o legítimo. Entre las palabras que frecuentemente utilizaron se hallan: correo, dominio, link, enlace, URL, archivo,

remitente, dato, información, cuerpo. Se concluyó que, para tomar la decisión de respuesta, los usuarios tienden a revisar dentro de los ejercicios los enlaces, el dominio de procedencia del correo electrónico, así como su remitente, la información contenida en el cuerpo del mensaje y el tipo de archivo adjunto.

Figura 32

Palabras que los usuarios asociaron para su decisión

Nota. En la figura se visualiza el conjunto de palabras que más repitieron los usuarios al dar el comentario del porqué de su decisión.

Capítulo VI

Conclusiones Y Recomendaciones

Conclusiones

- En el presente estudio se presentó una revisión sistemática de Literatura de las técnicas, métodos y herramientas actuales de seguridad y psicología cognitiva donde se involucra al factor humano en la detección de Phishing. Se encontró que existen varias técnicas para aplicar seguridad cognitiva como es la Inteligencia artificial, aprendizaje automático, minería de datos, Big Data, teorías de juego, entre otras. Así mismo, se identificó que la susceptibilidad, la percepción del riesgo, el estrés, el miedo, incluso en algunos casos los datos demográficos, influyen en que un usuario sea vulnerable a ciberataques como es el caso de Phishing.
- La utilización de metodologías ágiles, en este caso SCRUM permitió un desarrollo sólido y una comunicación efectiva entre los desarrolladores y el cliente, que en este caso fueron los expertos en psicología y ciberseguridad. Así mismo, garantiza llevar una organización de requerimientos determinante para el cumplimiento en el tiempo establecido para la implementación de las funcionalidades.
- El manejo de microservicios con el framework Spring Boot facilitó el desarrollo y la implementación de la API REST que expone los servicios para la obtención, almacenamiento y modificación de los datos que se registran de cada uno de los usuarios en la base de datos MongoDB Atlas, los cuales son consumidos por el Front-End.
- Se utilizó el framework Angular para el desarrollo de las interfaces gráficas que pertenecen al Front-End para el cumplimiento de los requerimientos funcionales de la

plataforma, ya que proporcionó librerías que facilitaron el desarrollo y la conexión con el Back-End.

- Para el despliegue de la plataforma de entrenamiento se eligieron los servicios en la nube de Microsoft Azure, ya que proporcionó las herramientas necesarias para un despliegue adecuado y permitió tener un acceso seguro a la plataforma por parte de los usuarios.
- El porcentaje de usabilidad obtenido mediante el cuestionario SUS a la población de 59 usuarios es de 85,12, lo cual indicó que tuvieron una experiencia aceptable que tiende a ser excelente al realizar el entrenamiento en la plataforma.
- Se desarrolló e implementó un algoritmo basado en la teoría de juegos en la plataforma de entrenamiento, que permitió determinar los tres niveles (difícil, intermedio y fácil), donde el profesional tanto como el estudiante pudieron avanzar con respecto a sus respuestas y el puntaje asignado. Se concluyó que los profesionales tienden a obtener caminos difíciles y la mayoría mantuvieron el mismo nivel de dificultad correspondiente al segundo camino para concluir con un resultado exitoso y una detección efectiva. Sin embargo, los estudiantes obtuvieron niveles de dificultad difíciles e intermedios, para los dos caminos, con lo que obtuvieron así, un resultado final de detección media.
- El nivel de detección de Phishing por género dio como resultado que las mujeres tuvieron un nivel alto y bueno, mientras que los hombres tuvieron un nivel de detección alto, bueno y bajo. Por otra parte, cabe mencionar que en el promedio de edad entre los 45 años tuvieron un nivel de detección bajo, mientras que un promedio entre los 34 años su nivel fue alto y entre los 31 años un nivel de detección bueno. También, es importante recalcar que en los datos obtenidos se visualizó que los años de experiencia en ciberseguridad no influyeron en la detección de Phishing dentro del entrenamiento.

