Análisis cognitivo de la respuesta de estudiantes de la Universidad del Valle de Guatemala frente a ataques informáticos y sus respectivas medidas de protección para fortalecer la educación en seguridad informática

Walter Danilo Saldaña Salguero, Juan Manuel Marroquin Alfaro, Jose Abraham Gutierrez Corado, Carlos Alberto Ráxtum Ramos y Javier Alejandro Cotto Argueta

UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

UNIVERSIDAD DEL VALLE DE GUATEMALA
Facultad de Ingeniería

Análisis cognitivo de la respuesta de estudiantes de la Universidad del Valle de Guatemala frente a ataques informáticos y sus respectivas medidas de protección para fortalecer la educación en seguridad informática

Trabajo de graduación en modalidad de Megaproyecto de Tecnología
presentado por
Walter Danilo Saldaña Salguero, Juan Manuel Marroquin Alfaro, Jose Abraham Gutierrez Corado, Carlos Alberto Ráxtum Ramos y Javier Alejandro Cotto Argueta
para optar al título universitario Licenciados en Ingeniería en Ciencias de la Computación y Tecnologías de la Información

Guatemala,

2024

UNIVERSIDAD DEL VALLE DE GUATEMALA
Facultad de Ingeniería

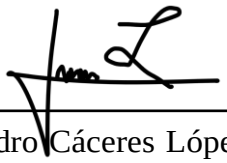
Análisis cognitivo de la respuesta de estudiantes de la Universidad del Valle de Guatemala frente a ataques informáticos y sus respectivas medidas de protección para fortalecer la educación en seguridad informática

Trabajo de graduación en modalidad de Megaproyecto de Tecnología
presentado por
Walter Danilo Saldaña Salguero, Juan Manuel Marroquin Alfaro, Jose Abraham Gutierrez Corado, Carlos Alberto Ráxtum Ramos y Javier Alejandro Cotto Argueta
para optar al título universitario Licenciados en Ingeniería en Ciencias de la Computación y Tecnologías de la Información

Guatemala,

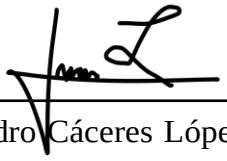
2024

Vo.Bo.:

(f) 

Ing. Juan Pedro Cáceres López

Tribunal Examinador:

(f) 

Ing. Juan Pedro Cáceres López

(f) 

Ing. Eddy Omar Castro Jauregui

(f) 

Ing. Douglas Leonel Barrios Gonzáles

Fecha de aprobación: Guatemala, 5 de febrero de 2024.

Prefacio

La presente investigación consta de dos fases principalmente, donde cada una tiene un enfoque distinto que permite segmentar diferentes puntos de análisis que terminan por correlacionarse a la hora de discutir resultados. El primero de dichas fases es el análisis de sesgos, y el segundo es el análisis de ataques.

La primera fase ofrece una perspectiva más panorámica de los incentivos y sesgos que conducen a los estudiantes a tomar decisiones en situaciones diarias. La segunda fase proporciona una visión más focalizada en las decisiones que toman los estudiantes ante uno o varios estímulos de interés.

De esta forma, se logra crear una implementación del método ACT para descomponer en componentes eventos, con el fin de entender de forma más completa los procesos cognitivos que realiza un individuo para tomar una decisión, enfocado en ambientes de ciberseguridad.

Se lo dedicamos a Dios, por bendecirnos con amigos, familia, hogar y una casa de estudios que nos apoyó en todo momento. La elaboración de este proyecto ha sido un arduo esfuerzo que fue posible gracias al apoyo de personas a quienes les dedicamos este logro y a quienes apreciamos incondicionalmente.

Cada aporte ha sido de suma importancia para sacar adelante el proyecto, y hemos demostrado nuestra capacidad para afrontar desafíos de forma eficaz y con un profesionalismo inigualable. Les debemos mucho a nuestros asesores por su acompañamiento durante este largo proceso; sus consejos han sido invaluables y su experiencia ha sido clave para cumplir los objetivos establecidos.

Siempre agradecemos a la comunidad "delvalleriana", que nos ha dado la oportunidad de ejecutar este proyecto, y a los estudiantes por su participación, que hizo posible todo esto. A Douglas Barrios, director del departamento de computación, y Heidy Ortega, secretaria del departamento, muchas gracias por siempre estar presentes en todo el trayecto.

Y, por último, a nuestras familias por su apoyo y comprensión en los momentos más difíciles y los más alegres; apreciamos mucho su soporte para seguir adelante.

Índice

Lista de figuras

Lista de cuadros

Resumen

Debido a que los estudiantes universitarios se encuentran en alto riesgo de ser expuestos a los riesgos del internet, se plantea un marco de análisis derivado del método ACT para comprender desde el punto de vista cognitivo la razón por la que los estudiantes son susceptibles a ataques informáticos para contribuir a una mayor conciencia de la seguridad informática entre los jóvenes y proporcionar recomendaciones para protegerse de las amenazas cibernéticas.

Se eligieron cinco sesgos (confirmación, optimismo, anclaje, Dunning-Kruger, y autoridad) además de cuatro ataques (open Wi-Fi, password leak, phishing y bait) para enfocar esta investigación, fundamentado en los sesgos y ataques más comunes en la actualidad.

Dentro de la investigación se demuestra que los estudiantes son principalmente susceptibles a los sesgos de confirmación (el 83.8%), anclaje (91.9%) y Dunning-Kruger (86.9%). En cuanto al sesgo de autoridad, está relativamente balanceado, con un 58.1% de estudiantes susceptibles. Y, por último, el sesgo al que menos fueron susceptibles fue al sesgo de optimismo donde con un 55% de estudiantes que no fueron sesgados.

Las conclusiones destacan la necesidad de concienciación y educación sobre amenazas cibernéticas y medidas de protección. Los estudiantes muestran sesgos cognitivos como el sesgo de novedad y optimismo en sus decisiones de seguridad. Además, los varios ataques realizados demostraron que en la materialidad de la población estudiada los sesgos son completamente dependientes del contexto en el que se ejecutan, más no de la persona, siendo cualquier individuo vulnerable bajo el contexto adecuado.

Abstract

Due to the fact that university students are at a high risk of being exposed to internet risks, a framework of analysis derived from the ACT method is proposed to comprehend, from a cognitive perspective, the reasons why students are susceptible to cyber-attacks. This aims to contribute to greater awareness of cybersecurity among young people and provide recommendations to protect themselves from cyber threats.

Five biases (confirmation, optimism, anchoring, Dunning-Kruger, and authority) and four attacks (open Wi-Fi, password leak, phishing, and bait) were chosen to focus this research, based on the most common biases and attacks today.

The research demonstrates that students are primarily susceptible to confirmation bias (83.8%), anchoring bias (91.9%), and Dunning-Kruger bias (86.9%). As for the authority bias, it is relatively balanced, with 58.1% of students being susceptible. Finally, the least susceptible bias was optimism, with only 55% of students not exhibiting this bias.

The conclusions highlight the need for awareness and education about cyber threats and protective measures. Students exhibit cognitive biases such as novelty bias and optimism in their security decisions. Furthermore, the various attacks conducted showed that in the studied population, biases are completely dependent on the context in which they are executed, rather than on the individual, making anyone vulnerable under the right circumstances.

CAPÍTULO 1

Introducción

La seguridad en la información conforme ha pasado los años se ha convertido en un tema bastante importante que procura la protección de todo recurso de información que una organización, persona o individuo tiene en sus manos a ataques cibernéticos. Ésta depende no sólo de los mecanismos de defensa que se han desarrollado, sino también del factor humano que juega un rol importante en todo este tema de la seguridad, debido a que son la primera línea de defensa con respecto a estos ataques y al mismo tiempo el eslabón más débil.

El humano es considerado el eslabón más débil debido a que contamos con sesgos cognitivos los cuales, si el atacante conoce a su perfección, puede adquirir lo que quiera de las personas, basándose en manipulaciones leves las cuales damos por alto por los mismos sesgos. La investigación relaciona la seguridad con la psicología, de esa forma brinda información bastante relevante para protegerse y autocapacitarse a lo que puede pasar antes, durante y después de un ataque informático en nuestro cerebro.

El objetivo principal de esta investigación es fomentar la educación en seguridad de sistemas de información en la población joven, los cuales son más propensos a recibir estos ataques. Esto se debe a que, están empezando a vivir por su cuenta, además de que son la mayor parte de la era digital, brindándoles una materialización de los ataques cibernéticos y sus respectivas propuestas de seguridad.

CAPÍTULO 2

Objetivos

2.1. Objetivo general del proyecto

- Identificar las soluciones de seguridad más adecuadas a las principales vulnerabilidades en los jóvenes acorde a la capacidad cognitiva de los mismos y presentarlas de forma comprensible para fomentar la educación para mitigar los casos de riesgo con respecto a recibir un ciberataque.

2.2. Objetivos generales

- Comprender la susceptibilidad de los estudiantes a ataques informáticos desde el punto de vista cognitivo.
- El propósito de este estudio es analizar las vulnerabilidades cognitivas que impactan a los jóvenes en su interacción con aplicaciones web. Se busca comprender cómo estas vulnerabilidades pueden ser explotadas en ataques informáticos, desarrollar soluciones de diseño de UI que minimicen los riesgos de seguridad. Además, se pretende identificar las vulnerabilidades que más afectan la capacidad cognitiva de los jóvenes y comprender cómo interactúan con las aplicaciones web durante un ataque, así como identificar los patrones de UI/UX utilizados por ciberdelincuentes en sus ataques.
- Evaluar posibles casos de conexión y uso de redes Wi-Fi potencialmente peligrosas, detectar comportamientos inseguros a la hora de navegar por internet, evaluar la efectividad de las medidas de protección existentes y estudiar la conciencia en seguridad informática de este grupo demográfico, para fortalecer la educación en seguridad informática y proponer recomendaciones de mejora en las medidas de protección en el ámbito de la ciberseguridad.
- Analizar los datos según las respuestas de los estudiantes de la Universidad del Valle de Guatemala frente a los ataques informáticos, con el objetivo de evaluar su nivel de conocimiento, conciencia y prácticas en seguridad informática.

2.3. Objetivos específicos

- Identificar los sesgos cognitivos a los que son más vulnerables los estudiantes.
- Correlacionar el uso de técnicas de manipulación cognitiva con el riesgo a ser víctima de un ataque informático.
- Explorar los ataques a los que los estudiantes son más susceptibles desde el punto de vista cognitivo.
- Implementar amenazas informáticas orientadas al ataque de sistemas de la información, controlados, en jóvenes para entender su respuesta cognitiva.
- Identificar cuáles serían los ataques más comunes a los sistemas de información y que tienen más frecuencia de que los estudiantes sean víctimas.
- Investigar las recomendaciones y estrategias que más funcionan para la mitigación de estos ataques cibernéticos.
- Implementar distintas amenazas informáticas controladas a un grupo de jóvenes para comprender sus respuestas cognitivas y cómo reaccionan ante estas.
- Examinar cómo los sesgos cognitivos influyen en las decisiones de los estudiantes al interactuar con elementos de interfaz de usuario (UI) y experiencia del usuario (UX), con el fin de identificar áreas de mejora y posibles vulnerabilidades susceptibles de explotación.
- Identificar mediante pruebas controladas a que elementos del UI los estudiantes le dedican más tiempo en promedio para la toma de decisiones.
- Identificar las debilidades más prevalentes en el entorno de la navegación por Internet, centrándose en diferentes temas como el análisis de redes públicas, descargas y la detección de ataques de phishing, y proporcionar posibles soluciones que los usuarios puedan aplicar para protegerse.
- Identificar los sesgos cognitivos de los usuarios frente a escenarios de múltiples decisiones, que los puedan convertir en usuarios vulnerables a un ataque cibernético.
- Conocer las diferentes herramientas de software que otros usuarios han implementado para reducir el porcentaje de ataques, pros y contras de cada una de estas. Analizar la frecuencia y gravedad de los ataques informáticos en los estudiantes de la Universidad del Valle de Guatemala, para entender mejor la magnitud del problema.
- Identificar posibles ataques informáticos a los que los estudiantes de la Universidad del Valle son más vulnerables, con el fin de fortalecer la seguridad de su información.
- Con base en la información recopilada durante las pruebas, en el análisis de datos verificar y cuantificar la percepción de los estudiantes sobre los riesgos asociados con posibles escenarios de ataques informáticos, medir la conciencia de los estos riesgos y la probabilidad de ser víctima de un ataque informático.
- Proponer estrategias educativas y de concienciación específicas, con el fin de fortalecer la educación en seguridad informática entre los estudiantes universitarios.

CAPÍTULO 3

Justificación

Los avances informáticos crecen exponencialmente en nuestra sociedad y cada día incorporamos más y más herramientas tecnológicas que nos facilitan las tareas cotidianas. Sin embargo, cada nueva tecnología, algoritmo o sistema informático desarrollado implica nuevas vulnerabilidades y *exploits* que aún no han salido a la luz, y los crackers lo saben, por lo que se dedican a encontrar estos fallos para aprovecharse de las personas. Incluso las tecnologías antecesoras que ya han sido probadas y testeadas tienen sus vulnerabilidades, ya sean nuevas por descubrir, u otras que ya son de conocimiento público, e independientemente de cuál sea la procedencia de la vulnerabilidad, un cracker siempre estará dispuesto a aprovecharla.

Dicho esto, hay que entender entonces, que hay un desfase entre el crecimiento de los sistemas de información y la seguridad de los mismos, de modo que esta última naturalmente tiende a quedarse por detrás. Por lo tanto, es indispensable buscar soluciones más eficaces y ágiles a los ataques informáticos. Para lograrlo, se debe de saber que el eslabón más débil de la seguridad informática es el factor humano, ya que nuestra naturaleza es propensa a cometer errores dados los sesgos cognitivos que muchas veces gobiernan nuestra vida inconscientemente. De hecho, un estudio realizado en 2017 por la empresa de seguridad Kaspersky, demostró que el 46% de las fallas de seguridad más relevantes en empresas a nivel mundial durante ese año fueron causadas por el poco o ningún conocimiento de ciberseguridad por parte de los empleados (Kapersky, 2017). Por lo que, la raíz de los principales problemas de seguridad informática nace desde el punto de vista cognitivo en los seres humanos.

Según lo anterior, es necesario brindar una solución justificada en los procesos cognitivos de los individuos para educar en ciberseguridad, y los estudiantes universitarios, se encuentran en la edad en la que son lo suficientemente jóvenes como para adquirir fácilmente nuevas destrezas cognitivas en el ámbito de la informática, y lo suficientemente maduros como para entender los riesgos del mundo digital, ya que esta es la edad en la que tienden a explorar más este mundo sin la supervisión de un adulto responsable, por lo que también son el grupo más vulnerable a ser víctimas de ataques informáticos.

Por lo tanto, este estudio busca ofrecer un marco de análisis destinado para elaborar soluciones justificadas en los procesos cognitivos de la población más vulnerable, los jóvenes que se exponen día a día a los riesgos de la informática, ante las principales vulnerabilidades de los mismos. Lo que puede impactar de manera positiva la cultura de ciberseguridad en Guatemala, ya que ellos serán los futuros profesionales de nuestro país y un conocimiento más profundo de los riesgos

informáticos puede evitar que sean víctimas de ataques que repercutan económica, reputacional, física o negativamente a las organizaciones de las que son parte, o bien que perjudiquen su propia integridad.

Consideramos que la UVG, al ser referente de tecnología e innovación en Guatemala, es el punto de partida perfecto para iniciar la presente investigación de forma que podamos generar un modelo de análisis que a futuro sea replicable en más sectores para expandir los alcances de la investigación.

CAPÍTULO 4

Marco teórico

4.1. Conceptos de ciberseguridad

La NICCS (National Initiative for Cybersecurity Careers and Studies) de los Estados Unidos define la siguiente manera los conceptos que a continuación se enlistan.

4.1.1. Sistema de información

Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización (INCIBE, 2020). Se debe de considerar que los recursos humanos, sean conocidos o colaboradores, también forman parte de los sistemas de información, al tener participación directa en el uso y compartimiento de la información.

4.1.2. Vulnerabilidad

Una característica o debilidad específica que hace que una organización o activo (como información o un sistema de información) esté abierto a la explotación por una amenaza determinada o susceptible a un peligro determinado (NICCS, 2023).

La parte más grande y vulnerable de cualquier sistema de tecnología de la información es el ser humano. Los seres humanos representan una de las mayores debilidades de la ciberseguridad de sus sistemas y resultan altamente vulnerables a la manipulación psicológica (ingeniería social) de maneras que permiten a un actor de ciber amenazas obtener fácilmente acceso a los sistemas seguros de los objetivos sin necesidad de la infiltración bruta. Si bien el malware potente y las habilidades avanzadas de piratería refuerzan significativamente las capacidades de cualquier actor cibernético, en última instancia son los humanos los que representan un exploit irreparable en ciberseguridad (Truitte, 2019).

4.1.3. Amenaza

Una circunstancia o evento que tiene o indica el potencial de explotar vulnerabilidades y de impactar negativamente (crear consecuencias adversas para) las operaciones organizacionales, los activos organizacionales (incluida la información y los sistemas de información), los individuos, otras organizaciones o la sociedad. Incluye un individuo o grupo de individuos, entidad como una organización o una nación), acción o suceso (NICCS, 2023).

4.1.4. Riesgo

La posibilidad de que se produzca un resultado adverso o no deseado como resultado de un incidente, evento o suceso, según lo determinado por la probabilidad de que una amenaza particular aproveche una vulnerabilidad particular, con las consecuencias asociadas (NICCS, 2023).

4.1.5. Exposición

La condición de estar desprotegido, permitiendo así el acceso a información o acceso a capacidades que un atacante puede utilizar para ingresar a un sistema o red (NICCS, 2023).

4.1.6. Cracker

Ciberdelincuente que se caracteriza por acceder de forma no autorizada a sistemas informáticos con la finalidad de menoscabar la integridad, la disponibilidad y el acceso a la información disponible en un sitio web o en un dispositivo electrónico (INCIBE, 2020).

4.1.7. Ciberataque

Un ciberataque es un acto malintencionado realizado por actores de amenazas también llamados cibercriminales, con el fin de alterar, robar o destruir información, o bien tomar el control de cuentas de bancos, correos electrónicos o dispositivos informáticos por medio del acceso a una red de forma no autorizada.

Los atacantes con motivaciones delictivas buscan obtener ganancias financieras mediante el robo de dinero, el robo de datos o la interrupción del negocio. Los ciberdelincuentes pueden piratear una cuenta bancaria para robar dinero directamente o utilizar estafas de ingeniería social para engañar a las personas para que les envíen dinero. Los piratas informáticos pueden robar datos y utilizarlos para cometer robos de identidad o venderlos en la Dark Web o guardarlos para un rescate. (IBM, 2023)

Los atacantes con motivaciones delictivas buscan obtener ganancias financieras mediante el robo de dinero, el robo de datos o la interrupción del negocio. Los ciberdelincuentes pueden piratear una cuenta bancaria para robar dinero directamente o utilizar estafas de ingeniería social para engañar a las personas para que les envíen dinero. Los piratas informáticos pueden robar datos y utilizarlos para cometer robos de identidad o venderlos en la Dark Web o guardarlos para un rescate. (IBM, 2023)

4.1.8. Ingeniería social

Según la IEEE en su artículo "Defining Social Engineering in Cybersecurity", la ingeniería social es un tipo de ataque en el que el atacante explota vulnerabilidades humanas a través de interacciones sociales para abrir brechas en el ciberespacio. Este ataque se realiza influenciando el comportamiento social de la víctima a través de técnicas sociales, las cuales incluyen, pero no se limitan a manipulación, sesgos cognitivos, persuasión, inducción, entre otros (Wang, Sun, y Zhu, 2020).

Cuando se habla de vulnerabilidades humanas, se hace referencia a los factores humanos que pueden ser aprovechados por un atacante para lograr sus cometidos.

Como se explica en el artículo "*Social Engineering Attacks: A Survey*" por Salahdine, el proceso de ingeniería social generalmente se realiza por fases, las cuales son las siguientes:

1. Investigación de la víctima
2. Desarrollo de la relación con la víctima
3. Ejecución del ataque
4. Salida

En la primera fase, el atacante se dedica a investigar a fondo el comportamiento de su víctima, esto para garantizar que el ataque sea efectivo y poder aprovechar al máximo los sesgos particulares de la víctima que mejor se puedan aprovechar para lograr el cometido.

La segunda fase busca una conexión con la víctima, es buscar una entrada a su "vida social" para poder llegar a la siguiente fase.

La tercera fase consiste en realizar el ataque planeado, más adelante se profundizará en el tipo de ataque que este puede ser. La efectividad de esta fase depende meramente de la calidad de las fases anteriores.

La cuarta y última fase consiste en la salida del atacante de la vida de la víctima. Una vez realizado el ataque, el atacante busca desaparecer para no hacerse responsable de los perjuicios ocasionados en el mismo (Salahdine y Kaabouch, 2019).

Vulnerabilidades más frecuentes de ingeniería social

Existen varias vulnerabilidades que pueden ser explotadas por técnicas de ingeniería social, sin embargo, según la investigación de 2019 titulada *Social Engineering Attacks: A Survey*, en la que se realizó una encuesta sobre los ataques más relevantes se concluyó que los siguientes son los ataques que más afectan a las personas a nivel mundial:

- Phishing
- Baiting
- Ransomware

4.1.9. Otros ataques y vulnerabilidades relevantes

- Data breach: El movimiento no autorizado o la divulgación de información confidencial a una parte, generalmente fuera de la organización, que no está autorizada a tener o ver la información (NICCS, 2023).
- Password leak: Data breach en el cual la información exfiltrada son las credenciales o contraseñas de la víctima.
- Open Wi-Fi: La mayor amenaza para la seguridad del Wi-Fi gratuito open Wi-Fi es la capacidad del hacker de posicionarse entre usted y el punto de conexión. Entonces, en lugar de hablar directamente con el punto de acceso, estás enviando tu información al hacker, quien luego la transmite (*Public WiFi Risks and what you can do about it*, 2023).

4.2. Conceptos cognitivos

4.2.1. Psicología cognitiva

La Psicología Cognitiva es la rama que estudia los procesos mentales que intervienen en nuestra capacidad para razonar y pensar, asimilar nuevos conocimientos y resolver problemas. La Psicología Cognitiva investiga los mecanismos subyacentes al comportamiento humano y las variables externas que lo determinan, es decir qué procesos y estructuras internas desencadenan la respuesta humana ante un estímulo.