- El promedio de percepción de riesgo de la población es alto en sus tres dimensiones (Probabilidad percibida, Susceptibilidad percibida y Gravedad percibida). No obstante, se tiene que el nivel de detección es bueno o medio, por lo tanto, se puede decir que existe una confianza por parte de los usuarios al percibir y detectar un ataque Phishing, sin tener en cuenta que existe la probabilidad de ser víctimas de dichos ataques.

Recomendaciones

- Se recomienda la utilización de herramientas como Rayyan que permiten tener un control significativo de la revisión sistemática de literatura, así como también se puede hacer un trabajo colaborativo y tener un buen resultado.
- Se recomienda que, al utilizar SCRUM, se debe mantener reuniones constantes con los expertos que permita un cumplimiento de las tareas en el tiempo establecido y no exista ningún contratiempo. Además, para tener un control de desarrollo colaborativo se recomienda utilizar GitHub, repositorio que permite tener un respaldo y versiones del código.
- Se sugiere utilizar las buenas prácticas de programación como Clean Code (código limpio) para tener una calidad considerable, de la misma forma tener mantenimiento y diseño de código.
- Se recomienda que antes de desarrollar el Front-End se realice prototipos del diseño. Así mismo se utilicen frameworks de estilo de diseño como Bootstrap para agilizar el desarrollo de las interfaces gráficas de la plataforma de entrenamiento.
- Para el despliegue de la aplicación se recomienda buscar una plataforma de servicios en la nube que permita realizar las configuraciones necesarias para una integración y

distribución continuas (CI/CD). Del mismo modo, se recomienda utilizar un framework como DevOps para optimizar el tiempo de desarrollo.

- Para mejorar el porcentaje de la usabilidad se propone realizar una inducción previa a los usuarios con el fin de guiar en la navegación de la plataforma, así como también tomar en cuenta en qué preguntas del cuestionario SUS obtuvo un menor puntaje para corregir estos aspectos.
- Se sugiere aumentar la cantidad de ejercicios en sus niveles difíciles, intermedios y fáciles, del mismo modo, profundizar en la investigación para replicar correos electrónicos Phishing y aumentar la dificultad de los mismos. Cabe mencionar que el algoritmo es modificable y se lo puede retroalimentar con la ampliación de los ejercicios para cada uno de los caminos.
- Es aconsejable tener la misma cantidad de población en género para realizar comparaciones. Del mismo modo se debe aumentar la población de entrenamiento para obtener mayores cantidades de datos y se pueda analizar mediante Big Data o aprendizaje automático con el fin de conocer en profundidad los factores humanos que influyen en un ataque tipo Phishing.
- Al aumentar la población se deberá tener en cuenta seguir con el proceso de entrenamiento a los usuarios dentro de empresas, organizaciones o instituciones para conseguir una validez acertada del cuestionario de percepción de riesgo, y a su vez, ayudar a las personas en la capacitación sobre ataques Phishing en correos electrónicos.

Trabajo Futuro

Para continuar el presente estudio se podría implementar un algoritmo con redes neuronales dentro del proceso de visualización de ejercicios con respecto al perfil del usuario, de forma que garantice así, un mejor entrenamiento ante ataques de tipo Phishing.

Un aporte significativo sería adaptar la plataforma a dispositivos móviles, ya que en la actual versión se encuentra direccionada a ser utilizada en computadoras, con el fin de incrementar la detección de Phishing en distintos escenarios.

Referencias

A Younis, Y., & Musbah, M. (2020, junio 14). *A Framework to Protect Against Phishing Attacks*. https://doi.org/10.1145/3410352.3410825

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, *8*(1), 5. https://doi.org/10.1186/s13673-018-0128-7

Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1), 7. https://doi.org/10.1186/s42400-020-00047-5

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: Toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing*, *25*(5), 829-841. https://doi.org/10.1007/s00779-021-01551-2

Alturki, A., Alshwihi, N., & Algarni, A. (2020). Factors Influencing Players' Susceptibility to Social Engineering in Social Gaming Networks. *IEEE Access*, *8*, 97383-97391. https://doi.org/10.1109/ACCESS.2020.2995619

Altvater, A. (2017, septiembre 17). *What is Agile Methodology? How It Works, Best Practices, Tools*. Stackify. https://stackify.com/agile-methodology/