4.2.2. Estimulo respuesta

La teoría del estímulo-respuesta es una teoría conductual que explica cómo se produce el aprendizaje a través de la interacción de estímulos y respuestas. Fue propuesto por primera vez por Edward Thorndike a principios del siglo XX. La teoría sugiere que una respuesta a un estímulo se vuelve más frecuente o predecible en un entorno determinado como resultado del refuerzo. La teoría del estímulo-respuesta forma la base del condicionamiento clásico, que es un tipo de aprendizaje en el que un organismo aprende a asociar un estímulo neutral con un estímulo significativo (Thorndike, 1932).

Estimulo respuesta en ciberseguridad

Como indica el artículo *Distinguishing response from stimulus driven history biases*, la percepción está determinada por la experiencia pasada, tanto acumulativa como contextual, y la dependencia en serie refleja un atractivo sesgo contextual para percibir o informar que el mundo es más estable de lo que realmente es. En el contexto de la ciberseguridad, esto implica que los individuos tienden a verse sesgados por eventos aprendidos de experiencias pasadas.

4.2.3. Procesos cognitivos

Es una rama de la psicología que se enfoca y centra en el estudio de los procesos mentales que hemos ido adquiriendo, almacenando, manipulando y para qué ha sido utilizada la información que hemos aprendido, se centra en la idea que la mente humana es un sistema complejo que procesa

activamente la información. La premisa fundamental es que todo lo cognitivo, es decir lo que pensamos, es de gran importancia e influencia en nuestro funcionamiento dentro de la sociedad, esto quiere decir que, dada una situación específica, todas nuestras experiencias pasadas, nuestros pensamientos y nuestros sesgos afectan cómo reaccionemos u actuemos ante esta situación.

La psicología cognitiva tiene un papel importantísimo tanto al momento de desarrollar una aplicación como al interactuar con ella. Ya que, por el lado de los desarrolladores, tendrán que tomar en cuenta todos los factores cognitivos que pueden llevar a un usuario a realizar una acción. Así como los usuarios interactúan con nuestra aplicación. La Psicología Cognitiva es una rama compleja de la psicología llena de grandes procesos complejos, por lo que sólo nos enfocaremos en los sesgos.

4.2.4. Procesos cognitivos básicos

Los procesos cognitivos básicos son la base para el procesamiento y la manipulación de la información que permitan obtener un producto mental. Estos procesos nos permiten capturar y retener información en nuestro sistema para poder utilizarla. Los más importantes son:

- Sensopercepción: Es la facultad para captar las sensaciones a través de los diferentes receptores.
- Memoria: Permite mantener en el sistema la información captada por los receptores para poder ser trabajada.
- Atención: Permite seleccionar, focalizar y mantener los recursos mentales en un estímulo en particular.
- Procesamiento de la información: permite que la información captada sea procesada y pueda llegar a ser elaborada.

4.2.5. Procesos cognitivos superiores

Son los que requieren mayor integración en la información para poder generar una respuesta. Algunos procesos cognitivos superiores son:

- Lenguaje
- Pensamiento
- Aprendizaje
- Creatividad

4.2.6. Análisis cognitivo de tareas

El análisis de tareas cognitivas (ACT) es un tipo de análisis de tareas que tiene como objetivo comprender tareas que requieren mucha actividad cognitiva por parte del usuario, como la toma de decisiones, la resolución de problemas, la memoria, la atención y el juicio. ACT amplía el análisis de tareas tradicional para aprovechar los procesos mentales que subyacen al comportamiento observable y revelar las habilidades y estrategias cognitivas necesarias para abordar eficazmente

situaciones desafiantes (Vicente y Rasmussen, 1992).

Para realizar un análisis de tareas cognitivas, es necesario identificar los objetivos de la observación, dividir la tarea en subtareas que sean observables y mensurables, decidir un tipo de análisis cognitivo como pensar en voz alta, entrevista u observación que pueda capturar los procesos mentales y las estrategias de los artistas, realizar el análisis recopilando y registrando datos de los artistas utilizando el método y las herramientas elegidos, preparar los resultados organizando, codificando e interpretando los datos e identificar los conocimientos, habilidades y errores involucrados. en la tarea (Vicente y Rasmussen, 1992).

4.3. Importancia de la Psicología Cognitiva en la ciberseguridad

La relevancia de la Psicología Cognitiva en la ciberseguridad radica en la facultad de poder comprender las motivaciones y estrategias de un cracker, así como las pautas de comportamiento de las víctimas de los ataques que las hacen vulnerables.

4.3.1. Sesgos cognitivos

Los sesgos cognitivos son atajos mentales que nuestro cerebro toma para dar respuesta a un estímulo de forma que pueda ahorrar tiempo y energía. Si bien pueden ser útiles, en ocasiones la falta de racionalidad, de información u objetividad nos pueden llevar a cometer errores. Estos errores sistemáticos en los procesos cognitivos nos producen una desviación, o sesgo, en el procesamiento mental, nos pueden alejar de la racionalidad o nublar nuestro juicio y hacernos víctimas de ataques.

Steve Durbin, CEO de la Information Security Forum (ISF), indica que los sesgos cognitivos más relevantes en ciberseguridad son:

- Heurística de afecto: La heurística de afecto es un atajo mental que está fuertemente influenciado por el estado emocional actual.
- Anclaje: El anclaje es un sesgo generalizado en el que los seres humanos aceptan la primera información como la verdad absoluta al tomar una decisión.
- Heurística de disponibilidad: Cuantas más veces uno se encuentre con un tipo de situación, más accesible estará en su memoria, y, por lo tanto, tendrá prioridad en la toma de decisiones.
- Racionalidad limitada: Se refiere a la tendencia humana a tomar decisiones basadas en la satisfacción de criterios aceptables o suficientes en lugar de buscar la opción óptima.
- Sobrecarga de opciones: También conocido como parálisis por análisis, se refiere a la tendencia humana a tener dificultades para tomar decisiones cuando se enfrentan a una amplia variedad de opciones.
- Fatiga de decisiones: Tomar decisiones repetitivas agota los recursos mentales y puede llevar a la fatiga de decisiones.
- Comportamiento de manada: Los seres humanos imitan inconscientemente las acciones de un grupo más amplio, incluyendo las malas prácticas de seguridad.

- Efecto de licencia: Es la tendencia humana a permitirse comportamientos negativos o arriesgados después de haber realizado previamente acciones positivas o moralmente aceptables.
- Fatiga de voluntad: Es experimentar una disminución de la autodisciplina y la fuerza de voluntad después de haber realizado tareas que requieren esfuerzo mental o autocontrol de manera repetitiva o prolongada.
- Efecto Dunning-Kruger: Las personas con conocimientos o competencias limitadas en un determinado dominio intelectual o social sobreestiman en gran medida su propio conocimiento o competencia en ese dominio en relación con criterios objetivos o con el desempeño de sus pares o de la gente en general.
- Confirmación: Un sesgo en donde las personas buscan que los conocimientos nuevos adquiridos mediante interpretar y recordar información de una manera selectiva las cuales confirmen sus experiencias y conocimientos previos (Eldridge, 2016).
- Optimismo: Este sesgo explica detalladamente que "las personas piensan que son menos propensas a recibir un ataque debido a que existen otras entidades las cuales son más importantes" para los atacantes, por lo tanto, no toman medidas de protección, recomendaciones o se informan acerca de seguridad (Nikolopoulou, 2023).
- Disponibilidad: El sesgo donde las personas dan mayor valor a los conocimientos que tienen actualmente que los nuevos, por lo que pueden tender a sólo quedarse con la información de los ataques con una antigüedad mayor, dando oportunidad a que caigan en ataques nuevos o amenazas mayores a las que conocen (Li, 2022).
- Anclaje: Un sesgo importante para la toma de decisiones, debido a que estas se ven influenciadas por la primera información proveída (Nikolopoulou, 2022).
- Ilusión de la seguridad: Las personas suelen sentirse seguras con el sistema actual de seguridad, lo que ocasiona que varios de estos no implementen otras medidas y prácticas para mejorar en este ámbito. El estar en un lugar que parece seguro no significa que pueda recibir ataques de mayor fuerza o influencia y que ocasiona estragos, riesgos y prejuicios negativos de mayor nivel (Kim, 2016).
- Norma social: Es un fenómeno en el que las personas siguen y copian las acciones de otros para mostrar un comportamiento aceptado o correcto, basado en la idea de influencia social normativa. Sin embargo, las personas miran a los demás cuando no están seguras de cuál es la forma correcta de comportarse. Por lo tanto, este sesgo psicológico se “activará” si un individuo se siente indeciso, inseguro (Mullin, 2015).
- Sobre confianza: Este sesgo ocasiona que las personas generen mayor confianza por lo que saben o se creen mejores en ciertas actividades, áreas y situaciones de lo que en realidad son (Hayes, 2023).
- Automatización: Este sesgo ocasiona que las personas tengan confianza o una sobre confianza respecto a las actividades y tareas que realiza un computadora o aplicación. Se debe a que por la normativa que se automatiza un proceso, hacemos caso omiso a los fallos que se puedan presentar o tener en algún punto. Este sesgo puede resultar en beneficios o prejuicios (Adcock Solutions, 2022).
- Novedad: Este sesgo se refiere a la tendencia de las personas a dar preferencia a cosas nuevas o innovadoras sobre las existentes, a menudo sin una evaluación crítica adecuada. En seguridad informática, este sesgo podría llevar a la adopción de nuevas tecnologías o

soluciones de seguridad sin una evaluación adecuada de sus méritos y posibles riesgos (Nikolopoulou, 2023).

- Confirmación social: El sesgo de confirmación social se manifiesta cuando las personas tienden a adoptar una acción o creencia porque otros en su entorno lo hacen. En seguridad informática, esto puede llevar a la adopción de prácticas o tecnologías de seguridad simplemente porque son populares o respaldadas por otros, sin considerar su idoneidad para las necesidades específicas (Nikolopoulou, 2023).
- Autoridad: Este sesgo se produce cuando las personas tienden a confiar en la autoridad o en fuentes de confianza, como expertos, instituciones o figuras de autoridad, sin cuestionar críticamente su validez (Morgan, 2021).
- Necesidad o urgencia: El sesgo de necesidad se refiere a la tendencia de las personas a tomar decisiones apresuradas basadas en la percepción de que tienen una necesidad urgente de algo (Zhu et al., 2018).
- Complacencia: El sesgo ocurre cuando las personas subestiman los riesgos potenciales o sobreestiman su nivel de seguridad debido a una sensación de comodidad (Furst, 2022).
- Ilusión de control: Consiste en sobreestimar la influencia que nuestra conducta ejerce sobre resultados incontrolables. La evidencia disponible sugiere que un factor importante en el desarrollo de esta ilusión es la participación personal de los participantes que intentan obtener el resultado. Esto puede ocurrir por motivaciones sociales y a la protección de la autoestima (Yarritu et al., 2014).
- Resultado (Outcome bias): A menudo se juzga una decisión pasada por su resultado sin considerar la calidad de la decisión en el momento en que se tomó, teniendo presente lo que se sabía en ese momento. Por lo que, outcome bias no implica el análisis de los factores que conducen a un evento previo y, en cambio, resta importancia a los eventos que preceden a los resultados y se da más énfasis al resultado (Baron, Hershey, 1988).
- Status quo: La gente tiende a preferir que los estados del mundo se mantengan consistentes. Al tomar una decisión, las personas suelen optar por el curso de acción más fácil: no hacer nada o mantener el curso de acción actual. Describe nuestra preferencia irracional por una opción predeterminada simplemente porque preserva el estado actual de las cosas. Un gran ejemplo de este sesgo sería "¿Por qué arreglar algo que no se encuentra roto?" (Smiley, Fisher, 2022).

4.4. Los sesgos cognitivos y el peligro de ser víctima de un ataque cibernético

En el ámbito de la ciberseguridad para que un usuario pueda llegar a ser víctima de una de las formas de ataque cibernético tales como: DNS spoofing, Phishing, Malware, Rasonmware, Cryptojacking o cualquier otro intento de intrusión, existen varios factores que se deben tomar en cuenta y puedan ser la causa de hacer más vulnerable a uno u otro dispositivo. En un gran porcentaje de los ataques exitosos el factor que ha sido determinante es el factor humano.

En el ámbito de la seguridad informática, existe un dicho popular que señala que "la principal amenaza se encuentra entre la silla y el teclado". Esta afirmación subraya la idea de que los usuarios representan uno de los mayores desafíos para la seguridad informática. Si bien esta afirmación no es completamente precisa, es indudable que en numerosas situaciones los usuarios contribuyen

significativamente a los problemas de ciberseguridad. Esto se debe a su falta de educación y conocimiento sobre las diversas formas de ataque cibernético, así como a su desconocimiento y desinterés en comprender los mecanismos y herramientas necesarios para protegerse frente a cualquier modalidad de ataque.

Por lo anterior, cuando las personas utilizan un dispositivo electrónico interconectado a una red local o a internet, y acceden a diversas aplicaciones y servicios, tienden inconscientemente a actuar guiados por sus sesgos cognitivos. Estos sesgos influyen en la toma de decisiones de todo ser humano. En la vida cotidiana, casi a diario, se deben tomar decisiones rápidas y, a menudo, bajo presión. Esta situación nos obliga a decidir sin tener toda la información oportuna para determinar si la decisión es correcta o no. Es en este contexto donde los distintos sesgos cognitivos entran en juego y afectan nuestras decisiones.

En un escenario en el que un estudiante se encuentra en la cafetería de la universidad y necesita de conexión a internet para realizar diversas tareas, al verificar las redes Wi-Fi disponibles, puede ver que se encentra la que ofrece la universidad y que además es una red Wi-Fi abierta y por el sesgo cognitivo de control y sobre confianza que le hace creer que el conectarse a esa red es algo seguro y que el estudiante tiene todo bajo control, y a su vez influenciado por el sesgo de norma social que le hace pensar que si todos los estudiantes se conectan a dicha red entonces también debe hacerlo sin ningún inconveniente. Sin embargo, el estudiante ignora las consecuencias reales de conectarse a esa red y que pudiera llevarlo ser víctima de un ataque de *Man-in-the-Middle* que permitirá que alguien estuviera en medio de esa red filtrando todo el tráfico que pasa por ella y adueñarse de cualquier información o credenciales a las cuales pudiera sacar provecho posteriormente.

En otro orden de eventos, en un escenario en el que un estudiante recibe un correo electrónico o un mensaje en su teléfono móvil en el cual se le presenta contenido que parece atractivo e interesante a él por medio de un enlace, y al desconocer los riegos y actuar basado en sus propias percepciones, puede verse influenciado por el sesgo cognitivo de optimismo y abrir el enlace pensando que este lo llevara a algo seguro y de su interés, pensando que nada malo puede pasar al abrir el enlace y que esto es algo que no presenta ningún peligro o riesgo de amenaza, y s actuar lo lleva a caer en un ataque de Phishing y posiblemente a un ataque de Web Spoofing, ya que dicho enlace puede llevarlo a un sitio web que aparentemente sea verídico, sin embargo, en realidad se trate de un sitio falso con la finalidad de robo de credenciales u otra información.

Uno de los comportamientos más comunes y que causan más amenaza a la hora de navegar por la red es realizar descargas de contenido de páginas de dudosa procedencia, o hacer uso constantemente de páginas web que ofrecen contenido audiovisual de paga de manera gratuita, y en este sentido el usuario obviando que nadie nos va a brindar un servicio de forma gratuita sin esperar obtener un beneficio, se ve influenciado por varios sesgos como son el sesgo de status quo, el sesgo de optimismo, el sesgo de sobre confianza y el sesgo de anclaje. Estos sesgos lo llevan a ignorar las amenazas ya que al realizar descargar o navegar por sitios de dudosa procedencia podría ser víctima de ataques de Cryptojacking, o de algún tipo de ataque de malware como Rasomware, Spyware u otro, que podría en riesgo el equipo que se esté utilizando y toda la información almacenada y procesada a través de él.

4.5. Conceptos UI/UX

4.5.1. Accesibilidad

Cómo define Rodríguez (2022), la accesibilidad son un conjunto de pautas, directrices o estándares que permiten que cualquier persona pueda acceder a una página web o aplicación, estas pautas, facilitan el acceso y la interacción con nuestra aplicación a los usuarios independientemente de los conocimientos, capacidades y características que estos posean. Actualmente no existe una definición formal sobre la accesibilidad, sin embargo, la organización W3C (World Wide Web) ha creado una iniciativa llamada WAI (Web Accessibility Initiative) que reúne los conceptos más relevantes para que una aplicación web logre ser accesible. Como consecuencia, los estándares promovidos por la WAI, nos permite definir los patrones que logran la accesibilidad para nuestra aplicación, los cuales son:

- Texto y contenido
- Colores
- Diseño y fluidez
- Elementos interactivos
- Animaciones
- Informar al Usuario

Así mismo, existen varios recursos que nos ayudan a evaluar la accesibilidad de nuestra aplicación web, la cual nos ayuda a obtener información valiosa a la hora de desarrollar estas aplicaciones de forma que esta retroalimentación nos ayude a hacer más accesible nuestra aplicación web. Entre esos recursos podemos encontrar los siguientes:

- *WAVE Web Accessibility Evaluation Tool*
- *HeadingsMap*
- *Cynthia Says*
- *LERA*

4.5.2. Usabilidad

La usabilidad se puede definir como la medida en que una aplicación o producto puede ser utilizado por usuarios específicos para lograr objetivos específicos con efectividad, eficiencia y satisfacción del contexto. (ISO 9241-11: Ergonomics of human-system interaction 2018). Todo con el objetivo de que el usuario logre completar tareas sin experimentar, dificultad o frustración, mientras el proceso de la tarea sea de manera fluida. Este es un factor importante para el diseño de experiencias de usuarios, ya que mientras más fácil sea nuestro producto de usar y que le sea útil al usuario, mejor experiencia tendrá. Existen varios principios básicos o reglas para desarrollar interfaces, sin embargo, nos enfocaremos en las 8 reglas de oro de Ben Shneiderman las cuales son (Shneiderman y cols., 2016):

- Esforzarse por la consistencia
- Buscar la usabilidad universal
- Ofrecer comentarios informativos
- Diseñar diálogos para producir un cierre

- Prevenir errores
- Permitir la reversión de acciones
- Mantener a los usuarios en control
- Reducir la carga de la memoria a corto plazo

Estas heurísticas nos permiten diseñar productos que sean usables de manera sencilla por parte de los usuarios.

4.5.3. Heurísticas

Una heurística, son reglas generales, en este caso enfocado al desarrollo de interfaces. Dentro del entorno del desarrollo interfaces y todo lo que rodea el UI/UX existen varias heurísticas que nos permiten evaluar elementos, sobre todo la usabilidad, de una aplicación, entre ellas una de las más famosas, las Heurísticas de Nielsen, que son 10 reglas que nos permiten encontrar una gran cantidad de errores de usabilidad sin la necesidad de probar nuestra aplicación con usuarios, de esta manera podemos obtener resultados de cómo funciona nuestro sistema sin tener que hacer pruebas con usuarios, todo esto con el objetivo de mejorar nuestro producto. Para el motivo de nuestro estudio, utilizaremos las heurísticas de Nielsen para poder hacer análisis sobre las aplicaciones de prueba que le pasaremos a los usuarios, tanto de la versión correcta, como de la versión maliciosa, la que intenta replicar el ataque, de forma en la que nosotros podamos tener una métrica sobre las pruebas que le pasaremos a los usuarios y ver si ellos son capaces de detectar si están en la versión maliciosa o no. Los 10 principios heurísticos de Nielsen son los siguientes:

- Visibilidad del estado del sistema
- Adecuación entre el sistema y el mundo real
- Libertad y control por parte del usuario
- Consistencia y estándares
- Prevención de errores
- Reconocimiento antes que recuerde
- Flexibilidad y eficiencia en el uso
- Diseño estético y minimalista
- Ayuda a los usuarios a reconocer, diagnosticar y recuperarse de los errores
- Ayuda y documentación

4.5.4. UI

El Diseño de Interfaz o User Interface (UI), se refiere a todo aquello con lo que los usuarios interactúan directamente (la capa externa de un producto o servicio digital). Es lo que ve y toca en una página web, una aplicación o un dispositivo cualquiera. Cabe destacar que, UI es la parte visible de la interfaz, mientras que UX es la parte oculta, conceptos que muchas veces prestan confusión. El diseño de interfaz se ocupa de los colores; las tipografías; los iconos; los formularios y botones; las animaciones y los sonidos de las notificaciones, por ejemplo, de las redes sociales. Un buen

diseño de interfaz debe ser funcional más allá de lo estético (De Gregorio, 2021a).

4.5.5. UX

La experiencia de usuario es la traducción de User eXperience (UX), y contempla todos los aspectos que participan en la interacción del usuario final con la empresa, sus servicios y productos. Tiene como objetivo principal satisfacer sus necesidades y deseos sin impedimentos ni frustraciones (De Gregorio, 2021b).

4.5.6. Frontend

El frontend es la parte del desarrollo web que se dedica a la parte frontal de un sitio web, en pocas palabras del diseño de un sitio web, desde la estructura del sitio hasta los estilos como colores, fondos, tamaños hasta llegar a las animaciones y efectos. Es esa parte de la página con la que interactúan los usuarios de la misma, es todo el código que se ejecuta en el navegador de un usuario, al que se le denomina una aplicación cliente, es decir, todo lo que el visitante ve y experimenta de forma directa (Bautista García, 2021).

4.6. Conceptos de ataques por medio de la navegación en la red

Con el alto número de personas conectadas a internet a través de un dispositivo inteligente y que crece cada día de forma exponencial, resulta atractivo y rentable para los ciber atacantes el crear nuevas estrategias y herramientas que les permitan llevar a cabo ciberataques. Por ello, hoy en día existen diversidad de formas de ataques cibernéticos a los que todos los usuarios se encuentran expuestos y que la mayoría desconoce. A continuación, se detallan los ataques cibernéticos más comunes que se presentan en la navegación web.