Amankwa, E., Loock, M., & Kritzinger, E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, 248-252. https://doi.org/10.1109/ICITST.2014.7038814

Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications*, *48*, 102352. https://doi.org/10.1016/j.jisa.2019.06.008

Andrade, R., & Torres, J. (2018). Self-Awareness as an enabler of Cognitive Security. *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 701-708. https://doi.org/10.1109/IEMCON.2018.8614798

Andrade, R., Torres, J., & Cadena, S. (2019). Cognitive Security for Incident Management Process. En Á. Rocha, C. Ferrás, & M. Paredes (Eds.), *Information Technology and Systems* (pp. 612-621). Springer International Publishing. https://doi.org/10.1007/978-3-030-11890-7_59

Angular. (s. f.). *Angular*. Recuperado 28 de julio de 2022, de https://angular.io/guide/what-is-angular

Atlassian. (s. f.). *Learn about the main artifacts of agile scrum including prod*. Atlassian. Recuperado 29 de julio de 2022, de https://www.atlassian.com/agile/scrum/artifacts

Austerlitz, H. (2003). CHAPTER 13—Computer Programming Languages. En H. Austerlitz (Ed.), *Data Acquisition Techniques Using PCs (Second Edition)* (pp. 326-360). Academic Press. https://doi.org/10.1016/B978-012068377-2/50013-9

Beltrán, L. G. M. (2016). JAVA como lenguaje universal de programación. *XIKUA Boletín Científico de la Escuela Superior de Tlahuelilpan*, *4*(8), Article 8. https://doi.org/10.29057/xikua.v4i8.332

Brewer, N. T., Chapman, G. B., Gibbons, F. X., Gerrard, M., McCaul, K. D., & Weinstein, N. D. (2007). Meta-analysis of the relationship between risk perception and health behavior: The example of vaccination. *Health Psychology*, *26*(2), 136-145. https://doi.org/10.1037/0278-6133.26.2.136

Brief: The role of cybersecurity and data security in the digital economy. (s. f.). UNCDF Policy Accelerator. Recuperado 17 de junio de 2022, de https://policyaccelerator.uncdf.org/policy-tools/brief-cybersecurity-digital-economy

Brinton Anderson, B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: A NeuroIS research agenda and empirical study. *European Journal of Information Systems*, *25*(4), 364-390. https://doi.org/10.1057/ejis.2015.21

Brooker, G. (1984). An Assessment of an Expanded Measure of Perceived Risk. *ACR North American Advances*, *NA-11*. https://www.acrwebsite.org/volumes/6292/volumes/v11/NA-11/full

Burke, S. (2021). How to prepare for the onslaught of phishing email attacks. *Computer Fraud & Security*, *2021*(5), 12-14. https://doi.org/10.1016/S1361-3723(21)00053-1

Bushong, V., Das, D., Al Maruf, A., & Cerny, T. (2021). Using Static Analysis to Address Microservice Architecture Reconstruction. *2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 1199-1201. https://doi.org/10.1109/ASE51524.2021.9678749

C3L Security. (2021, marzo 15). Cognitive Psychology and Cybersecurity. *C3L Security*. https://blog.c3l-security.com/2021/03/cognitive-psychology-and-cybersecurity.html

Carroll, F., Adejobi, J. A., & Montasari, R. (2022). How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society. *SN Computer Science*, *3*(2), 170. https://doi.org/10.1007/s42979-022-01069-1

Castillo, J. A. G. del. (2012). Concepto De Percepción De Riesgo Y Su Repercusión En Las Adicciones. *Salud y drogas*, *12*(2), 133-151.

Cazares, M. F., Arévalo, D., Andrade, R. O., Fuertes, W., & Sánchez-Rubio, M. (2022). A Training Web Platform to Improve Cognitive Skills for Phishing Attacks Detection. En A. K. Nagar, D. S. Jat, G. Marín-Raventós, & D. K. Mishra (Eds.), *Intelligent Sustainable Systems* (pp. 33-42). Springer Nature. https://doi.org/10.1007/978-981-16-6309-3_4

Chaudhry, J., Chaudhry, S., & Rittenhouse, R. (2016). Phishing Attacks and Defenses. *International Journal of Security and Its Applications*, *10*, 247-256. https://doi.org/10.14257/ijsia.2016.10.1.23

Cho, J.-H., Cam, H., & Oltramari, A. (2016). Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, 7-13. https://doi.org/10.1109/COGSIMA.2016.7497779

Cisco. (2021). *Cybersecurity threat trends: Phishing, crypto top the list*. Cisco Umbrella. https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

Collins, J., & Buttera, D. (2016). IBM cognitive tools in research and education. *Proceedings of the 26th Annual International Conference on Computer Science and Software Engineering*, 333-334.