4.6.1. DNS spoofing (suplantación de DNS)

Es un tipo de ataque en el que un atacante falsifica las respuestas del Sistema de Nombres de Dominio (DNS) con el fin de redirigir el tráfico de Internet a sitios web maliciosos o controlados por el atacante. Esto se puede lograr de las siguientes maneras:

- Caché Poisoning (Envenenamiento de caché). El atacante explota una vulnerabilidad en el software del servidor DNS para enviar respuestas DNS falsas y contaminar la caché del servidor DNS. De esta manera, cuando un usuario solicita un nombre de dominio en particular, recibirá la respuesta falsa del servidor DNS comprometido (Jakobsson, Myers, 2006, p. 124).
- Man-in-the-Middle (Hombre en el medio). El atacante se coloca entre el usuario y el servidor DNS legítimo, interceptando y modificando las respuestas DNS que se envían al usuario. De esta manera, el atacante puede redirigir al usuario a sitios web maliciosos sin su conocimiento (Jakobsson, Myers, 2006, p. 623).
- DNS Pharming. El atacante compromete el enrutador o servidor DNS de una red y modifica su configuración para redirigir a los usuarios a sitios web maliciosos. Esta técnica puede

afectar a múltiples usuarios dentro de una red y es particularmente peligrosa, ya que no requiere la intervención directa del usuario (Jakobsson, Myers, 2006, p. 123).

4.7. ARP Spoofing

En lugar de falsificar respuestas DNS, el atacante manipula las tablas ARP en una red local para asociar su propia dirección MAC con la dirección IP de otro dispositivo. Esto le permite interceptar y manipular el tráfico de red destinado a ese dispositivo (Ramesh, Bhaskari, 2010).

4.8. Web Spoofing

El atacante registra un nombre de dominio similar o mal escrito a un dominio legítimo con el objetivo de confundir a los usuarios y dirigirlos a un sitio web malicioso (Ramesh, Bhaskari, 2010).

- Rootkit Este malware está diseñado para modificar el sistema operativo para crear una puerta trasera, que los atacantes pueden usar para acceder a su computadora de forma remota. La mayoría de los rootkits aprovecha las vulnerabilidades de software para ganar acceso a recurso que normalmente no debería ser accesibles (escalada de privilegios) y modificar los archivos del sistema (Cisco, 2023).

4.9. Cryptojacking

“Es un tipo de delito informático que consiste en minar criptomonedas utilizando computadoras, smartphones, tablets o incluso servidores de personas que no han autorizado tal uso.” - Kaspersky

4.10. Intento de intrusión

Es un evento en el cual el intruso/cibercriminal trata de obtener acceso a un sistema y a sus recursos sin ninguna autorización a través de la explotación de una vulnerabilidad. También conocidas como ataques de día 0 (Sonic Wall, Cyber Thread, 2023, p. 53).

4.11. Conceptos importantes de seguridad en la información

4.11.1. Activos de información

Los activos de información son todos los recursos tangibles e intangibles que poseen un valor para los usuarios. Estos pueden ser de varios tipos, tales como bases de datos, sistemas informáticos, redes, software, hardware y todo dispositivo que contenga información en tránsito o en reposo (What Is an Information Asset? | Information Security, 2023).

4.11.2. Clasificación de los activos de información

Alta Categoría

Esta clasificación comprende todos los activos de información los cuales cualquier alteración, divulgación o pérdida de estos causaría varios daños y perjuicios a la empresa, organización, personas. Los cambios se reflejan en un impacto negativo en sus producciones, prestación de servicios, procesos (Massachusetts Institute of Technology, 2023.).

Ejemplos de estos son datos financieros, información de clientes, propiedad intelectual, secretos comerciales, nuevas tecnologías, procesos, información de empleados.

Media Categoría

Comprendes todos los activos los cuales su divulgación, pérdida o alteración pueden llegar a perjudicar negativamente los procesos, operaciones y la prestación de servicios de una organización a un punto donde estos pueden llegar a ser recuperables o reconstruibles en un tiempo que es posible estimar y alcanzable para retomar operaciones (Massachusetts Institute of Technology, 2023).

Como ejemplos de activos de información que son clasificados en esta categoría, se pueden encontrar, información operativa, documentaciones, datos de inventario, comunicaciones internas y externas.

Baja Categoría

Los menos importantes dentro de la clasificación, se debe a que estos activos por lo regular el impacto de la pérdida, divulgación o robo no impacta directamente la producción, operación y prestación de servicios de la organización (Massachusetts Institute of Technology, 2023.).

Debido a que la mayoría de estos son de dominio público o de prueba, son datos replicables en cualquier momento. Ejemplos de ellos serían la documentación existente de la persona, organización o empresa que existe en el internet, información que se utiliza para entrenamiento u información de eventos.

4.11.3. Instituciones educativas y sus activos de información

La mayoría de las instituciones educativas tienen consigo activos de información a su disposición, esto debido a que deben de guardar toda la información posible de sus empleados tales como: maestros, personal administrativo, personal de limpieza, cocineros, directores, entre otros además de sus clientes tales como; estudiantes y padres de familia. Estos datos corren peligro de ser robados, divulgados y alterados en estos tiempos, donde la ciberdelincuencia está creciendo y donde cada vez se vuelve común ver empresas grandes y de renombre caer ante ciberataques donde se filtra información confidencial de sus bases de datos, sistemas y aplicaciones. Los activos de información que se pueden encontrar y se deben de proteger en una institución educativo son los siguientes:

Bases de datos

Se le conoce así al sistema que permite el almacenamiento de información de forma ordenada y almacenada de forma electrónica. Esta tiene la capacidad de almacenar todo tipo de información, desde palabras, números, imágenes, vídeos y archivos. Las bases de datos tienen sistemas de administración que permiten la modificación, edición, recuperación y eliminación de datos.

En una institución educativa es importante el tener una base de datos de este tipo que permita tener la información de los clientes y todo tipo de empleados a la mano además de las interacciones nuevas que se contemplan al pasar de los años. Las bases de datos son esenciales para poder aumentar el alcance de la institución por el hecho de que se puede tener el acceso a miles y miles de datos. Los datos se mantienen ordenados e íntegros (Amazon Web Service, 2023.).

Sistemas Informáticos

Son el conjunto de elementos físicos y lógicos que tienen como funcionalidad principal el almacenaje, recibimiento y procesado de datos para luego mostrar resultados (Chavez, 2023.).

Claros ejemplos de SI (Sistemas Informáticos) son servidores, computadoras, routers, laptops. Estos debido a que manejan datos dentro de sus aplicaciones, softwares, instrucciones entre otros. Además de manejar datos, existe personal que interactúa con estos sistemas, en un centro educativo este personal son los estudiantes, maestros, directores y otros.

Redes Informáticas

Las redes informáticas son todas las redes de comunicación que transmiten datos a través de varios dispositivos electrónicos conectados, alámbrica o inalámbricamente, entre sí. El internet se puede considerar una red informática global la cual permite la comunicación directa entre varios dispositivos que puedan tener acceso a ella. Por lo tanto, en una institución educativa el internet, los laboratorios de computación, los teléfonos, laptops son parte de las redes, las cuales en su tráfico existe información de diferentes categorías (Editorial Etecé, 2021).

Softwares

Los softwares son un conjunto de reglas o programas que dan instrucciones al dispositivo, sea computadora, laptop, teléfono o cualquier dispositivo, para la ejecución de un programa o aplicación. El objetivo principal de estos es el automatizar desde los más simples procesos de un dispositivo como la escritura o más complejos (Jain, 2023).

Los softwares son parte de los activos de información que una institución cuenta, esto se debe a que son parte fundamental del funcionamiento de todos los dispositivos conectados a la red informática por lo que estos se mantienen en constante ejecución hasta que se hayan desconectado de la red.

4.11.4. Los tres pilares de la seguridad de la información

Confidencialidad

Una propiedad que se debe de mantener, el propósito principal es proteger la divulgación de información delicada con usuarios que no tienen acceso a ella. En esta investigación el enfoque de que nadie pueda acceder a la información de los usuarios, más que ellos. Previene la divulgación de información entre los usuarios que tengan acceso a ella con los que no lo tienen. Las organizaciones y personas para mantener su posición en el mercado tienen que mantener en secreto la información que les permite crecer como tal (Mifsud, 2022).

Integridad

Una propiedad que procura mantener la información de ser preciosa y completa, además de garantizar que estos no puedan alterarse en ningún momento sin autorización del usuario. El objetivo principal que se cumple es que la información no pueda ser accedida cuando esta no se encuentre en reposo, lo que permite que la información sea de confianza y no modificable entre el envío y recepción de esta. Esta propiedad promueve la confianza, exactitud y credibilidad de la información (Mifsud, 2022).

Disponibilidad

Última propiedad de la información está procurando que la información esté siempre disponible y accesible a la persona que lo requiera y tenga el permiso de acceder a ella. La disponibilidad siempre radicará en los permisos que la persona tenga en la organización o empresa para acceder a cierto tipo de información, por lo que es importante que cada una de estas tenga un nivel de gestión de acceso para determinar qué información se puede ver y por quien se puede ver (Mifsud, 2022).

4.11.5. Gestión de riesgos

El proceso de identificación, evaluación y mitigación de riesgos asociados a la seguridad informática de los usuarios. Lo más importante es la implementación de mecanismos de defensa y preventivos a estos ataques (Stanleigh, 2011).

Sistemas de gestión de riesgos

Los sistemas de gestión de riesgos están diseñados no solo para analizar los riesgos, sino también para cuantificarlos, clasificarlos y predecir el posible daño que podrían causar a un proyecto en desarrollo. Es importante entender que obtener datos cruciales sobre los riesgos potenciales no evitará que estos ocurran, pero sí permitirá mitigar sus impactos, clasificándolos como aceptables o inaceptables. La decisión sobre la aceptabilidad del riesgo dependerá siempre del encargado del desarrollo del proyecto (Stanleigh, 2011).

Los sistemas de gestión de riesgo bien configurados, mayormente de forma continua, permiten una mejoría en varios aspectos de la organización con respecto a planificación, calendarización de procesos, control de costos y presupuestos.

Gestión de riesgos de forma continua

La detección continua de los riesgos que pueden ocurrir gracias al sistema de gestión debe de ser clasificados en diferentes categorías que contemplen la posible ocurrencia de estos, es decir existen riesgos con más probabilidades de suceder que otros, por lo que, su nivel de importancia para mitigarlos es mayor.

La importancia de tener una gestión de riesgos continuo durante el ciclo de vida de un proyecto (desde el inicio hasta la puesta en producción) es que se debe de ser consiente de los posibles ataques y riesgos que se pueden presentar. Al principio los riesgos y medidas son leves, pues no hay tanto en juego, todavía se está en un nivel de exploración y planificación del proyecto, pero la curva y brecha entre el riesgo y lo posible a perder empieza a crecer conforme se está ejecutando el proyecto, lo que cualquier riesgo que se pueda encontrar, afectará negativamente y en gran manera el proyecto (Stanleigh, 2011).

4.11.6. Ciberseguridad

Son las prácticas y principios que se deben de implementar para la correcta protección de equipos, redes, datos y dispositivos tecnológicos que contengan información por posibles ataques informáticos y amenazas digitales (Amazon Web Service, n.d.).

La importancia de la ciberseguridad como se mencionan en varios artículos se basa plenamente en proteger los recursos digitales y todo sistema frente a ataques informáticos y amenazas digitales que permitan el obtener cualquier tipo de acceso a ellos.

Se le conoce como ataques informáticos, al intento de acceder a un dispositivo electrónico mediante diferentes métodos con diferentes fines. Los fines más comunes son intrusión al sistema informático, desactivación de servicios, robo de identidad, robo de datos y mayoritariamente causar daños irreparables a la víctima (Amazon Web Service, n.d.).

Todo proceso o método que atenta contra la seguridad de la información de cualquier persona o individuo se considera una amenaza digital. Estas pueden encontrarse al navegar por aplicaciones, páginas web, internet, entre otras.

¿De qué ataques se busca defenderse en la ciberseguridad?

Malware

Es el término que se utiliza para referirse a todo tipo de software malicioso. Se le conoce así a todo software que busca infiltrarse en el dispositivo en el cual fue accionado sin el conocimiento del usuario, con el motivo principal de divulgar, robar, alterar información y en casos mayores impactar negativamente el funcionamiento de los sistemas (Belcic, 2023).

En los ejemplos de malware se encuentran los siguientes:

- Adware
  Un malware que muestra anuncios con información llamativa a los usuarios para que estos caigan en la tentación de clicear en alguno de estos y de esta forma darles acceso a los atacantes a obtener datos de navegación, que posteriormente pueden ser vendidos a terceros y de esa forma lo compradores de estos datos, hacer anuncios personalizados ya verídicos

y de nuestro interés (AVAST, 2020).

- Spyware
  Es un tipo de software, similar al adware debido a que su principal objetivo es la recopilación de datos, aunque este es más peligroso, dado que se inyecta de forma sigilosa en el sistema operativo. El resultado de que este software se encuentre en el sistema operativo es que básicamente recopila cada dato de navegación, internet, información personal guardada en la computadora, entre otros datos que son importantes para la víctima (Seguin, 2020).

- Virus
  Uno de los malwares más peligrosos con respecto al alcance que pueden tener sobre la víctima. Este alcance se mide respecto a la cantidad de archivos, aplicaciones y documentos a los cual se adhiere, sumándole que puede alterar y en algunos casos borrar la información de estos. La propagación de este tipo de malware es sencilla, se va copiando de archivo en archivo hasta que sea encontrado por la víctima, mientras tanto su labor está hecha (Norton, n.d.).

- Troyanos
  Un malware que se esconde tras aplicaciones o archivos que parecen que no son maliciosos. Las aplicaciones tienen por detrás programadas las funciones de un malware y pues cada vez que esta se ejecuta, este malware empieza a hacer efecto en lo que es el dispositivo, información, entre otros (Kaspersky, n.d.).

Ransomware

Este a pesar de ser un tipo de malware, tiene su propia clasificación porque el objetivo principal no es recabar, divulgar o robar información (a pesar de que si lo hacen) sino que es obtener dinero de las víctimas reteniendo información importante para ellos. La evolución de estos ha incrementado hasta extorsionar más de tres veces, amenazando a la persona u organización de realizar cualquier acción con la data por la cual se pide el rescate (Amazon Web Service, n.d.).

Phishing

Un ataque que consiste habitualmente en el recibimiento de correos electrónicos, llamadas telefónicas, mensajes de texto o incluso hasta sitios web que parecen inofensivos con el fin de manipular a las personas para que estas lleguen a compartir información importante y confidencial sobre ellos, descarguen aplicaciones con malware he incluso realizar acciones que perjudiquen en un futuro a su persona u organización a la cual trabajan (IBM, n.d.).

Si bien el phishing es un ataque, es una de las maneras por la cual la ingeniería social toma fuerza en estos tiempos, como se mencionó anteriormente, la ingeniería social es un conjunto de técnicas de manipulación utilizadas por los ciberdelincuentes, lo cual permite que el atacante obtenga toda la información que desee, desde una apariencia inofensiva.

Los ejemplos de phishing más comunes son:

- Spam de correos electrónicos

  El atacante crea un correo que tiene apariencia inofensiva, esto se debe a que utilizan

dominios parecidos a empresas legítimas, organizaciones grandes y reconocidas alrededor del mundo, y luego enviándolo a millones de personas y posibles víctimas. Basado en probabilidades, mientras más grande sea la muestra, es más probable que se obtengan resultados favorables, en este caso la obtención de información de los destinarios (Kaspersky, n.d.).

El correo, además de tener una credibilidad con respecto al dominio similar que usan, también utiliza las emociones para la manipulación de las personas que lo reciben. Jugando con palabras que generan miedo, codicia, curiosidad, alegría y sentido de urgencia para resultar en tener la atención de los que reciben el phishing. Los asuntos más comunes son: "Actualiza Datos", "Problemas con su pedido", "Documentos Faltantes", entre otros.

El cuerpo del correo electrónico cuenta con oraciones coherentes y que tienen lógica con respecto a lo que se pide y por ello, las personas caen en estos correos compartiendo información importante y confidencial o peor aún descargar un malware que perjudique de mayor forma. Concluyendo que las personas toman decisiones según los sesgos que estos tienen.

- Suplantación de identidad

  Este tipo de phishing es diferente al anterior, esto debido a que no se envían correos electrónicos de forma masiva sino a un destinatario en particular el cual tiene acceso a información confidencial de una organización o que tiene información muy valiosa consigo. Por lo que el correo estará orientado a obtener permisos y accesos de una persona de alto valor y nivel en cualquier ámbito (Microsoft, n.d.).

  El proceso es sencillo, el atacante procura conocer a la víctima para poder falsificar la identidad de alguien de fiar, puede ser un amigo, familiar, jefe o compañero de trabajo. Luego procede a crear el perfil falso aprovechándose de las redes sociales, debido a la fácil interacción que estas ofrecen y los datos que estas proveen de forma pública, donde las personas postean varios de estos. Los mensajes más comunes que pueden encontrarse son: "¿Vas de vacaciones a X lugar?, aparta y paga de una vez", "Ahórrate tiempo pagando esta factura en línea", "Transfiere X cantidad, necesito pagar esto".

  En casos de mayor escala, el destinatario puede ser un CEO de una empresa, donde se le menciona que han perdido sus credenciales o permisos y que este actualice sus datos personales y credenciales, llenando así un formulario el cual se robara sus credenciales. Luego a partir del robo de credenciales el atacante puede solicitar cualquier acceso o permiso debido al robo de identidad del CEO de la empresa y este lo obtendrá debido al alto cargo que tiene esta identidad en la empresa.

Baiting

El baiting es como un "Caballo de Troya". Emplea medios físicos y se basa en la curiosidad o avaricia de la víctima. En muchos sentidos, es similar a los ataques de phishing. Sin embargo, lo que los distingue de otros tipos de ingeniería social es la promesa de un artículo u objeto que los hackers usan para atraer a sus víctimas. Los "baiters" (como se les llama a estos atacantes) pueden ofrecerles a los usuarios descargas gratuitas de música o películas, si les dan sus credenciales de inicio de sesión a una determinada página. Pero estos atacantes no se limitan a emplear tácticas online. También pueden enfocarse en explotar la curiosidad humana usando medios físicos. (Nadeem, 2022)

4.11.7. Frameworks de seguridad

CobIT

CobIT o Control Objectives for Informatión and Related Technology, es un framework para la evaluación y monitoreo del flujo de negocios y además de la seguridad de TI. Abarca controles específicos de tecnología orientados a una perspectiva de negocios. En el mundo de la seguridad informática, el objetivo principal de CobIT es proveer información que cumpla con los estándares; disponibilidad, integridad y confidencialidad (Editorial Esp, 2021).

Normas ISO

Son el conjunto de normas estandarizadas a nivel internacional para ayudar a las empresas a homogeneizar la relación de gestión, prestación de servicios y desarrollo de productos. Las normas ISO orientadas a la seguridad de la información son:

- ISO 15408 (Common Criteria)

  Esta ISO tiene como objetivo principal, presentar una evaluación de la seguridad en productos tecnológicos que almacenen información. Siendo este un conjunto de criterios y requisitos para la evaluación y certificación de seguridad de productos (Organización Internacional de Normalización, 2022).

  Existen varios niveles de evaluación, con diferentes requisitos y procedimientos específicos. Por lo que, es importante fijarse en que los productos hayan pasado por estándares, revisiones, evaluaciones y que estos hayan cumplido con la mayoría para que se consideren seguros por parte de los elaboradores y usuarios.

  En instituciones estudiantiles, el implementar esta norma a los sistemas de gestión y almacenamiento de datos personales, es requerido debido a que es necesario que estos datos no se divulguen, alteren o similar por ningún motivo, porque no cumpliría con los estándares principales de los datos, confidencialidad, integridad y disponibilidad. El tener acreditada esta norma en la organización, determinará y garantizará un nivel alto de seguridad en la misma.

- ISO 27001

  Una norma que establece varios requisitos para los sistemas de gestión de riesgos, los cuales deben velar por la seguridad de la información con respecto a cualquier posible riesgo que pueda suceder (Organización Internacional de Normalización, 2022).

  El implementar esta norma en una institución, generaría una mejora continua con respecto a la adaptabilidad de nuevos riesgos y amenazas, además que establecería que la organización cumple con los criterios y estándares acerca de la privacidad de datos y controles de seguridad. Estos criterios y estándares pueden verse a la hora de que el establecimiento tenga evaluación constante de los datos estudiantiles, evaluación de riesgos para estos datos, autenticaciones fuertes para acceder a recursos de la universidad y realización de auditorías para el avance continuo.

- ISO 27002

Similar a la anterior ISO, proporciona directrices y controles detallados de seguridad para la implementación de un sistema de gestión enfocado en esta. Acreditar esta norma en instituciones u organizaciones, permitirá la adaptación de controles de seguridad con requisitos específicos y riesgos además de tener las mejores prácticas reconocidas para la seguridad de la información (Organización Internacional de Normalización, 2022).

Una institución puede aprovechar esta norma para poner en marcha políticas para la creación de contraseñas seguras y doble autenticación a los usuarios, políticas y controles en el firewall, detección de intrusos. Lo más importante de esta norma es activar un manejo de incidentes correcto para abordar todas las violaciones de seguridad de la mejor manera y un sistema de evaluaciones y análisis continuos para la mejoría del sistema seguro.

- ISO 27004

  Una norma que tiene como objetivo principal monitorear que los sistemas de gestión de seguridad de la información estén bien implementados, proveyendo directrices y controles para mantener un programa de medición con métricas de seguridad (Organización Internacional de Normalización, 2016).

  Como se explicó anteriormente, se debe a que va por un enfoque de monitorear lo que se haya implementado antes por las demás normas ISO, sus ventajas se basan en evaluar la efectividad de los sistemas, tomar decisiones para protección de los datos, y como la mayoría de las normas, mejoras. En una organización estudiantil, el poner en práctica el monitoreo constante de los sistemas seguros, se pueden definir tasas de ocurrencia de incidentes, tasa de recuperación del sistema, documentación para la seguridad y evaluación de efectividad de los sistemas de gestión.

- ISO 27005

  Una norma que brinda explicaciones detalladas para establecer un proceso de gestión de riesgos que ayude a la identificación, evaluación y solución de estos para proveer una seguridad correcta de la información. Es provechosa esta norma, al permitir la identificación de riesgos, logra una postura temprana para actuar y proteger la información y datos de los usuarios, también establece una gestión ordenada para saber en qué riesgo enfocar más recursos y tiempo, resultando en una eficiencia mayor con respecto a estos (Organización Internacional de Normalización, 2022).

  Dentro de las ventajas de poner en práctica la teoría de esta norma, se pueden conseguir avances con respecto a la identificación de activos de información del instituto escolar, evaluar sus riesgos y amenazas asociados e implementar las soluciones de seguridad como controles, políticas y exploración de nuevos ataques.

- ISO 27032

  Esta norma es una de las más importantes a tomar en cuenta para la mejora en ciberseguridad de cualquier organización, porque presenta conjuntos de directrices y consejos para mejorar la protección de datos, gestión de ciberataques (Organización Internacional de Normalización, 2023).

  Las directrices permiten un buen fortalecimiento en temas de seguridad y protección de la información frente a incidentes, riesgos y amenazas. Esto implementado en instituciones educativas puede dar resultados positivos en temas de planeación de respuesta para ataques, establecer comités entre varias instituciones para buscar soluciones en conjunto, junto a concientización de los ataques actuales y comunes. Por último, las buenas y mejores

prácticas para la protección de la información de los estudiantes.

La implementación de estas normas en la Universidad del Valle de Guatemala presentará resultados muy beneficiosos para la seguridad informática de la misma. Los activos de información críticos son los que se deberían de velar siempre en cualquier institución, en el caso de un instituto escolar, universitaria el activo más importante de información son los estudiantes, empleados, padres de familia por lo que concientizar y asegurar la protección de los datos de estos, procurará en gran manera mitigar cualquier riesgo y amenaza.

En conjunto, estas prácticas y enfoques son fundamentales para crear un entorno académico seguro y resistente a amenazas cibernéticas, permitiendo que los estudiantes, empleados, padres de familias adquieran las habilidades necesarias para protegerse de cualquier riesgo, amenaza, ataque. La protección de datos sensibles y confidenciales, la toma de decisiones informadas en la gestión de riesgos son componentes esenciales de esta iniciativa para la mejora continua de seguridad en un entorno que contenga activos de información críticos. Es esencial el implementar estas normas, pues el beneficio es para todos los que estén involucrados incluso en los que rodean a estos indirectamente saldrán provechosos, pues el conocimiento se comparte entre todos.

4.12. Tipos de información

4.12.1. Fuentes de información

Son todos aquellos medios de los cuales procede la información, que satisfacen las necesidades de conocimiento de una situación o problema presentado y, que posteriormente será utilizado para lograr los objetivos esperados (Miranda, 2008).

4.12.2. Información primaria

Son todos aquellos usuarios y acompañantes a quienes se les aplicó un instrumento de investigación. En este caso, los datos provienen directamente de la población o una muestra de la misma. Estas fuentes contienen información original, que se publicó por primera vez y que no ha sido filtrada, interpretada o evaluada por nadie más. Son producto de una investigación o de una actividad eminentemente creativa (Miranda, 2008).

4.12.3. Información secundaria

Son las que contienen información primaria, sintetizada y reorganizada. Están especialmente diseñadas para facilitar y maximizar el acceso a las fuentes primarias o a sus contenidos. Parten de datos preelaborados, como pueden ser datos obtenidos de anuarios estadísticos, de Internet, de medios de comunicación, de bases de datos procesadas con otros fines, artículos y documentos relacionados con la enfermedad, libros, tesis, informes oficiales, entre otros (Miranda, 2008). Las fuentes secundarias pueden proceder de:

- Fuentes oficiales: Cuando los datos son suministrados por cualquier ente gubernamental.
- Fuentes privadas: Cuando la información es suministrada por personas u organismos no gubernamentales.

4.13. Python

4.13.1 Definición Python

Python es un lenguaje de programación interpretado de tipado dinámico cuya filosofía hace hincapié en una sintaxis que favorezca un código legible. Se trata de un lenguaje de programación multiparadigma y disponible en varias plataformas (Gaston, s.f). Dicho de otro modo, Python es, interpretado, la ejecución sin necesidad de ser procesado por el compilador y se detectan los errores en tiempo de ejecución. Soporta programación funcional, programación imperativa y programación orientada a objetos. Las variables se comprueban en tiempo de ejecución. Multiplataforma disponible para plataformas de Windows, Linux o MAC. Gratuito: No dispone de licencia para programar (Gaston, s.f).

4.14 Bibliotecas para análisis de datos

4.14.1. Numpy

Es la abreviatura de Numerical Python: una biblioteca que provee entre otras funciones, arreglos multidimensionales, Funciones operando sobre 8 los objetos de los arreglos, herramientas de escritura y lectura al disco, operaciones de álgebra lineal y conexión con otros lenguajes de programación como C, C++ y Fortran. Debido a la velocidad de procesamiento de las operaciones sobre arreglos de NumPy hacen que Python se convierta en uno de los principales lenguajes para manipulación de datos intermedios sin necesidad de copiar la información durante las manipulaciones (McKinney, s.f).

4.14.2. Pandas

Esta biblioteca de Python provee estructuras de datos con funciones para diseñadas para su manipulación con el objetivo de análisis de datos rápido y eficiente. La estructura de datos más utilizada de la biblioteca es el DataFrame, un objeto bidimensional con filas y columnas similar a una matriz. Combinado con la capacidad de manipulación de bases de datos Relacionales como SQL (McKinney, s.f).

4.14.3. Matplotlib

Es una de las bibliotecas más populares de Python para producir gráficos y representaciones bidimensionales de información. Bajo continuo mantenimiento por una comunidad voluntaria de programadores. Provee un entorno interactivo durante la exploración de la información (McKinney, s.f).

4.14.4. Seaborn

Seaborn es una biblioteca para crear gráficos estadísticos en Python. Se basa en matplotlib y se

integra estrechamente con las estructuras de datos de pandas (Waskom, s.f.).

Seaborn ayuda a explorar y comprender sus datos. Sus funciones de trazado operan en marcos de datos y matrices que contienen conjuntos de datos completos y realizan internamente el mapeo semántico y la agregación estadística necesarios para producir gráficos informativos (Waskom, s.f.).

4.14.5. Scipy

Scipy es la colección de múltiples paquetes de Python, es el paquete estándar de computación científica que incluye solucionadores de ecuaciones, optimizadores de Funciones, herramientas de proceso de señales, distribuciones de probabilidad estándar y herramientas de uso de C + + en computaciones de Arreglos (McKinney, s.f).

4.15 Análisis de datos

4.15.1. Definición de análisis de datos

El análisis de datos convierte datos sin procesar en información práctica. Incluye una serie de herramientas, tecnologías y procesos para encontrar tendencias y resolver problemas mediante datos. Los análisis de datos pueden dar forma a procesos empresariales, mejorar la toma de decisiones e impulsar el crecimiento empresarial (AWS, 2023).

4.15.2. Análisis exploratorio de datos

El Análisis Exploratorio de Datos (A.E.D.) es un conjunto de técnicas estadísticas cuya finalidad es conseguir un entendimiento básico de los datos y de las relaciones existentes entre las variables analizadas.

Los científicos de datos utilizan el análisis de datos exploratorios (EDA) para analizar e investigar conjuntos de datos y resumir sus características principales, a menudo empleando métodos de visualización de datos. Ayuda a determinar la mejor manera de manipular las fuentes de datos para obtener las respuestas que necesita, lo que facilita que los científicos de datos descubran patrones, detecten anomalías, prueben una hipótesis o verifiquen suposiciones.

4.15.3. Datos

Es la representación que se le da a cualquier tipo de información que al ser procesada se les muestra a los usuarios de forma legible (Fitzgibbons, 2019). Existen varias clasificaciones de los datos:

Datos en tránsito

Son datos que se mantienen en transmisión entre dispositivos (Fitzgibbons, 2019).

Datos en reposo

Son datos que se mantienen almacenados en una estructura, como una base de datos (Fitzgibbons, 2019).

Datos en uso

Son los datos con los cuales fueron procesados para mostrar información legible al usuario (Fitzgibbons, 2019).

Datos cualitativos

Se denominan datos cualitativos a todos aquellos que buscan caracterizar o resaltar atributos de un hecho, persona, comunidad, organización o situación no medible o sujeta a representación numérica (Peña,2017).

Datos nominales

Se refiere a una expresión realizada o forma de caracterizar una variable determinada (Peña, 2017).

Datos ordinales

Son aquellos que se usan para denotar un orden en un conjunto de atributos que se asignan para caracterizar una variable cualitativa (Peña, 2017).

Datos cuantitativos

Con aquellos susceptibles a la medición y representación numérica (Peña, 2017).

Datos discretos

Datos que sólo pueden tomar un conjunto finito de valores, surgen a partir de un conteo, se representan con cantidades enteras (Peña, 2017).

Datos continuos

Son aquellos datos que pueden toman un conjunto infinito de valores, estos datos se admiten valores expresados con números decimales o fraccionarios (Peña, 2017).

4.16 Limpieza de datos

Detección de valores atípicos

La detección de valores atípicos a menudo se enfoca en anomalías de datos con respecto a la definición de los valores normales para la implementación. Puede ayudar a detectar posibles intrusiones y actividades maliciosas dentro de la información (Ilyas, Chu, 2019).

Entre los desafíos de la detección de valores atípicos se encuentra la búsqueda del patrón normal. Además de esto, muchas técnicas de detección de valores atípicos pierden efectividad cuando el número de atributos en el conjunto de datos es extenso (Ilyas. Chu, 2019).

Duplicidad de datos

La duplicación de datos puede ocurrir por muchas razones, como por ejemplo tener múltiples representaciones después de integración de datos o ingreso de datos repetidos. La duplicación de datos se refiere a al proceso de identificación de tuplas que se refieren a la misma entidad del mundo real. Usualmente seguido de una consolidación de entidades para unificar las representaciones duplicadas para que representen de mejor manera a la entidad del mundo real (Ilyas, Chu, 2019).

Transformación de datos

La transformación de datos se refiere a la preparación de la información mediante a programas definidos que buscan convertir los datos en información que se adecue a un formato o estructura. Se dividen en dos categorías, transformaciones sintácticas y transformaciones semánticas (Ilyas, Chu, 2019).

CAPÍTULO 5

Antecedentes

5.1. Estudios relacionados

Puede encontrarse un trabajo relacionado en:

Estudio sobre los conceptos para desarrollar apps seguras sin dejar de lado la experiencia del usuario utilizando el sistema, de manera que no sea pesado ni complicado para el usuario utilizar el sistema y permanecer seguro durante su uso Saideep (Saideep, 2020).

Artículo que habla de los resultados que un equipo de investigadores obtuvo luego de realizar pruebas y juegos con adolescentes y niños. Posteriormente desarrollan herramientas en conjunto con los adolescentes y niños para ayudarlos a evitar ataques (Kumar y cols., 2023).

Artículo sobre los factores a tomar en cuenta para desarrollar páginas web y evitar ataques, asimismo nos muestran qué patrones pueden ayudar al usuario a reconocer páginas maliciosas (Doan, 2020).

Las ideas clave del cuarto artículo científico (Veksler y cols., 2020) radica en tener las dos caras de la moneda. Dentro de la investigación desarrollaron dos modelos basados en inteligencia artificial, uno para demostrar la defensa de una persona que va a recibir un ataque y el otro modelo para demostrar el comportamiento de un atacante para decidir la víctima de su próximo ataque. Las métricas evaluadas en el primer modelo fue el éxito para detectar que se está siendo atacado y la métrica de evaluación del segundo modelo fue el seleccionar cuales son las decisiones tomadas para escoger a la persona vulnerable, el crear un perfil de usuario vulnerable. Como conclusiones relevantes podemos obtener que:

- El desarrollo de modelos cognitivos debe de ser una disciplina de estudio para poder obtener mejoras en el ámbito de ciberseguridad y otros dominios.
- El poder realizar modelos cognitivos nos da la oportunidad de modelar tanto el procesamiento de pensamientos y toma de decisiones de los atacantes y víctimas, de esta forma desarrollar roadmaps que puedan orientar a las personas a no caer en estos ataques.

Cómo desconocimientos que se pueden extraer de este artículo radican en el tener un estudio

más centrado en el pensamiento de los jóvenes entre 16 a 21 años, pues no se menciona la edad de los participantes por lo que el estudio pudo haberse realizado con una muestra variada en temas de edad, características, experiencias y sesgos.

En los dos artículos siguientes, (Gate, 2021a), podemos encontrar un estudio más centrado en jóvenes entre las edades que se estudiarán en esta investigación, por lo que hay un enfoque más preciso. En uno de ellos se determinó que los ataques cibernéticos son más propensos a suceder que otros tipos de ataques que ellos mencionan. Estos ataques afectan a personas entre 10 a 16 años, por lo que concluye que, la gente mayor es más vulnerable a estos ataques, además de que la otra conclusión radica en que la falta de seguridad en la vida fuera de línea y sus comportamientos, pueden traspasarse a la vida en línea, donde hay más peligros y los cuales se deben mitigar con la correcta educación de las personas.

Esto último es importante, pues nuestros comportamientos, conocimientos, experiencias y sesgos no sólo existen en nuestro día a día entre interacciones con personas, sino que esta también existe a la hora de interactuar con algún objeto del mundo virtual, ya sea el internet, correos electrónicos, mensajes de texto y todo lo relacionado al mundo en línea.

El quinto artículos (Gate, 2021b) indica el éxito que tuvo un programa de capacitación con respecto a la seguridad de la información y como esta durante cada año que pasaba de implementación se veía un cambio en la comprensión de riesgos cibernéticos por parte de los estudiantes.

Esto indica que el proveer información y concientización acerca de seguridad informática, mejora el desempeño de los jóvenes al estar navegando en línea, compartir datos en redes sociales y además da un panorama más grande de los peligros que pueden existir en los casos de no darle importancia a estos.

Con respecto al desconocimiento de estos artículos, se pudieron obtener otras conclusiones más que el comportamiento de las personas, tales como las prácticas, estímulos y reacciones que las personas tenían durante estos ataques, lo cual se centra nuestra investigación.

El sexto artículos (Saeed, 2023) habla acerca de un estudio realizado en una universidad de Arabía Saudi, en donde por obtención de datos empíricos mediante cuestionarios lograron determinar que los estudiantes no consideran la gestión de buenas prácticas para la elaboración de contraseñas como parte de la seguridad de la información además de que no relacionaban la percepción como parte de la seguridad. Lo importante de este artículo, es que el presentar recomendaciones generaría riqueza en conocimiento para las instituciones escolares y gubernamentales para la mejora de la seguridad.

Según la investigación llamada *The Human Factor in Phishing*, por Markus J. se mencionan diferentes puntos por los cuales un usuario puede caer en una estafa de tipo Phishing a través de un estudio realizado entre 2500 personas. Estos son algunas de las conclusiones:

- La gramática y diseño del mensaje/página web influye mucho en la decisión del usuario. Si la página no es llamativa, el usuario probablemente perderá interés dado a que no hay nada que le llame la atención. Y respecto a la gramática, si no cuenta con una buena redacción el mensaje el usuario puede pensar que es una estafa o simplemente lo ignorará porque no le encuentra sentido al mensaje.
- Si el correo/página web contiene el nombre y/o logo de una compañía, esto le dará al usuario confianza dado a que se basa en el hecho de que, si “el contenido que ve es por parte de una empresa reconocida, entonces ha de ser importante”. Por esta razón muchos de los correos

de tipo phishing hoy en día usan logos de empresas famosas a nivel mundial para que el usuario crea que sí vale la pena leer las indicaciones de dicho contenido.

- Las personas juzgan primero la relevancia antes que la autenticidad. Varios de los correos de tipo phishing contienen contenido que puede "jugar" con las emociones del usuario. En su mayoría empiezan diciendo algo similar a "tu cuenta de . . . ha sido bloqueada por problemas de autenticación. Para resolver este problema debe iniciar sesión usando el siguiente link". El usuario puede entrar en pánico e inicia sesión en la página web, y empieza a llenar todos los campos que se le piden. Incluso le piden tarjeta para conducir o número de pasaporte. Pero nunca se había percatado que la página web que ingresó no funciona del todo. Algunos botones al dar clic no realizan ninguna acción y la URL es una mezcla de letras y números. Esto es un ejemplo de cómo los estafadores usan una de las emociones que más hacen vulnerable al ser humano: el miedo.
- Símbolo de candado en la página web. Hoy en día, todos los navegadores proveen un indicador visual que permite al usuario ver si una página sigue los protocolos de seguridad actuales. Y este pequeño indicador juega un rol muy importante en la decisión del usuario. Cuando el usuario ve que el indicador no tiene una marca que indique "no es seguro" entonces eso aumentará su confianza y es muy posible que siga los pasos que se le indiquen. Páginas que fueron diseñadas para obtener la información del usuario sin su consentimiento intentan diseñar y programar páginas web que cumplan con los protocolos de seguridad de red para que se vea lo más verídico posible la página que intentan copiar.

En una investigación publicada por Forbes Advisor en 2023 llamada *The Real Risks Of Public Wi-Fi: Key Statistics And Usage Data*, con un grupo de estudio de 2,000 empleados que usaron Wi-Fi público en Estados Unidos concluyó en varios puntos:

- La mayoría (35%) de las personas accede a redes Wi-Fi públicas tres o cuatro veces al mes.
- El 23% de las personas utiliza Wi-Fi público para reducir el uso de datos móviles.
- El 20% utiliza Wi-Fi público para realizar transacciones financieras.
- Los lugares más comunes donde la gente usa Wi-Fi público son en restaurantes y hoteles.
- Cuatro de cada 10 han visto comprometida su información mientras utilizaban redes Wi-Fi públicas.
- La mayoría de las personas han visto comprometida su información en el Wi-Fi público de aeropuertos o restaurantes.
- La gente utiliza con mayor frecuencia Wi-Fi público en cafeterías y restaurantes (38%), hoteles (38%) y bibliotecas (33%).
- El 43% cree que el Wi-Fi público es algo seguro, el 23%, cree que es completamente seguro, el 20% considera que el Wi-Fi público es algo inseguro y el 5% lo considera nada seguro.
- El 40% de las personas utilizan una VPN cuando están conectadas a una red Wi-Fi pública.

5.1.1 El análisis cognitivo de tareas como estrategia metodológica para comprender y explicar la cognición humana

Esta investigación, elaborada por la PhD. Yenny Otálora, tiene como intención "describir e ilustrar el Análisis Cognitivo de Tareas (ACT)... para caracterizar la actividad cognitiva subyacente al desempeño de individuos cuando resuelven una tarea". El estudio abarca una variedad de modelos que implementan el ACT, además de una adaptación propia de la autora, para analizar los procesos cognitivos en tareas en psicología y educación, particularmente en la evaluación de habilidades matemáticas a nivel escolar. Por último, el estudio concluye que el método ACT es efectivo para la evaluación cognitiva de tareas.

Los aspectos relevantes que se relacionan con la presente investigación radican en la intención de entender los procesos cognitivos y de pensamiento que realiza un individuo al enfrentarse a la realización de una tarea y la toma de decisiones que la misma desencadena. Esta fuente aporta una metodología para identificar dichos procesos cognitivos a través de la separación de tareas en componentes, la cual se basa en los mismos principios psicológicos que rigen la metodología empleada en el presente estudio; así como una perspectiva simétrica de la forma en que los sujetos resuelven las tareas indicadas. Además, así como el estudio de la PhD. Otálora tiene un enfoque en la educación, el presente estudio tiene el objeto de proponer soluciones a ciertas vulnerabilidades, y para hacer efectiva dichas soluciones es importante tener presente el punto de vista educativo dado que la población al ser el eslabón más débil en ciberseguridad debe de ser educado en los riesgos del mundo digital, qué hacer, que no hacer y cómo mantenerse seguro.

En comparación, esta investigación se diferencia de que la autora del artículo realiza adaptaciones a los métodos contemporáneos de ACT para hacerlo más accesible a contextos escolares, mientras que en este estudio el enfoque es hacia estudiantes universitarios y su relación con la ciberseguridad.

En éste se explican conceptos para desarrollar apps seguras sin dejar de lado la experiencia del usuario utilizando el sistema, de manera que no sea pesado ni complicado para el usuario utilizar el sistema y permanecer seguro durante su uso Saideep (Saideep, 2020).

Este artículo habla de los resultados que un equipo de investigadores obtuvo luego de realizar pruebas y juegos con adolescentes y niños. Posteriormente desarrollan herramientas en conjunto con los adolescentes y niños para ayudarlos a evitar ataques (Kumar y cols., 2023).

En este artículo, nos dan factores a tomar en cuenta para desarrollar páginas web y evitar ataques, asimismo nos muestran qué patrones pueden ayudar al usuario a reconocer páginas maliciosas (Doan, 2020).

CAPÍTULO 6

Metodología

6.1. Sesgos de referencia

Dada la inmensa cantidad de sesgos reconocidos por la academia de psicología, para la realización de esta investigación fue indispensable contar con puntos de referencia que guíen el análisis para enfocarse en los hallazgos más relevantes y así entonces tener un impacto más significativo sobre los objetivos propuestos. Para lograrlo, se realizó una investigación en la que se determinaron cuáles serían los sesgos que servirían de referencia.

Se inició por investigar cuáles son los ataques más relevantes de ingeniería social, y como se muestra en la sección 4.1.8, estos fueron los siguientes: open Wi-Fi, phishing, password leak y bait.

Posteriormente, se enlistaron los posibles sesgos que con mayor facilidad podían ser explotados en cada uno de dichos ataques para así ver cuales sesgos se repetían más, y por lo tanto tenían más relevancia en este estudio, estos serían los que se utilizarían como referencia.

Cabe destacar que existe una infinidad de sesgos que pueden ser explotados en un sólo ataque y por lo tanto la investigación no se limitó a los sesgos de referencia (razón por la cual en los resultados y discusión se podrá observar la mención a varios sesgos que no forman parte de este grupo), pero desde el punto de vista cognitivo, estas referencias nos permitirán un marco de análisis base para entender de mejor manera el comportamiento de la población de estudio y encontrar de forma más eficiente correlaciones entre las respuestas de cada uno de los individuos de la muestra.

6.2. Desarrollo del marco de análisis ACT

Una vez que se conoce qué es lo que se busca estudiar de los individuos con los ataques más relevantes y los sesgos de referencia, nace la duda de ¿cómo evaluar a la muestra sin sesgarlos? Pues no se puede simular al cien por ciento un ataque; póngase el ejemplo de un phishing: sería muy sesgado decirle a un participante que responda al mensaje de phishing que le acabamos de

enviar, y enviarle un correo de phishing sin indicaciones puede introducir variables externas derivadas dela confusión del individuo al no saber qué hacer, sin embargo los eventos que nos interesan para la investigación no están inherentemente en el ataque, sino en cómo el individuo interactúa con los componentes clave de este. Siguiendo con el ejemplo del phishing estos componentes clave serían fijarse en la dirección de correo del emisor o prestarle poca atención, leer el contenido del correo o sólo escanearlo, entre otros factores que son propios de cualquier correo, pero pueden marcar la diferencia entre ser víctima de un ataque de phishing o no. Por esta razón, se dividió cada ataque en componentes clave que simulen de forma holística el ataque en cuestión, implementando de esta forma un marco de análisis que implementa un modelo de ACT adecuado a un contexto de ciberseguridad. Cada componente clave es denominado AOI (Area Of Interest) y para este estudio se midió la interacción de los individuos en cada AOI de forma separada utilizando un eye tracker de RealEye.io.