Confense. (2020, junio 4). *Phishing Email Database | Real Phishing Email Examples*. https://cofense.com/real-phishing-examples-and-threats/

Conteh, N. Y., & Schmick, P. J. (2021). *Cybersecurity Risks, Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks* [Chapter]. Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention; IGI Global. https://doi.org/10.4018/978-1-7998-6504-9.ch002

Copeland, M., Soh, J., Puca, A., Manning, M., & Gollob, D. (2015). Microsoft Azure and Cloud Computing. En M. Copeland, J. Soh, A. Puca, M. Manning, & D. Gollob (Eds.), *Microsoft Azure: Planning, Deploying, and Managing Your Data center in the Cloud* (pp. 3-26). Apress. https://doi.org/10.1007/978-1-4842-1043-7_1

Cui, Q., Jourdan, G.-V., Bochmann, G. V., Couturier, R., & Onut, I.-V. (2017). Tracking Phishing Attacks Over Time. *Proceedings of the 26th International Conference on World Wide Web*, 667-676. https://doi.org/10.1145/3038912.3052654

Dixon, M., Gamagedara Arachchilage, N. A., & Nicholson, J. (2019). Engaging Users with Educational Games: The Case of Phishing. *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1-6. https://doi.org/10.1145/3290607.3313026

Ellis, D. (2020). *7 Ways to Recognize a Phishing Email: Email Phishing Examples*. SecurityMetrics. https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

Eset_threat_report_t22021.pdf. (s. f.). Recuperado 23 de junio de 2022, de https://www.welivesecurity.com/wp-content/uploads/2021/09/eset_threat_report_t22021.pdf

Faniran, V. T., Badru, A., & Ajayi, N. (2017). Adopting Scrum as an Agile approach in distributed software development: A review of literature. *2017 1st International Conference on Next Generation Computing Applications (NextComp)*, 36-40. https://doi.org/10.1109/NEXTCOMP.2017.8016173

Franco, E., Menéndez Domínguez, V., Bolaños, E., & Quintal, L. (2019). *Usabilidad de un simulador para la enseñanza de la Programación de Sistemas*. *26*, 56-72.

Fuertes, W., Arévalo, D., Castro, J. D., Ron, M., Estrada, C. A., Andrade, R., Peña, F. F., & Benavides, E. (2022). Impact of Social Engineering Attacks: A Literature Review. En Á. Rocha, C. H. Fajardo-Toro, & J. M. R. Rodríguez (Eds.), *Developments and Advances in Defense and Security* (pp. 25-35). Springer. https://doi.org/10.1007/978-981-16-4884-7_3

Gibson, K. (2003). Games Students Play: Incorporating the Prisoner's Dilemma in Teaching Business Ethics. *Journal of Business Ethics*, *48*(1), 53-64. https://doi.org/10.1023/B:BUSI.0000004367.60776.b3

Google Cloud. (s. f.). *Introducing a Google Cloud architecture diagramming tool | Google Cloud Blog*. Recuperado 4 de agosto de 2022, de https://cloud.google.com/blog/topics/developers-practitioners/introducing-google-cloud-architecture-diagramming-tool

Greitzer, F. L., Li, W., Laskey, K. B., Lee, J., & Purl, J. (2021). Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility. *ACM Transactions on Social Computing*, *4*(2), 8:1-8:48. https://doi.org/10.1145/3461672

Gupta, S., Kar, A. K., Baabdullah, A., & Al-Khowaiter, W. A. A. (2018). Big data with cognitive computing: A review for the future. *International Journal of Information Management*, *42*, 78-89. https://doi.org/10.1016/j.ijinfomgt.2018.06.005