6.3. Investigación de campo

Para la investigación se solicitará la participación voluntaria, anónima y no remunerada de una muestra de estudiantes de la UVG representando equitativamente las distintas facultades y los distintos años estudiantiles.

Antes de iniciar la investigación, los sujetos serán advertidos por medio de un consentimiento informado de los objetivos e implicaciones de la participación en la misma. Cada sujeto firmará un compromiso indicando que se someten de forma voluntaria sin esperar retribución alguna, y que el equipo investigador no se hace responsable por daños que no estén al alcance de la investigación. Asimismo, el equipo investigador se compromete a mantener confidencial el perfil de los sujetos, a mantener controladas las vulnerabilidades a las que serán sometidos, ser transparentes en el proceso, y respetar la privacidad e información de los participantes. No se recolectará ningún tipo de información personal privada que no haya sido concedida por el participante.

La presente investigación consistió en dos fases:

6.3.1. Fase 1

Datos generales

Seguridad de la información

- ¿Tienes conocimiento sobre las medidas de seguridad que debes de implementar para proteger la información que tienen tus dispositivos (laptop, teléfono, computadora, entre otros) de ciberdelincuentes o ataques?

  La primera pregunta tenía como respuestas posibles, Sí o No.

- ¿Cuánto tiempo esperas para actualizar tus aplicaciones, softwares, navegadores, tecnologías instaladas en tu dispositivo? Entiéndase dispositivos como computadora, teléfono, tablet, ipad, entre otros.

  La segunda pregunta contenía las respuestas posibles tal que los encuestados tuvieran un mejor acercamiento respecto a cómo y cuándo actualizan sus aplicaciones de dispositivos:

  - Inmediatamente al salir la actualización.
  - Espero que haya revisiones de estas actualizaciones para hacerla.

- Mi dispositivo cuenta con la configuración de que se actualice automáticamente.
- Cuando vuelvo a utilizarlas me doy cuenta de las actualizaciones.
- Nunca.

- ¿Cada cuánto tiempo cambias tus contraseñas?

  La tercera pregunta contenía como posibles respuestas rango de tiempos en lo que la persona cambia su contraseña:

  - Entre 3 a 6 meses.
  - Cada año.
  - Cuando la plataforma me lo pida.
  - Nunca.

- Normalmente a la hora de crear una cuenta en algún sitio el cual no admita iniciar con Google o similar. ¿Qué es lo primero que se te viene a la mente para crear tu contraseña?

  La cuarta pregunta al ser de escoger muchas opciones, estas contenían los siguientes métodos de creación de contraseñas, además de una opción que permitía que ellos fueran libres de escoger su propio método:

  - Nombres y personajes de series.
  - Mi nombre y fecha de nacimiento.
  - El nombre de mi mascota.
  - Nombre de mi “celebrity crush”.
  - Palabras que uso en mi día a día.
  - Palabras largas con alteraciones.
  - Busco en internet ejemplos de contraseñas.
  - Recurrir a software que me genere una contraseña segura.
  - Otro

- ¿Te conectas a las redes de lugares que tienen WIFI abierto? (ejemplo: restaurantes, food courts, cafeterías, entre otras)

  La quinta pregunta era una pregunta de Sí o No, orientada a saber si las personas son conscientes de las consecuencias de conectarse a redes WIFI abiertas.

- ¿Cuentas con alguna medida de protección en tu dispositivo?

  La sexta pregunta contaba con las siguientes opciones de seguridad para dispositivos, las cuales se podían escoger varias o una opción para responder según su criterio y libre expresión:

  - Antivirus.
  - Ningún dato personal como credenciales y contraseñas en la computadora.
  - Ninguna medida de seguridad.
  - Gestor de contraseñas.
  - Two Factor Authentication
  - Otro.

El motivo principal de las preguntas es diseñar y realizar una prueba que sea la más provechosa y significativa para los interesados al final del megaproyecto, por lo tanto, con base en esas preguntas y resultado de cada una de ellas se puede obtenerse ciertos indicios de donde los

estudiantes pueden caer más fácilmente por lo que someterlos a esta prueba en específico puede dar mejores resultados con respecto a los estímulos que el cerebro recibirá.

La primera pregunta es para evaluar al encuestado y su conocimiento general con respecto a la seguridad en sistemas de información. Tomando los resultados de esta pregunta con una muestra representativa de los estudiantes de la UVG, puede llegar a generalizarse el conocimiento con respecto a este tema y puede fortalecerse de varias maneras por parte de la universidad o mediante el interés propio de los estudiantes de estar lo más seguros con respecto a su información que es vital para cualquier ciberdelincuente.

La segunda pregunta es necesaria porque que los ciberdelincuentes utilizan exploits, bugs, errores que existen en las versiones de las aplicaciones, softwares, navegadores, tecnologías. Es necesario tener en cuenta y dar conciencia de lo que las versiones viejas de estos productos pueden prestarse para realizar ataques de una manera muy sencilla y de cero complejidades para la recabación de datos importantes para la víctima y que de igual forma pueden perjudicar gravemente. La necesidad de las empresas de publicar y postear nuevas versiones de estas herramientas es el arreglar bugs, errores, exploits de los cuales ellos tienen el conocimiento de su existencia, pero que por sacar su producto a la venta antes de la competencia, resultan en versiones no terminadas. Lo importante aquí, es que las actualizaciones que estas herramientas reciben con el tiempo no resuelven todos los errores, bugs y exploits que tienen anteriormente, pues con la mayoría de estas sólo se "intentan" reducir estos y en la mayoría de los casos llegan a surgir más de estos lo que ocasiona que los productos siempre tengan maneras de vulnerar y perjudicar a los usuarios.

La tercera pregunta es para saber la importancia que las personas le dan a tener una contraseña en los diferentes dispositivos, software, aplicaciones y tecnologías debido a que las recomendaciones de varios expertos informáticos es que el cambio de esta sea entre tres a seis meses. Esto se debe a que muchas de las empresas son propensas a tener ataques frecuentemente para obtener datos de sus clientes o que tienen accidentalmente fugas de datos los cuales vulneran toda la información de las víctimas, en este caso los estudiantes. Muchas plataformas que utilizan los estudiantes, tras los años han tenido fuga de datos como Canva, una plataforma para realizar varios diseños de presentaciones, pancartas, videos y varios elementos de publicidad, en 2019 o ataques informáticos como el que tuvo Deezer, una aplicación que se utiliza para escuchar música y podcasts, que dejó millones de datos públicos los cuales varios atacantes seguramente aprovecharon para obtener más de ellos. El problema acá no es la obtención de datos por problemas de terceros sino lo que se puede hacer con ellos, pues resulta que a muchas personas se les hace difícil recordar varias contraseñas o no tienen buenas prácticas de almacenamiento como en gestores de contraseñas o el anotarlas en agendas de contraseñas las cuales se mantienen escondidas o con el mismo individuo esto ocasiona que se utilice la misma contraseña en varios sitios, lo que permite que con una sola fuga de datos en alguna de las empresas, los atacantes tengan acceso a varias de las herramientas a las cuales estamos vinculados mediante correo y contraseña por la utilización de la misma.

El motivo de la cuarta pregunta es que el grado de dificultad que la contraseña tenga con base en la combinación de caracteres especiales, mayúsculas, minúsculas, números, cantidad de caracteres y si tienen relación con algo cotidiano o que a la víctima le gusta va a distinguir y diferenciar una contraseña de una mala. Es por eso que esta pregunta busca ver que, tanto los estudiantes implementan buenas prácticas, en este caso el uso de palabras clave como el nombre de su mascota, celebrity crush, fecha de nacimiento, personajes de series, palabras de mi día a día, entre otras. Preguntar sobre cómo los estudiantes arman sus contraseñas actuales, nos puede dar un indicio de si ponen en prácticas las mejores metodologías y formas para la creación de contraseñas

buenas o si éstas se consideran malas con respecto a los estándares que existen según los expertos en informática. Tener una buena contraseña consigue, en la mayoría de los casos, que los atacantes prefieran a una víctima “más sencilla” y que por descarte se decidan ir por un camino más fácil que seguramente le consiga lo mismo que es información importante y personal para el estudiante.

La penúltima pregunta es necesaria para saber qué personas son más propensas a ser atacadas en lugares públicos que compartan internet para todos sus clientes como es el caso de restaurantes, cafeterías, food courts. Esto se debe a que los lugares que comparten internet de forma gratuita pueden ser lugares atractivos para los atacantes cibernéticos debido a que con simples pasos como detectar el tráfico de red pueden llegar a adquirir credenciales, como usuarios, correos electrónicos y contraseñas además del sitio al cual permiten el acceso. Tomar las precauciones debidas puede ahorrar bastantes problemas con respecto a perder credenciales de una manera tan fácil y despistada como lo es conectarse a redes no ajenas.

La última pregunta está orientada a saber si los estudiantes toman en cuenta e implementan alguna medida de seguridad para sus dispositivos que contienen información importante y personal. El saber esto ayudará a identificar cuáles serían los ataques que pueden ser más propensos a caer debido a que tienen cierta medida de seguridad y no otras, incluso si no tienen ninguna puede dar a entender que al estudiante no le importa mucho su seguridad con respecto a ataques.

Análisis de sesgos

Consiste en implementar una encuesta con casos de los sesgos más relevantes en la población. Cada respuesta para cada uno de los casos dados establece en una escala numérica qué tan susceptible es el individuo a ser víctima del sesgo en cuestión, donde mientras menor será el número (1) menor será la probabilidad de que el individuo sea susceptible a ser víctima del sesgo en cuestión, y mientras más grande sea el número, implica mayor probabilidad de ser sesgado.

El objetivo de esta fase comprender de forma abstracta la toma de decisiones de los estudiantes en situaciones comunes en las que puedan verse afectados por un sesgo.

Cada sujeto tendrá acceso a un formulario de Google Forms con las preguntas para ser respondidas en el tiempo que consideren necesario de forma anónima.

En el formulario, los participantes recibieron las siguientes instrucciones: A continuación, se le presentarán 5 escenarios de situaciones cotidianas. Por favor, responda con honestidad la opción que más se acerque a lo que usted haría en respuesta al escenario propuesto. Base sus respuestas en experiencias pasadas, por si ha experimentado alguna situación similar, de lo contrario seleccione la que más se adecúe a su forma de actuar. Es probable que usted no se identifique con ninguna de las respuestas, en ese caso seleccione la respuesta hipotéticamente más probable".

Los casos evaluados fueron los siguientes:

Caso de sesgo de confirmación

Enunciado: Lees por redes sociales un post o comentario que se alinea con tus creencias acerca de un tema muy controversial. ¿Qué haces?

A. Le das tu aprobación al post (por medio de un like, repost, o mentalmente).

B. Investigas más acerca del autor y otras perspectivas antes de formar tu opinión.
C. Analizas más el post y descartas cualquier información contradictoria como poco confiable o sesgada.

Puntuación:

A. 3 puntos. En este caso el individuo le da aprobación ciegamente al evento por el mero hecho de compartir el mismo punto de vista.

B. 1 punto. El hecho que el evento refleje los intereses o perspectivas del individuo no implica que el individuo se apegue al criterio del mismo.

C. 2 puntos. Esta situación demuestra que el individuo tiene cierta tendencia a verse influenciado por la semejanza de ideas, sin embargo, aún hace un esfuerzo por encontrar otras perspectivas.

Caso de sesgo de optimismo

Enunciado: Te enteras por redes sociales que a algunos usuarios del banco en el que tienes tu cuenta principal, les han robado sus credenciales de su banca en línea, ¿qué piensas?

A. No fue a ti así que sigues con tu vida.

B. Inmediatamente cambias la contraseña de tu banca en línea.

C. Esperas que el banco mejore sus medidas de seguridad.

Puntuación:

A. 3 puntos. El individuo tiene seguridad en que es poco o nada probable que haya sido víctima del evento negativo.

B. 1 punto. El individuo es consciente de que el riesgo le afecta y, por lo tanto, toma acción para mitigarlo.

C. 2 puntos. En este caso el individuo tiene presente que el riego puede afectarle, pero no lo suficiente como para tener la motivación de mitigar el riesgo.

Caso de sesgo de anclaje

Enunciado: Te ofrecen un trabajo en un campo laboral del que no tienes ni idea de cuánto cobrar, pero es el trabajo que querías así que le consultas a un amigo que labora en un puesto muy similar y con un perfil que se parece mucho al tuyo, y te dice que gana Q17,000. Luego recibes una llamada del reclutador y te ofrece un salario de Q9,000, haciendo énfasis en que es un salario competitivo para tu perfil. ¿Qué decides?

A. Aceptas la propuesta salarial.

B. Te parece mala paga y negocias un salario similar al de tu amigo.

C. Eres escéptico de ambas respuestas así que investigas más el mercado laboral para descubrir qué salario se adecúa a tu perfil.

Puntuación:

A. 1 punto. El evento/conocimiento pasado no influyó en la decisión del individuo, es decir, no lo ancló en la toma de su decisión y es libre de aceptar la nueva información como verdadera.

B. 3 puntos. En esta situación el individuo rechaza la nueva información al estar anclado a la información pasada, señalizando que está anclado a dicha información.

C. 2 puntos. Existe un anclaje presente en la decisión del individuo, mas no es lo suficientemente fuerte como para rechazar por completo la nueva información recibida.

Caso de sesgo de Dunning-Kruger

Enunciado: ¿Con cuál de las siguientes te identificas más?

A. Sé cómo mantenerme seguro en internet, y el riesgo a que me hackeen es bajo.

B. No sé cómo mantenerme seguro en internet, pero el riesgo a que me hakeen es bajo.

C. Sé cómo mantenerme seguro en internet, aunque el riesgo a que me hakeen es alto.

D. No sé cómo mantenerme seguro en internet y el riesgo a que me hakeen es alto.

Puntuación:

A. 3 puntos. En este escenario el individuo sobrestima sus habilidades en seguridad, y subestima el riesgo de las amenazas cibernéticas.

B. 2 puntos. El individuo no sobrestima sus habilidades para mantenerse seguro, pero aún subestima el riesgo.

C. 2 puntos. El individuo no subestima el riesgo, pero sí sobrestima sus habilidades.

D. 1 punto. Aquí el individuo es consciente del riesgo y no sobrestima su capacidad de mantenerse seguro.

Caso de sesgo de autoridad

Enunciado: Recibes un mensaje de tu papá, mamá o tutor legal indicando urgencia en que le envíes una foto de tu DPI (Documento Personal de Información) y otros documentos personales para finalizar un trámite.

A. Se la envías inmediatamente.

B. Lo llamas directamente para saber más al respecto antes de tomar cualquier acción.

C. Revisas por tu cuenta que el emisor efectivamente sea la persona quien dice ser y se la envías.

Puntuación:

A. 3 puntos. El individuo le atribuye completa veracidad a la situación por la figura de autoridad involucrada.

B. 1 punto. El hecho de que sea una figura de autoridad la que solicita la información, no influye en la decisión del individuo.

C. 2 puntos. Hay cierta influencia de la autoridad en la decisión del individuo por lo que su esfuerzo en verificar la identidad del emisor no es muy grande.

Cabe destacar que las respuestas a los enunciados no fueron colocadas en ningún orden en particular, esto para evitar sesgar la respuesta de los estudiantes al identificar un patrón en el orden de respuesta para procurar obtener la respuesta "adecuada" o "correcta".

Estos casos buscan apegarse lo más posible a situaciones cotidianas de la población que podrían llegar a materializarse en la realidad, ya sea con o sin fines negativos sobre el individuo. Sin embargo, se procuró evitar escenarios "cliché" que pudieran llegar a sesgar la respuesta del participante. Por ejemplo, un caso más concreto del sesgo de autoridad sería la de un banco solicitando datos privados de la tarjeta de crédito de la víctima, no obstante, este es un escenario que suele ser de conocimiento común entre los estudiantes debido al gran esfuerzo de los bancos en comunicar estos casos, por lo que los participantes sabrían cómo actuar correctamente porque ya se les ha indicado como actuar en esa situación en particular y no porque no sean susceptibles a este tipo de sesgos. Además, es importante recordar que un ataque de ingeniería social (efectivo) implica una investigación profunda de la víctima, por lo que un sólo sesgo puede ser explotado en una gran variedad de posibles ataques, y cada ataque puede ser más o menos efectivo dependiendo de la personalidad, conocimientos, sentimientos y conducta de la víctima, y esta es la razón por la que este estudio se dividió en dos fases, para separar el análisis de los sesgos que representan una visión más focalizada en los procesos cognitivos que guían las decisiones del individuo, de los ataques que explotan esos sesgos que nos dan a entender la forma en que el individuo percibe los estímulos.

Psicometría

1. "Estás en un sitio web de compras en línea y notas que la interfaz se ve ligeramente diferente, pero aun así te pide iniciar sesión. ¿Cómo responderías?"

    a) No proporcionaría mis credenciales y cerraría la ventana.

    b) Ingresaría mis credenciales sin pensar demasiado, ya que podría ser una nueva actualización.

    c) Compararía cuidadosamente la URL con la del sitio web oficial antes de tomar alguna acción.

2. "Estás en una aplicación web donde hay muchos anuncios, pop-ups, que al ser presionado te abren nuevas pestañas y no te dejan interactuar con la página. ¿Qué harías para mejorar tu experiencia en sitios similares?"

    a) Cierro cuidadosamente los pop-ups, aunque abran nuevas pestañas.

    b) Tengo configurado que en mi navegador no abrir ventanas emergentes sin mi autorización.

    c) Utilizo un add-blocker.

    d) Cierro la página.

3. "Estás por ingresar a tu banca en línea a través del navegador y notas que hay algo raro en ella. ¿En qué elementos te fijas primero para corroborar que estás en el lugar correcto?"

a) Los botones

b) Los campos del formulario

c) Las barras de navegación

d) Colores/Tema

e) Otros elementos visuales (multimedia,fonts)

4. “Tu catedrático les manda un link para descargar un material que será necesario para la clase, al ingresar el link y llenar un formulario te aparecen los siguientes botones para descargar el material. ¿Qué botón presionamos primero?”

a) Opción 1

b) Opción 2

c) Opción 3

d) Opción 4

e) Ninguno

Figura 6.1: Opciones pregunta 4, encuesta

Redes

1. “¿Visitas constantemente páginas web que ofrecen contenido audiovisual de paga de manera gratuita? Como Cuevana”.

a) Sí
b) No

2. "¿Te conectas a menudo al Internet que los restaurantes u otros lugares públicos ofrecen?"
   a) No
   b) Pocas veces
   c) A menudo
3. "¿Te preocupan los riesgos de seguridad al usar redes Wi-Fi públicas?"
   a) Sí
   b) No
   c) Algunas veces
4. "¿Haces una búsqueda de amenazas a los archivos que descargas?"
   a) Sí
   b) No
5. "¿Sabes qué es la huella digital?"
   a) Sí
   b) No

La primera pregunta tiene la finalidad de mostrar el porcentaje de estudiantes que visitan páginas que comparten contenido de paga de manera gratuita. Estas páginas al no tener una manera de pago directo por parte del consumidor para mantener sus operaciones y servidores, estos muestran anuncios invasivos que aparecen en cantidades considerables para ser molestos para el usuario cayendo así en un ataque de phishing. Por su puesto, algunos ignoran estos y siguen usando el servicio, pero cuando alguien intenta cerrarlos este puede abrir otras pestañas del navegador sin permiso alguno e incluso pueden descargar contenido igual sin ningún tipo de permiso (en su gran mayoría virus tipo malware) [Gormally, 2019].

La segunda pregunta tiene la finalidad de mostrar qué tan a menudo se conectan a redes públicas que la mayoría de los locales ofrecen. Esto es porque existen diferentes maneras en las cuales un tercero puede extraer información del tráfico de la red sin consentimiento. Incluso algunos lugares pueden "ofrecer" internet gratuito, pero en realidad el punto de conexión fue creado por alguien externo y que no está relacionado al lugar y los llevaría a ser víctima de un ataque de Man-in-the-Middle.

La tercera pregunta está conectada a la anterior, en la cual se quiere saber si el estudiante a pesar de conocer los riesgos de conectarse a redes públicas aun así lo hace o simplemente omite esto y continúa navegando, siendo influenciado más por los sesgos cognitivos.

La cuarta pregunta tiene la finalidad de saber si los estudiantes analizan los documentos/archivos antes de abrirlos/ejecutarlos. Esto se debe a que algunos descargables traen contenido malicioso que con sólo abrir un documento o correr un ejecutable, esto abre la posibilidad de que un virus infecte el sistema sin que el usuario se percate y llegue a ser víctima de un ataque de Rasomware.

La quinta pregunta está relacionada a si los estudiantes saben diferenciar la huella digital y la huella dactilar, dado a que muchos usuarios confunden estos dos términos. Sin embargo, son completamente diferentes. Es importante que los estudiantes tengan presente que cada página que visitan, cada tarea y acción que realizan en Internet aporta a sus huellas digitales.

Fase 2: Análisis de los ataques informáticos

Una vez analizada la información recopilada en la fase 1, los sujetos fueron sometidos a una simulación de los ataques más relevantes para la población forma controlada.

Bajo este contexto, una amenaza "controlada" implica que se ejecutó el ataque al participante sin afectar positiva o negativamente al mismo o a su integridad, sin obtener nada que no sean los hallazgos indispensables para cumplir los objetivos de la investigación, respetando en todo momento la privacidad del participante y que el participante fue informado (al finalizar las pruebas para evitar el sesgo) con total transparencia del flujo del ataque y qué ocurrió en cada etapa de la prueba.

Se puede describir el proceso de la ejecución de los ataques de la siguiente forma: al realizar los ataques, se utilizaron pruebas heurísticas, psicométricas y un eye tracker para medir la actividad visual y comprender la percepción del participante a estímulos determinados al ser atacado. Los datos fueron interpretados extrapolando los componentes clave que más motivaron la decisión del individuo a caer en el ataque.

A continuación, se describe cada uno de los ataques simulados haciendo uso del eye tracker. Cada ataque es simulado por medio de una diapositiva que despliega el software durante un tiempo limitado mientras registra las miradas, fijaciones y clics del usuario.

Nota: las áreas amarillas en cada una de las diapositivas usadas en el eye tracker representan cada AOI.

Open Wi-Fi

Consistió en simular que el participante seleccionaba una red en su dispositivo, incluyendo redes abiertas. Cabe destacar que ninguna de las redes incluidas en la diapositiva existe genuinamente en los alrededores del campus de la universidad, de forma que conectarse a cualquiera de las redes con esos nombres sería un riego en la vida real.

Enunciado: Se te mostrará una lista de redes wifi a las cuales te puedes conectar en la UVG.

Duración de la diapositiva: 7 segundos.

Diapositiva:

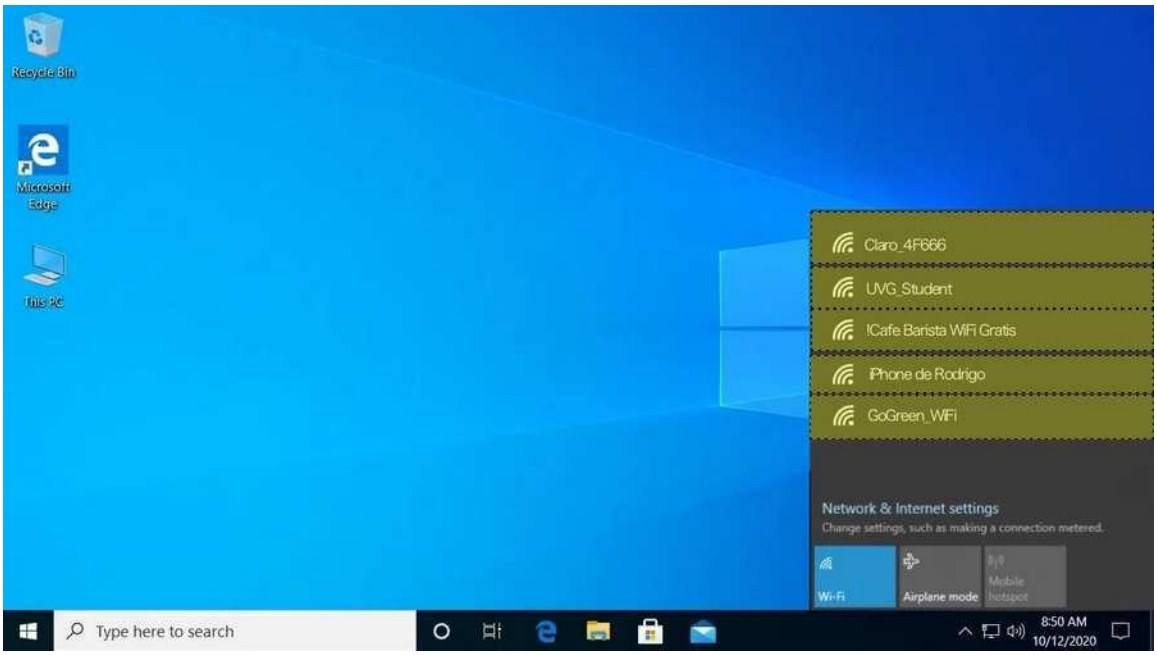


Figura 6.2: AOI's del ataque de open Wi-Fi

Preguntas realizadas al finalizar la diapositiva:

1. ¿Cuáles crees que serían las opciones más seguras?
   - Claro_4F666
   - UVG Student
   - !Café Barista WiFi Gratis
   - iPhone de Rodrigo
   - GoGreen_WiFi
   - Ninguna
2. Justifique su elección - (entrada de texto libre)
3. ¿Qué importancia le da a cada criterio para conectarse a la red? - (escala del 1 al 5)
   - Nombre
   - Señal
   - El orden en que aparecen
   - Conexiones previas
4. ¿Usualmente se conecta a redes abiertas?
   - Siempre
   - Nunca
   - De vez en cuando
   - Sólo si es emergencia
   - Sólo si no hay otra red disponible
   - Sí se conecta automáticamente

Password leak

Se simuló el login a una plataforma de dudosa confiabilidad.

Enunciado: A continuación, suponga que usted se está registrando en un sitio web.

Duración de la diapositiva: 7 segundos.

Diapositiva:

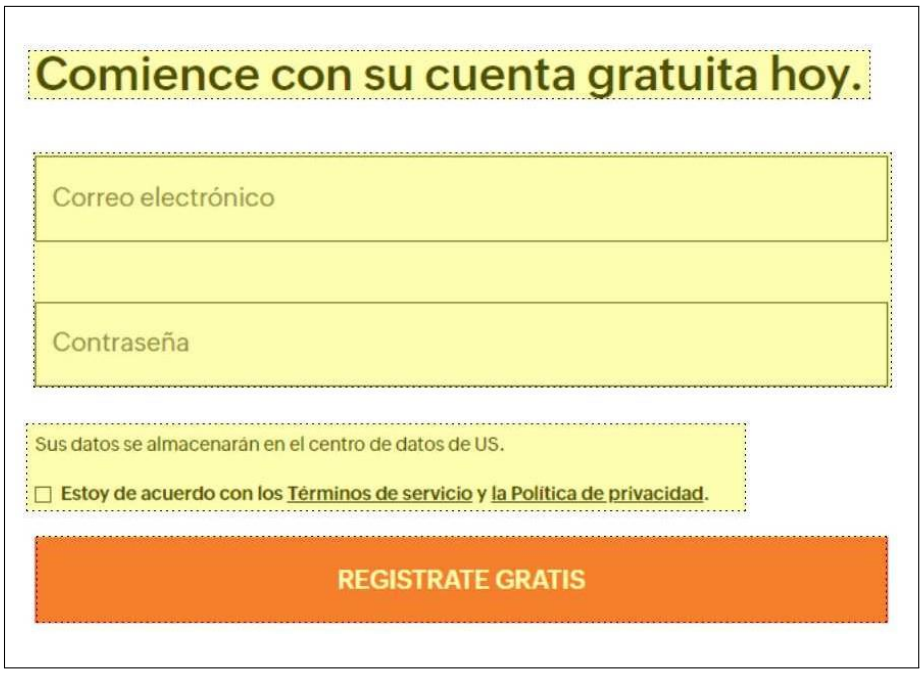


Figura 6.3: AOI's del ataque de password leak

Preguntas realizadas al finalizar la diapositiva:

1. Escriba una contraseña que considere segura (no escriba credenciales reales o en uso) - (entrada de texto libre)
2. ¿Tu contraseña contiene alguno de estos elementos?
   - Fecha(s) importante(s)
   - Tu nombre o de algún conocido
   - Nombre de mascotas
   - Secuencia de números
   - "password"
   - Algúna cosa o actividad que te guste (personajes, celebrity crush, etc)
3. ¿Cómo recuerdas tus contraseñas?
   - Siempre
   - Nunca

- De vez en cuando
- Sólo si es emergencia
- Sólo si no hay otra red disponible
- Si se conecta automáticamente

4. ¿Cree que sus contraseñas son lo suficientemente seguras como para no ser descubiertas?
   - Sí
   - No
5. ¿Qué importancia cree que tiene la seguridad de la contraseña para proteger sus cuentas y datos en línea? - (escala del 1 al 5)

Phishing

Este ataque se dividió en dos partes: la primera es la perspectiva de la bandeja de entrada, y la segunda la perspectiva del contenido del correo. Dentro de la bandeja de entrada hay un correo de phishing y un correo de una campaña de seguridad legítima.

Enunciado parte 1: A continuación, se le mostrará una captura de una bandeja de entrada de gmail. Suponga que esta es la bandeja de entrada de su correo institucional. Revise los correos que le han llegado Y HAGA CLIC en los correos que le interesaría abrir para leer. Al hacer clic no verá ninguna acción, así que puede hacer clic en todos los correos que quiera.

Duración de la diapositiva: 15 segundos.

Diapositiva:

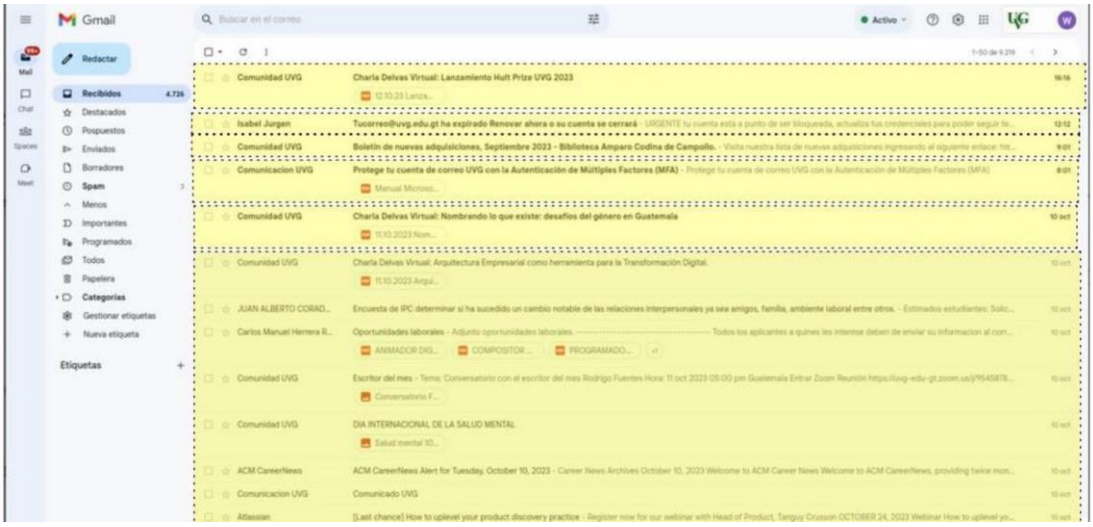


Figura 6.4: AOI's del ataque de phishing en bandeja de entrada

Preguntas realizadas al finalizar la diapositiva:

1. ¿Algún correo llamó su atención por fuera de lo normal? Explique - (entrada de texto libre)

Enunciado parte 2: De la bandeja de correo anterior, usted decide entrar al siguiente correo...

Duración de la diapositiva: 20 segundos.

Diapositiva:

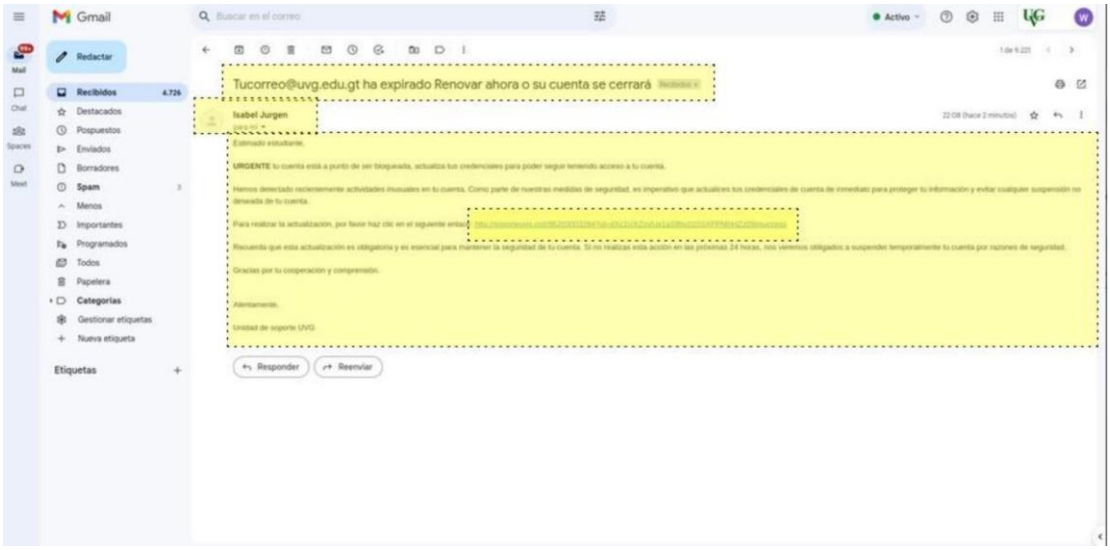


Figura 6.5: AOI's del ataque de phishing en contenido de correo

Preguntas realizadas al finalizar la diapositiva:

1. Si ese correo efectivamente le hubiera llegado a su bandeja de entrada, ¿qué pensaría al respecto?
   - Que debo seguir las instrucciones para actualizar mis credenciales
   - Que se confundieron de destinatario
   - No le daría ninguna importancia
   - Que es una estafa
2. ¿En qué se basó para decidir si el correo era de fiar o no? Elija el criterio que más le convenció.
   - El nombre/correo del emisor
   - Contenido del correo
   - No me fijé
   - El asunto
   - El correo institucional es seguro
   - No habría razón para que el correo no fuera de fiar

Bait

En este caso se simuló una conversación en una aplicación de mensajería instantánea de un

grupo de un curso. En el mismo chat un contacto desconocido comparte un link no confiable para descargar un libro gratuito.

Enunciado: Suponga que usted lleva actualmente el curso de pensamiento cuantitativo, donde se solicita tener el libro del curso para la tarea que se entrega el día de hoy y usted no tiene el libro. A continuación, verá el grupo de whatsapp de su clase.

Duración de la diapositiva: 11 segundos.

Diapositiva:

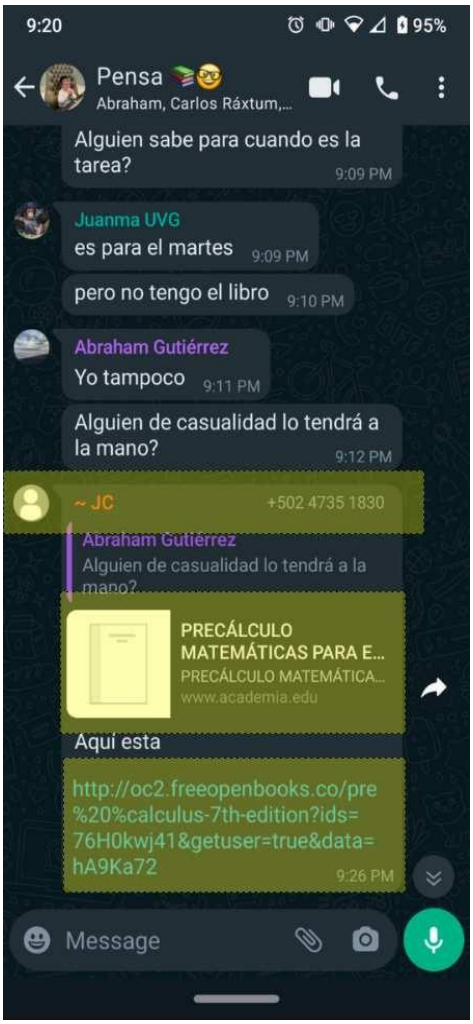


Figura 6.6: AOI's del ataque de bait

Preguntas realizadas al finalizar la diapositiva:

3. ¿Descargarías el libro que te compartieron?
   - Sí
   - No
4. Si tu respuesta anterior fue sí, justifica por qué (si no, continúa a la siguiente pregunta)

- Es un libro gratis.
- El libro es difícil de conseguir.
- Lo necesito lo antes posible para hacer la tarea.
- Porque lo compartieron en el grupo de la clase, es de confianza.
- El preview del archivo me muestra que claramente es el libro que necesito.
- No hay razón en particular, sólo lo abriría.
- Otro.

5. Si su respuesta fue no, ¿por qué no lo abriría? (si su respuesta fue si deje en blanco esta pregunta)

    - La piratería es mala.
    - El link no se veía confiable.
    - No conozco al que lo envío.
    - Sólo no lo haría.
    - Otro.

Métricas del eye tracker

El eye tracker retorna las siguientes métricas por cada AOI:

- Avg. TTFF (Average Time To First Fixation): Tiempo promedio para la primer fijación.
- Fixations Avg. Time Spent: Tiempo promedio dedicado en una fijación.
- Fixations: Fijaciones.
- Fixations Ratio: Proporción de fijaciones.
- Avg. Fixation Duration: Duración promedio de las fijaciones.
- Avg. FFD (Average First Fixation Duration): Tiempo promedio de la primera fijación.
- Attention: Atención.
- Avg. Revisits: Revisitas promedio.
- Clics
- Avg. TTFC (Average Time To First Clic): Tiempo promedio para el primer clic.
- AOI Size: Tamaño del AOI
- Avg. TTFG (Average Time To First Gaze): Tiempo promedio para la primer mirada
- Gazes Avg. Time Spent: Tiempo promedio dedicado en miradas.
- Gazes: Miradas.
- Gazes Ratio: Proporción de miradas.

Además, se utilizarán los heatmaps y las grabaciones del eye tracker para analizar el flujo de atención del participante.

CAPÍTULO 7

Resultados

7.1. Investigación de ataques y sesgos

	Open Wi-Fi	Phishing	Password leak	Bait
Confirmación				
Optimismo				
Anclaje				
Dunning-Kruger				
Autoridad				

Figura 7.1: Correlación entre los ataques de ingeniería social más relevantes y los sesgos más frecuentes entre dichos ataques. El color rojo marca la existencia de una relación entre las variables.

7.2. Fase 1

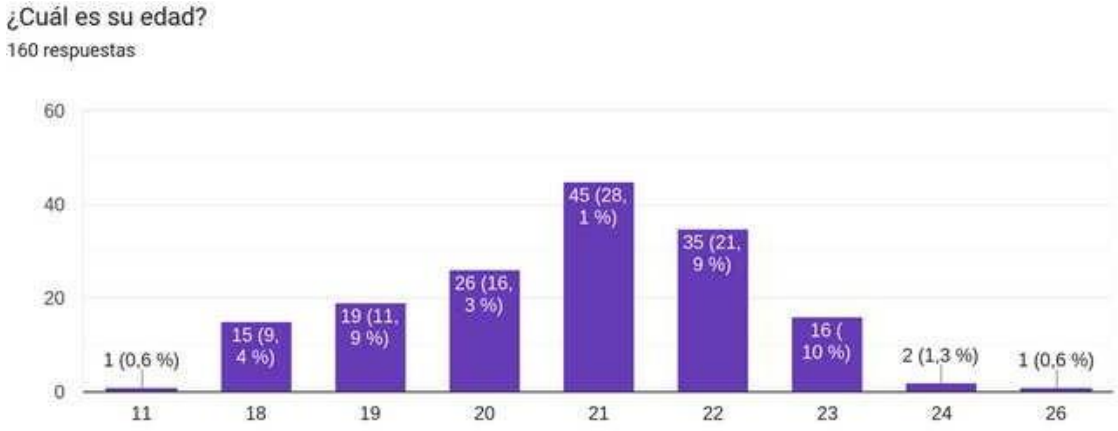


Figura 7.2: Respuestas a la pregunta: ¿Cuál es tu edad?

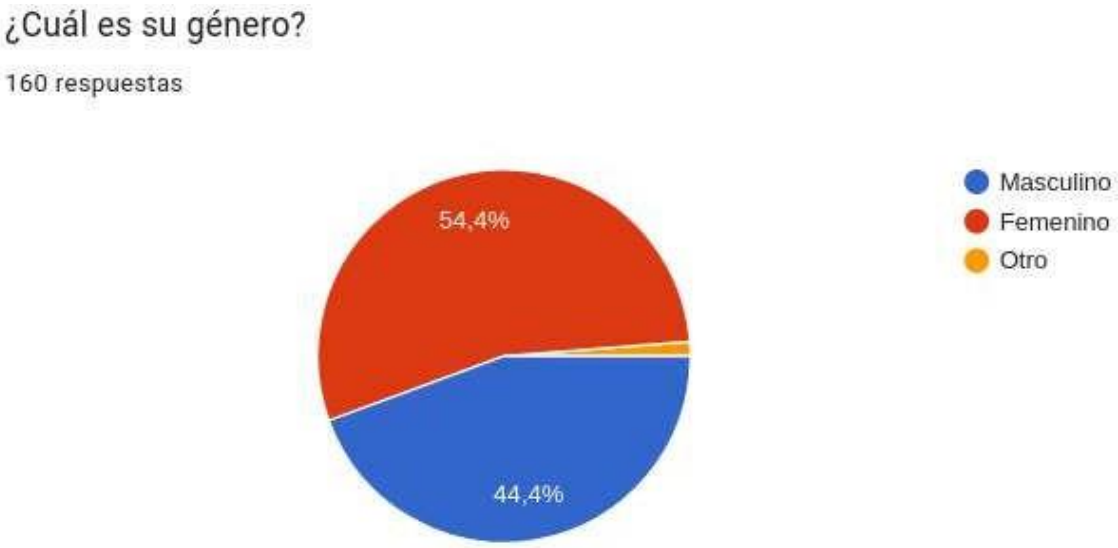


Figura 7.3: Respuestas a la pregunta: ¿Cuál es su género?

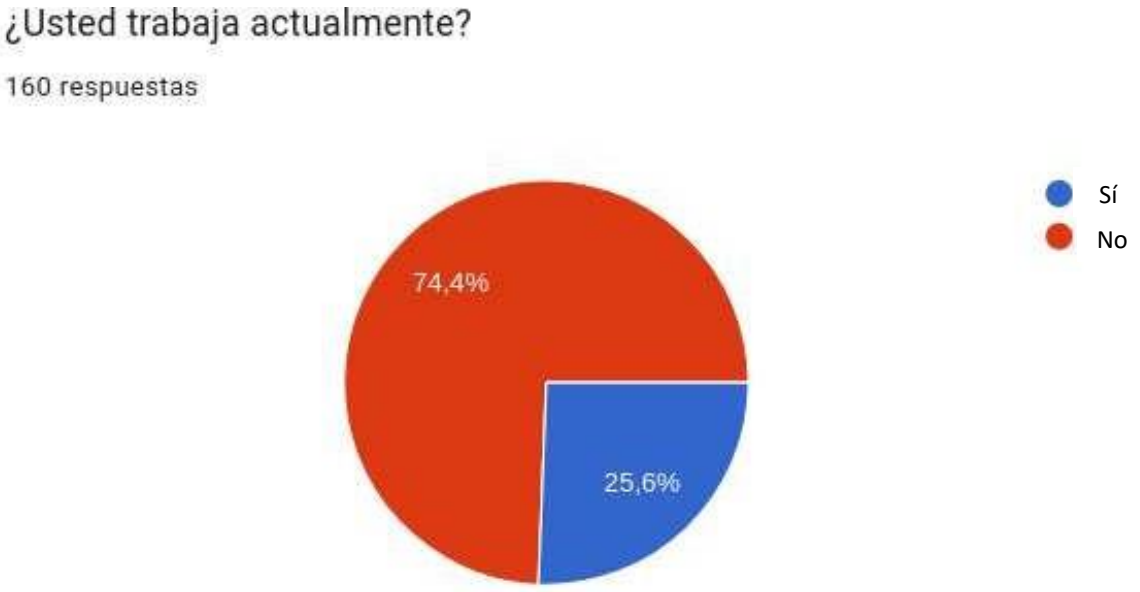


Figura 7.4: Respuestas a la pregunta: ¿Usted trabaja actualmente?