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 537-540. https://doi.org/10.1109/CCAA.2016.7813778

Hakim, Z. M., Ebner, N. C., Oliveira, D., Getz, S. J., Levin, B., Lin, T., Lloyd, K., Lai, V. T., Grilli, M. D., & Wilson, R. (2019). *Evaluating the cognitive mechanisms of phishing detection with PEST, an ecologically valid lab-based measure of phishing susceptibility*. PsyArXiv. https://doi.org/10.31234/osf.io/7b5an

Hakim, Z. M., Ebner, N. C., Oliveira, D. S., Getz, S. J., Levin, B. E., Lin, T., Lloyd, K., Lai, V. T., Grilli, M. D., & Wilson, R. C. (2021). The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. *Behavior Research Methods*, *53*(3), 1342-1352. https://doi.org/10.3758/s13428-020-01495-0

Hossain, E., Babar, M. A., & Paik, H. (2009). Using Scrum in Global Software Development: A Systematic Literature Review. *2009 Fourth IEEE International Conference on Global Software Engineering*, 175-184. https://doi.org/10.1109/ICGSE.2009.25

Huang, C., Cahill, M., Fekete, A., & Röhm, U. (2019). Data Consistency Properties of Document Store as a Service (DSaaS): Using MongoDB Atlas as an Example. En R. Nambiar & M. Poess (Eds.), *Performance Evaluation and Benchmarking for the Era of Artificial Intelligence* (pp. 126-139). Springer International Publishing. https://doi.org/10.1007/978-3-030-11404-6_10

IBM. (2022, junio 20). *IBM Security X-Force Threat Intelligence Index*. https://www.ibm.com/security/data-breach/threat-intelligence/www.ibm.com/security/data-breach/threat-intelligence

IBM Docs. (2021, marzo 2). *IBM Docs*. https://prod.ibmdocs-production-dal-6099123ce774e592a519d7c33db8265e-0000.us-south.containers.appdomain.cloud/docs/en/rational-soft-arch/9.7.0?topic=diagrams-use-case

ISO 25010. (s. f.). *ISO 25010*. Recuperado 5 de agosto de 2022, de https://iso25000.com/index.php/normas-iso-25000/iso-25010?start=3

Jones, C. (2021, mayo 21). Phishing Stats You Should Know In 2022. *Expert Insights*. https://expertinsights.com/insights/50-phishing-stats-you-should-know/

Kemp, S. (2022, enero 26). *Digital 2022: Global Overview Report*. DataReportal – Global Digital Insights. https://datareportal.com/reports/digital-2022-global-overview-report

Kießling, S., Hanka, T., & Merli, D. (2021). Salt&Pepper: Spice up Security Behavior with Cognitive Triggers. En *European Interdisciplinary Cybersecurity Conference* (pp. 26-31). Association for Computing Machinery. https://doi.org/10.1145/3487405.3487656

Kinateder, M. T., Kuligowski, E. D., Reneke, P. A., & Peacock, R. D. (2015). Risk perception in fire evacuation behavior revisited: Definitions, related concepts, and empirical evidence. *Fire Science Reviews*, *4*(1), 1. https://doi.org/10.1186/s40038-014-0005-z

Kitchenham, B., & Brereton, P. (2013). A systematic review of systematic review process research in software engineering. *Information and Software Technology*, *55*(12), 2049-2075. https://doi.org/10.1016/j.infsof.2013.07.010

Klug, B. (2017). An Overview of the System Usability Scale in Library Website and System Usability Testing. *Weave: Journal of Library User Experience*, *1*(6). https://doi.org/10.3998/weave.12535642.0001.602

Lewis, J., & Fowler, M. (2014, marzo 25). *Microservices*. martinfowler.com. https://martinfowler.com/articles/microservices.html

Martínez, L. R., Benitez, L. I. C., Camacho, G. F., Nativitas, K. G. G., & Caballero-Morales, S.-O. (2022). Improvement of competitiveness through the application of analytic hierarchy process, game theory, decision trees and design of experiments tools. *DYNA*, *89*(220), 187-194. https://doi.org/10.15446/dyna.v89n220.92289

McAfee. (2021, marzo 15). Phishing Email Examples: How to Recognize a Phishing Email. *McAfee Blog*. https://www.mcafee.com/blogs/internet-security/phishing-email-examples-how-to-recognize-a-phishing-email/

McLeod, S. (2020). *Cognitive Approach | Simply Psychology*. https://www.simplypsychology.org/cognitive.html

Merriam-Webster. (s. f.). *Medical Definition of Cognitive Psychology*. Merriam-Webster.com. Recuperado 25 de julio de 2022, de https://www.merriam-webster.com/medical/cognitive+psychology

Miao, K., Li, J., Hong, W., & Chen, M. (2020). A Microservice-Based Big Data Analysis Platform for Online Educational Applications. *Scientific Programming*, *2020*, e6929750. https://doi.org/10.1155/2020/6929750

Microsoft Azure. (s. f.). *App Service—Build & Host Web Apps | Microsoft Azure*. Recuperado 5 de agosto de 2022, de https://azure.microsoft.com/en-us/services/app-service/

Montañez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*, *11*. https://www.frontiersin.org/articles/10.3389/fpsyg.2020.01755

Musuva, P. M. W., Getao, K. W., & Chepken, C. K. (2019a). A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. *Computers in Human Behavior*, *94*, 154-175. https://doi.org/10.1016/j.chb.2018.12.036

Musuva, P. M. W., Getao, K. W., & Chepken, C. K. (2019b). A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. *Computers in Human Behavior*, *94*, 154-175. https://doi.org/10.1016/j.chb.2018.12.036

Nasser, G., Morrison, B. W., Bayl-Smith, P., Taib, R., Gayed, M., & Wiggins, M. W. (2020). The Effects of Cue Utilization and Cognitive Load in the Detection of Phishing Emails. En M. Bernhard, A.

Bracciali, L. J. Camp, S. Matsuo, A. Maurushat, P. B. Rønne, & M. Sala (Eds.), *Financial Cryptography and Data Security* (pp. 47-55). Springer International Publishing. https://doi.org/10.1007/978-3-030-54455-3_4

Nicholson, J., Coventry, L., & Briggs, P. (2017). *Can We Fight Social Engineering Attacks By Social Means? Assessing Social Salience as a Means to Improve Phish Detection*. 15.

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71-88. https://doi.org/10.2478/hjbpa-2018-0024

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T., & Ebner, N. (2017). Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 6412-6424. https://doi.org/10.1145/3025453.3025831

Ortiz Garcés, I., Cazares, M. F., & Andrade, R. O. (2019). Detection of Phishing Attacks with Machine Learning Techniques in Cognitive Security Architecture. *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, 366-370. https://doi.org/10.1109/CSCI49370.2019.00071

PageSpeed. (s. f.). *About PageSpeed Insights*. Google Developers. Recuperado 5 de agosto de 2022, de https://developers.google.com/speed/docs/insights/v5/about

Pearson, E., Bethel, C. L., Jarosz, A. F., & Berman, M. E. (2017). «To click or not to click is the question»: Fraudulent URL identification accuracy in a community sample. *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 659-664. https://doi.org/10.1109/SMC.2017.8122682

Pingdom. (s. f.). *WebsitePerformance and Availability Monitoring | Pingdom—Pingdom*. Pingdom.Com. Recuperado 5 de agosto de 2022, de https://www.pingdom.com/

Policonomics. (2017). *Game theory I: Extensive form | Policonomics*. https://policonomics.com/lp-game-theory1-extensive-form/

QuestionPro. (2016, agosto 31). Escala de Likert: Qué es y cómo utilizarla en tus encuestas. *QuestionPro*. https://www.questionpro.com/blog/es/que-es-la-escala-de-likert-y-como-utilizarla/

Rayyan. (s. f.). Recuperado 29 de junio de 2022, de https://rayyan.ai/reviews/455450

Rosenthal, M. (2022, enero 12). Phishing Statistics (Updated 2022)—50+ Important Phishing Stats. *Tessian*. https://www.tessian.com/blog/phishing-statistics-2020/

Sachdeva, S. (2016). Scrum Methodology. *International Journal Of Engineering And Computer Science*. https://doi.org/10.18535/ijecs/v5i6.11