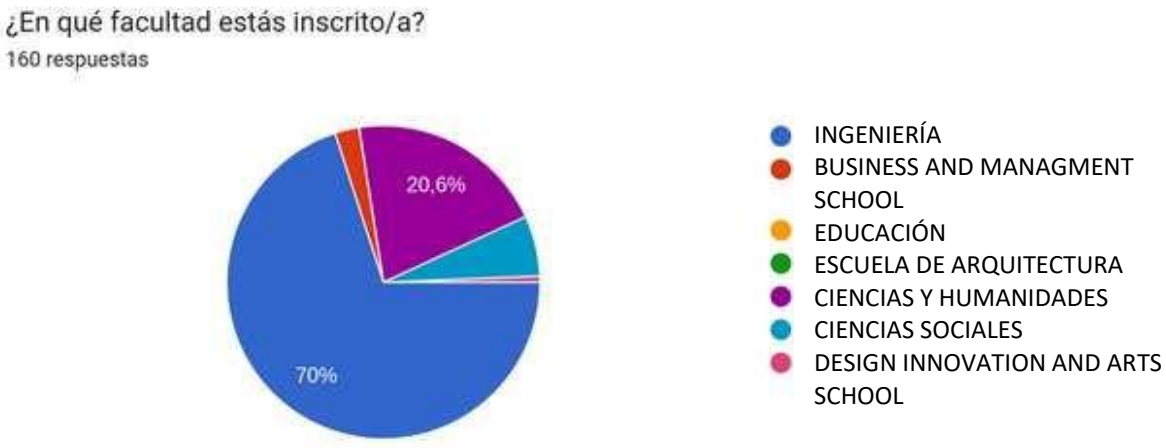


Figura 7.5: Respuestas a la pregunta: ¿Cuál es tu edad?

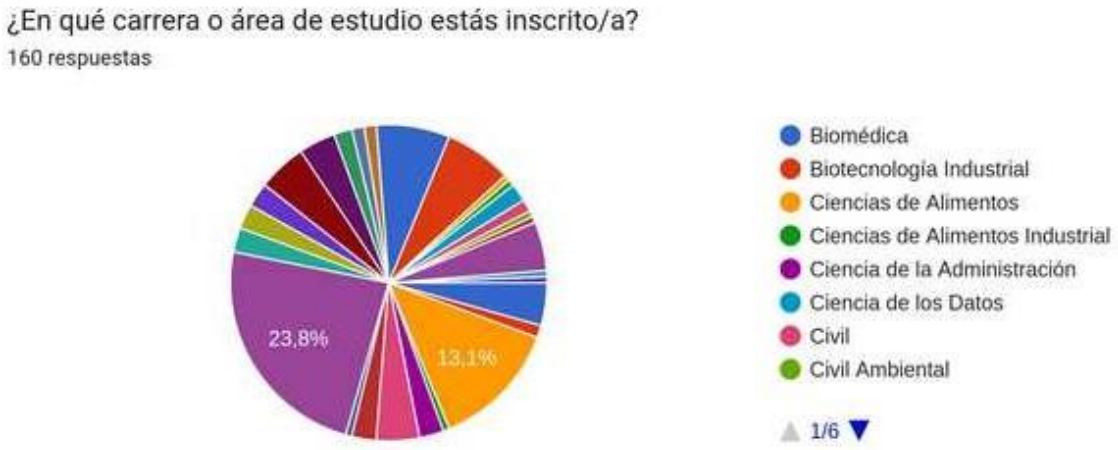


Figura 7.6: Respuestas a la pregunta: ¿En qué facultad estás inscrito/a?

Figura 7.7: Respuestas a la pregunta: ¿En qué carrera o área de estudio estás inscrito/a?

Figura 7.8: Respuestas a la pregunta: ¿En qué año te encuentras en tu programa académico?

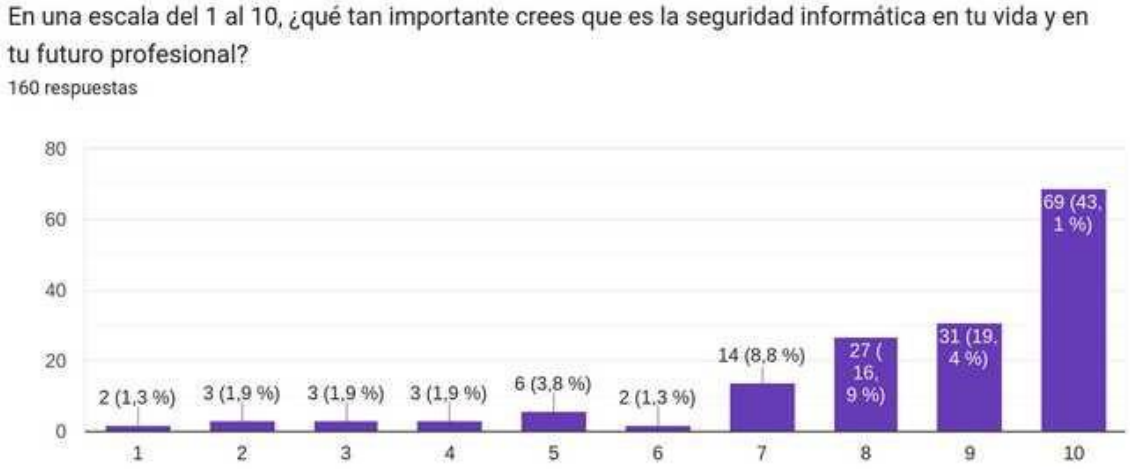


Figura 7.9: Respuestas a la pregunta: “En una escala del 1 al 10, ¿qué tan importante crees que es la seguridad informática en tu vida y en tu futuro profesional?"

¿Tienes conocimiento sobre las medidas de seguridad que debes de implementar para proteger la información que tienen tus dispositivos (laptop, teléfono, computadora, entre otros) de ciberdelincuentes o ataques?

160 respuestas

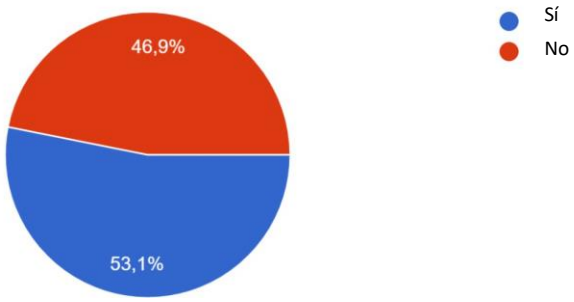


Figura 7.10: Respuestas recabadas con respecto a la pregunta 1.

¿Cuánto tiempo esperas para actualizar tus aplicaciones, softwares, navegadores, tecnologías instaladas en tu dispositivo? Entiéndase dispositivos como computadora, teléfono, tablet, ipad, entre otros.

160 respuestas

Figura 7.11: Respuestas recabadas con respecto a la pregunta 2.

Figura 7.12: Respuestas recabadas con respecto a la pregunta 3.

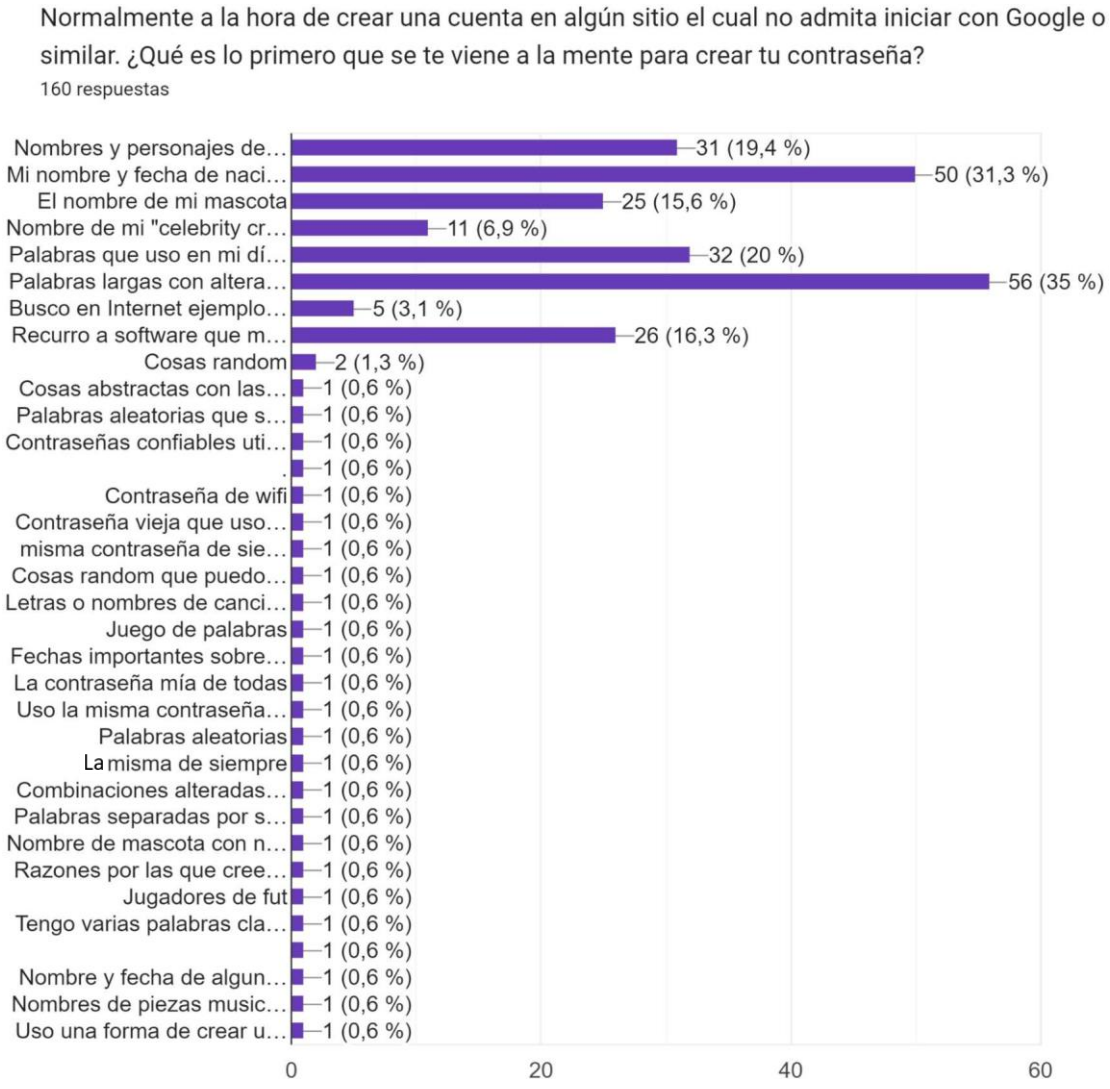


Figura 7.13: Respuestas recabadas con respecto a la pregunta 4.

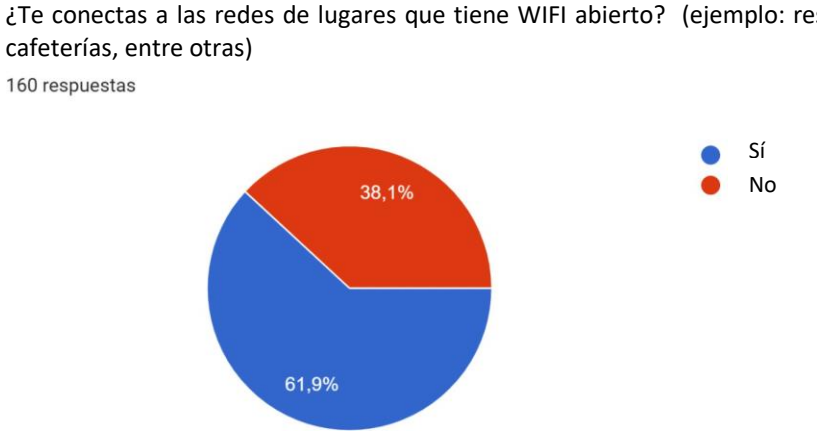


Figura 7.14: Respuestas recabadas con respecto a la pregunta 5.

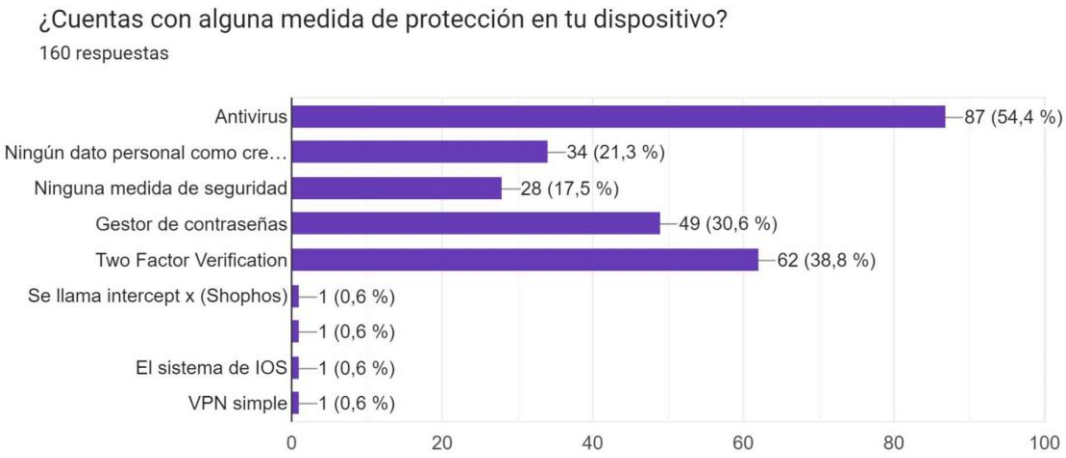


Figura 7.15: Respuestas recabadas con respecto a la pregunta 6.

Sesgo	count	mean	std	Min	25%	50%	75%	max
Confirmación	3.000	53.333	30.353	26.000	37.000	48.000	67.000	86.000
Optimismo	3.000	53.333	30.089	34.000	36.000	38.000	63.000	88.000
Anclaje	3.000	53.333	53.482	13.000	23.000	33.000	73.500	114.000
Dunning-Kruger	4.000	40.000	13.540	21.000	36.750	43.000	46.250	53.000
Autoridad	3.000	53.333	12.342	43.000	46.500	50.000	58.500	67.000

Tabla 7.1: Medidas de tendencia central de los casos de sesgos

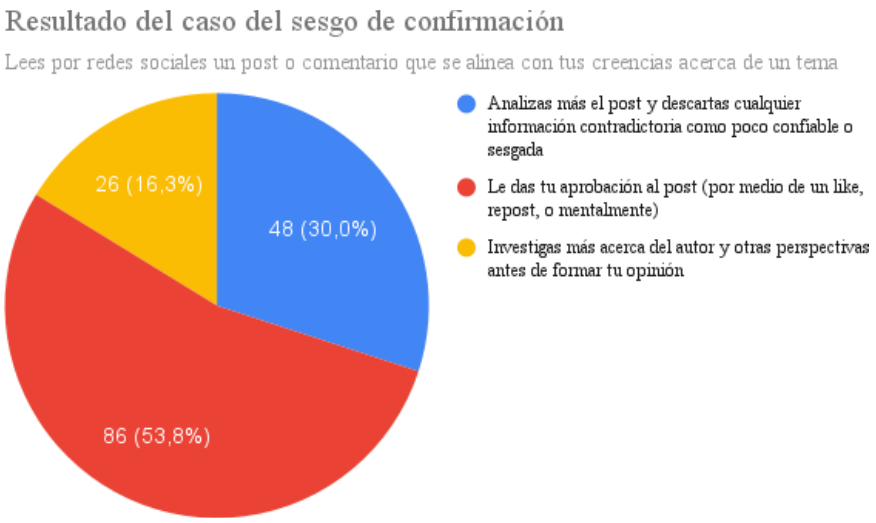


Figura 7.16: Recuento a la pregunta del sesgo de confirmación

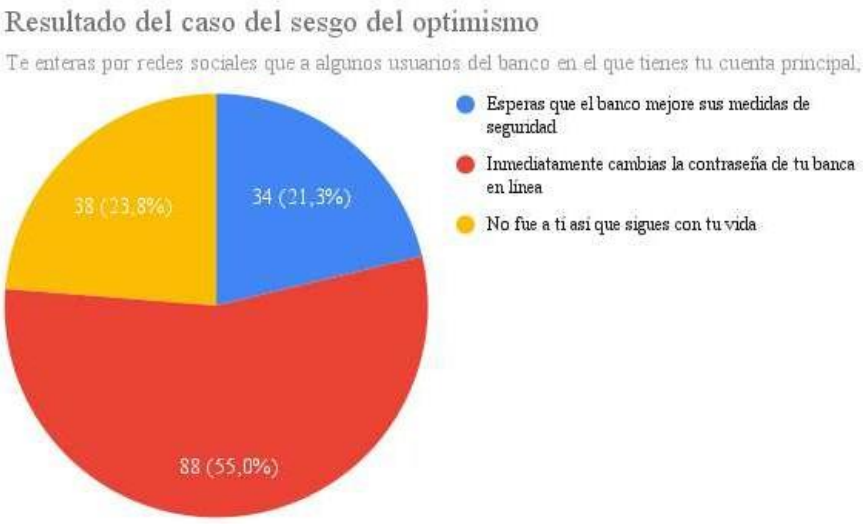


Figura 7.17: Recuento a la pregunta del sesgo del optimismo

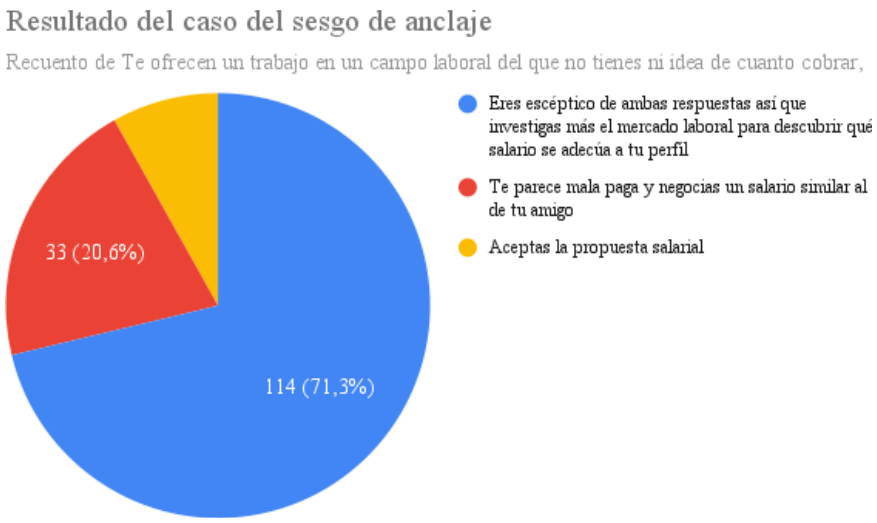


Figura 7.18: Recuento a la pregunta del sesgo de anclaje

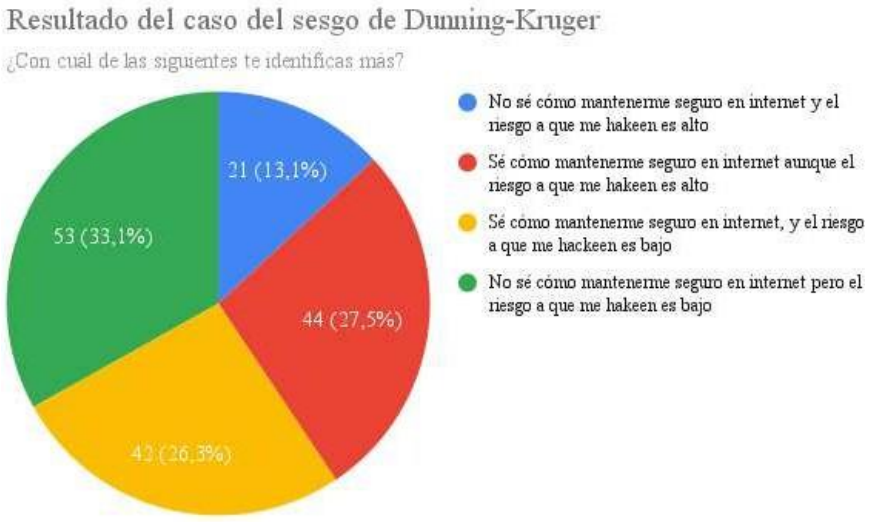


Figura 7.19: Recuento a la pregunta del sesgo de Dunning-Kruger

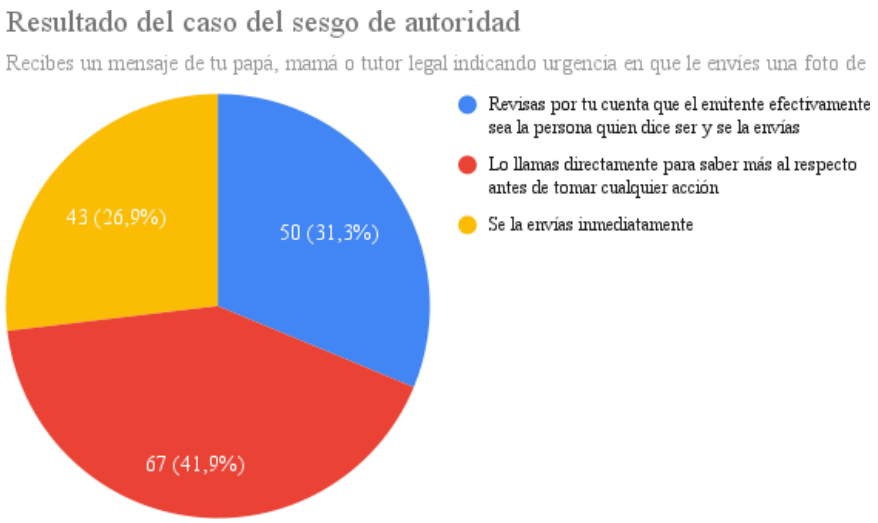


Figura 7.20: Recuento a la pregunta del sesgo de autoridad

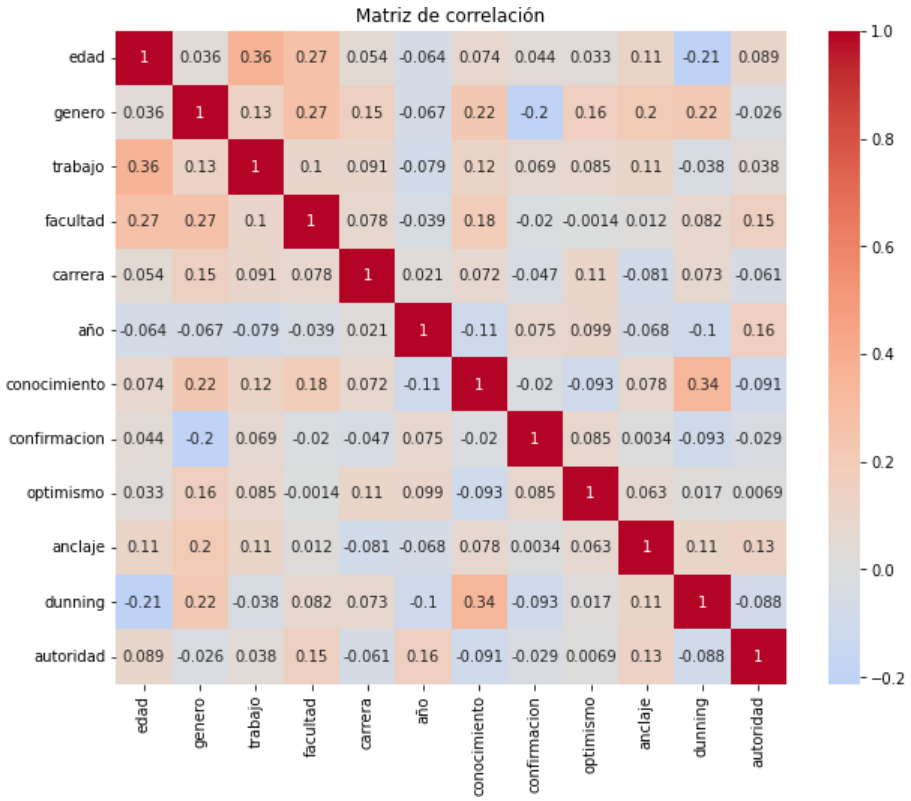


Figura 7.21: Matriz de correlación entre las variables demográficas y los casos de sesgo

Estás en un sitio web de compras en línea y notas que la interfaz se ve ligeramente diferente, pero aun así te pide iniciar sesión. ¿Cómo responderías?