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Samanta, A. K., & Chaki, N. (2021). Performance Monitoring of MongoDB on Varied Cluster Configuration: An Experimental Approach. *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 525-530. https://doi.org/10.1109/3ICT53449.2021.9581673

Sharfina, Z., & Santoso, H. B. (2016). An Indonesian adaptation of the System Usability Scale (SUS). *2016 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, 145-148. https://doi.org/10.1109/ICACSIS.2016.7872776

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, *58*, 216-229. https://doi.org/10.1016/j.cose.2015.12.006

Spring. (2020). *Spring Boot*. https://spring.io/projects/spring-boot#overview

Srinivasa Rao, R., & Pais, A. R. (2017). Detecting Phishing Websites using Automation of Human Behavior. *Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security*, 33-42. https://doi.org/10.1145/3055186.3055188

Sterling, A. (2019). NodeJS and Angular Tools for JSON-LD. *2019 IEEE 13th International Conference on Semantic Computing (ICSC)*, 392-395. https://doi.org/10.1109/ICOSC.2019.8665625

Sumner, A., & Yuan, X. (2019). Mitigating Phishing Attacks: An Overview. *Proceedings of the 2019 ACM Southeast Conference*, 72-77. https://doi.org/10.1145/3299815.3314437

Sutherland, J., Viktorov, A., Blount, J., & Puntikov, N. (2007). Distributed Scrum: Agile Project Management with Outsourced Development Teams. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 274a-274a. https://doi.org/10.1109/HICSS.2007.180

Tchakounte, F., Nyassi, V., Danga, D., Udagepola, K., & Atemkeng, M. (2020). A Game Theoretical Model for Anticipating Email Spear-Phishing Strategies. *EAI Endorsed Transactions on Scalable Information Systems*, *8*(30). https://eudl.eu/doi/10.4108/eai.26-5-2020.166354

Tian, C. A., & Jensen, M. L. (2019). *Effects of emotional appeals on phishing susceptibility*. 16.

Veksler, V. D., Buchler, N., LaFleur, C. G., Yu, M. S., Lebiere, C., & Gonzalez, C. (2020). Cognitive Models in Cybersecurity: Learning From Expert Analysts and Predicting Attacker Behavior. *Frontiers in Psychology*, *11*. https://www.frontiersin.org/articles/10.3389/fpsyg.2020.01049

Visual Studio Code. (2022). *Code Navigation in Visual Studio Code*. https://code.visualstudio.com/docs/editor/editingevolved

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Wash, R., & Cooper, M. M. (2018). Who Provides Phishing Training? Facts, Stories, and People Like Me. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1-12. https://doi.org/10.1145/3173574.3174066

Wen, Z. A., Lin, Z., Chen, R., & Andersen, E. (2019). What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1-12. https://doi.org/10.1145/3290605.3300338

Williams, N., & Li, S. (2017). Simulating Human Detection of Phishing Websites: An Investigation into the Applicability of the ACT-R Cognitive Behaviour Architecture Model. *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*, 1-8. https://doi.org/10.1109/CYBConf.2017.7985810

Word Art. (s. f.). *Word Art—Edit—WordArt.com*. Recuperado 11 de agosto de 2022, de https://wordart.com/create

Younis, Y. A., & Musbah, M. (2020). A Framework to Protect Against Phishing Attacks. *Proceedings of the 6th International Conference on Engineering & MIS 2020*, 1-6. https://doi.org/10.1145/3410352.3410825

Zheng, Y., Moini, A., Lou, W., Hou, Y. T., & Kawamoto, Y. (2016). Cognitive security: Securing the burgeoning landscape of mobile networks. *IEEE Network*, *30*(4), 66-71. https://doi.org/10.1109/MNET.2016.7513866

Zimmermann, O. (2017). Microservices tenets. *Computer Science - Research and Development*, *32*(3), 301-310. https://doi.org/10.1007/s00450-016-0337-0

Zohair, A. (s. f.). *What is Visual Studio Code?* Educative: Interactive Courses for Software Developers. Recuperado 29 de julio de 2022, de https://www.educative.io/answers/what-is-visual-studio-code