160 respuestas

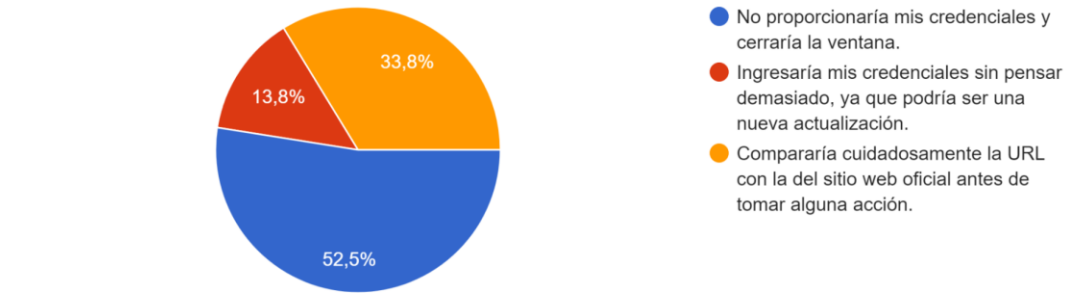


Figura 7.22: Respuestas a pregunta N.1 de UI/UX

Estás en una aplicación web donde hay muchos anuncios, pop-ups, que al ser presionado te abren nuevas pestañas y no te dejan interactuar con la página. ¿Qué harías para mejorar tu experiencia en sitios similares?

160 respuestas

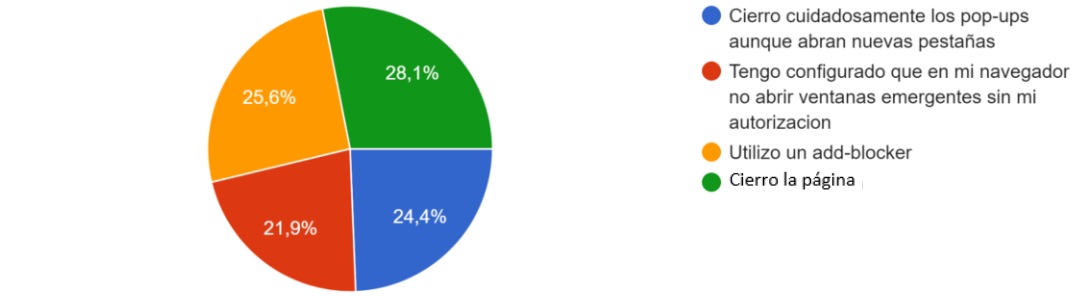


Figura 7.23: Respuestas a pregunta N.2 de UI/UX

Estás por ingresar a tu banca en línea a través del navegador y notas que hay algo raro en ella. ¿En qué elementos te fijas primero para corroborar que estás en el lugar correcto?

160 respuestas

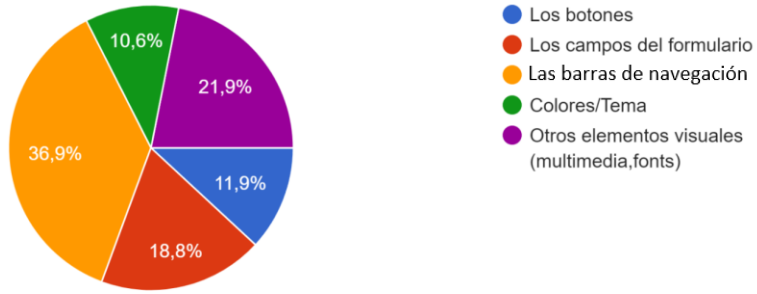


Figura 7.24: Respuestas a pregunta N.3 de UI/UX

Tu catedrático les manda un link para descargar un material que será necesario para la clase, al ingresar el link y llenar un formulario te aparecen los siguientes botones para descargar el material. ¿Qué botón presionamos primero?

160 respuestas

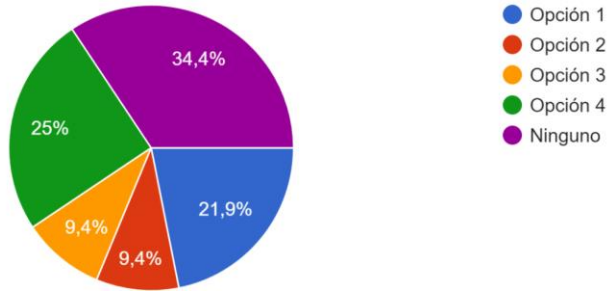


Figura 7.25: Respuestas a pregunta N.4 de UI/UX

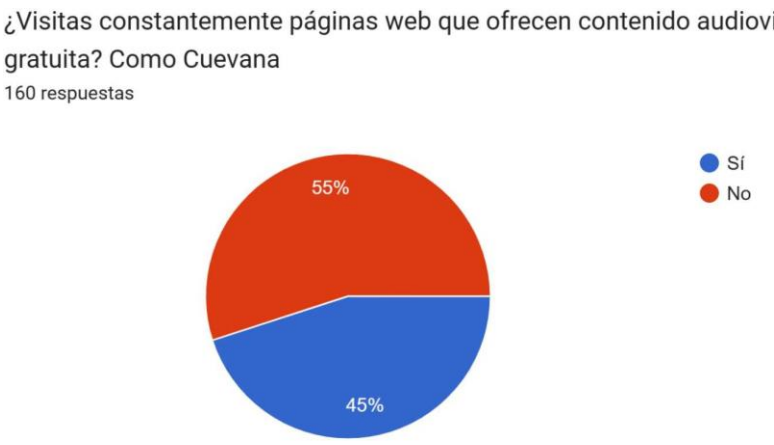


Figura 7.26: Respuestas a pregunta N.1 de tráfico de redes

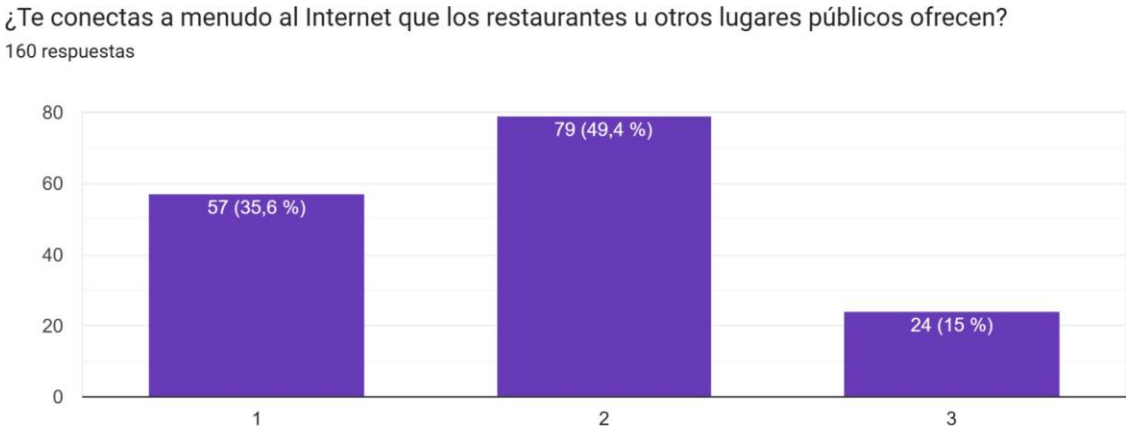


Figura 7.27: Respuestas a pregunta N.2 de tráfico de redes

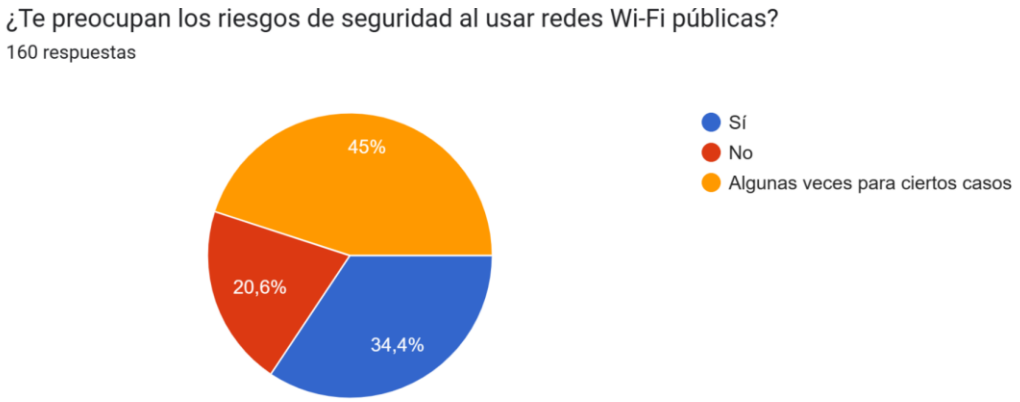


Figura 7.28: Respuestas a pregunta N.3 de tráfico de redes

Figura 7.29: Respuestas a pregunta N.4 de tráfico de redes

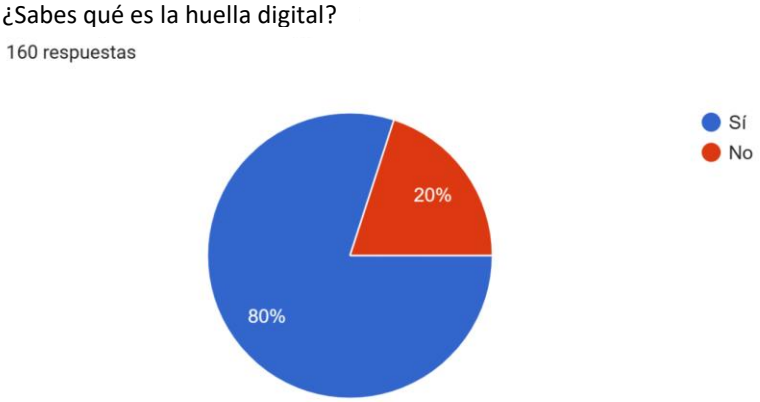


Figura 7.30: Matriz de correlación entre las variables demográficas y los casos de sesgos

7.3. Fase 2

7.3.1. Prueba de open Wi-Fi

AOI	Avg. TTFF	Avg. Time Spent	Fixations	Ratio	Avg. Fixation Duration	Avg. FFD	Attention	Avg. Revisits
Red claro	1.67	1.25	27	0.54	0.35	0.34	0.66	1.17
Red UVG	2.3	0.72	22	0.69	0.29	0.28	0.11	0.69
Red café	2.08	0.84	26	0.77	0.32	0.34	0.34	1
Red iPhone	1.95	1.01	21	0.54	0.32	0.35	0.6	0.62
Red restaurante	3	1.15	30	0.69	0.34	0.36	0.34	0.85

Tabla 7.2: Resultados de fijaciones en prueba de open Wi-Fi

AOI	Avg. TTFG	Avg. Time Spent	Gazes	Ratio
Red claro	1.37	0.99	425	0.77
Red UVG	1.29	0.82	400	0.85
Red café	1.49	0.71	314	0.77
Red iPhone	1.55	0.84	375	0.85
Red restaurante	2.3	0.99	467	0.85

Tabla 7.3: Resultados de miradas en prueba de open Wi-Fi

AOI	Clics	Avg. TTFC
Red claro	0	N/A
Red UVG	1	5.35
Red café	0	N/A
Red iPhone	0	N/A
Red restaurante	0	N/A

Tabla 7.4: Resultados de clics en prueba de open Wi-Fi

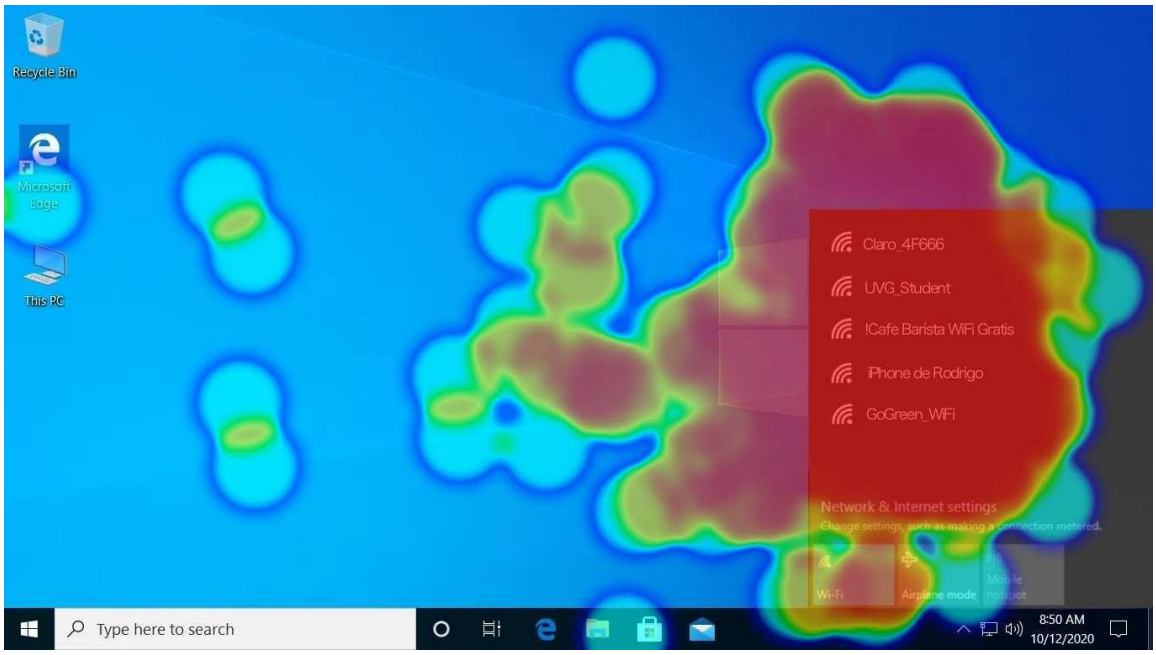


Figura 7.31: Heatmap de movimiento ocular en prueba de open Wi-Fi

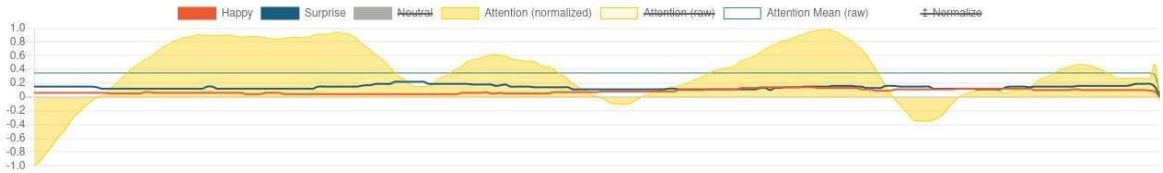


Figura 7.32: Atención y emociones captadas del movimiento ocular en prueba de open Wi-Fi

7.3.2. Prueba de phishing

AOI	Avg. TTFF	Avg. Time Spent	Fixations	Ratio	Avg. Fixation Duration	Avg. FFD	Attention	Avg. Revisits
Primer correo	4.73	1.93	64	0.77	0.28	0.27	0.18	3.08
Correo de phishing	6.4	1.1	32	0.69	0.32	0.3	-0.16	1.46
Tercer correo	5.57	0.75	23	0.69	0.3	0.28	-0.15	1.08
Correo de campaña	6.59	0.85	43	0.92	0.23	0.25	-0.51	2.08
Quinto correo	5.8	1.6	42	0.62	0.32	0.26	0.48	1.77
Correos leídos	6.47	2.94	95	0.77	0.24	0.24	-0.04	1.46

Tabla 7.5: Resultados de fijaciones en prueba de phishing en bandeja de entrada

AOI	Avg. TTFG	Avg. Time Spent	Gazes	Ratio
Primer correo	1.38	2.07	1015	0.85
Correo de phishing	2.13	0.9	475	0.92
Tercer correo	2.68	0.8	417	0.92
Correo de campaña	3.39	1.03	561	1
Quinto correo	6.18	1.34	631	0.85
Correos leidos	5.83	3.17	1424	0.85

Tabla 7.6: Resultados de miradas en prueba de phishing en bandeja de entrada

AOI	Clics	Avg. TTFC
Primer correo	9	3.87
Correo phishing	2	11.22
Tercer correo	1	5.57
Correo campaña	2	8.05
Quinto correo	1	3.23
Correos leidos	4	10.05

Tabla 7.7: Resultados de clics en prueba de phishing en bandeja de entrada

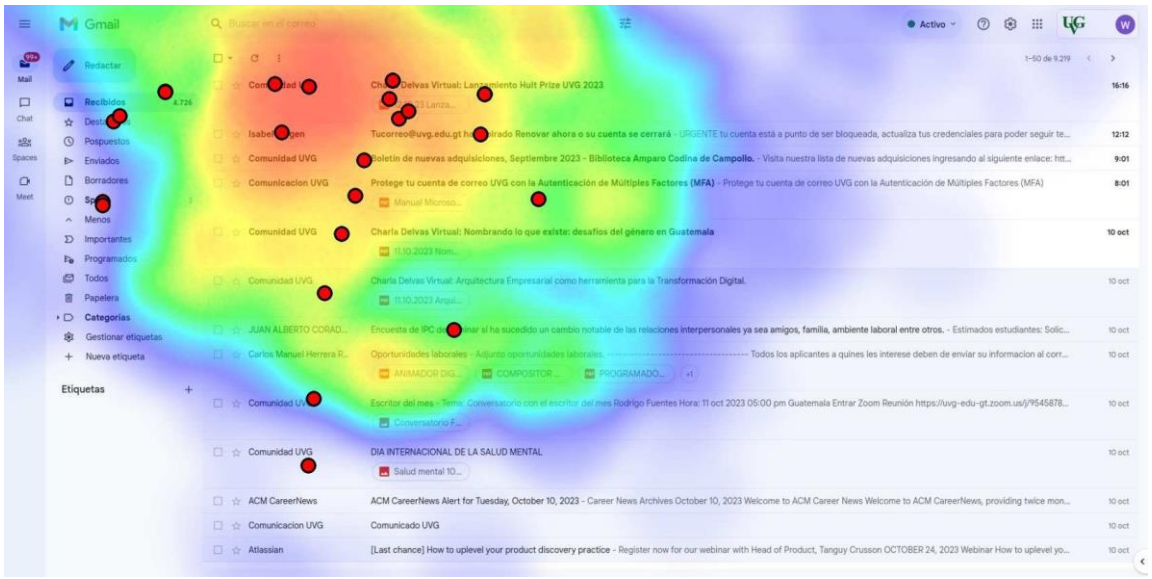


Figura 7.33: Heatmap de movimiento ocular en prueba de phishing en bandeja de entrada

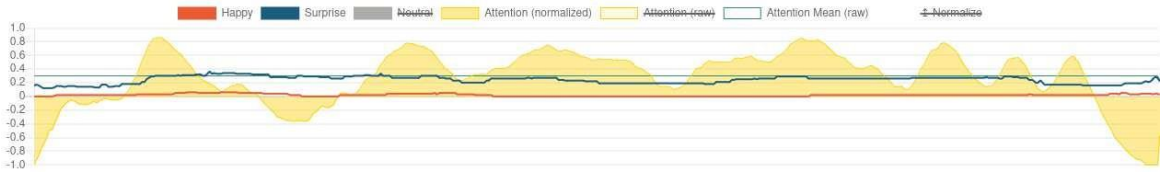


Figura 7.34: Atención y emociones captadas del movimiento ocular en prueba de phishing en bandeja de entrada

AOI	Avg. TTFF	Avg. Time Spent	Fixations	Ratio	Avg. Fixation Duration	Avg. FFD	Attention	Avg. Revisits
Asunto	8.38	1.57	62	0.85	0.26	0.3	-0.16	3.15
Emisor	7.92	0.76	28	0.69	0.25	0.3	0.48	1.23
Contenido	6.29	5.97	259	1	0.27	0.3	-0.3	5.85
Link	10.5	1.16	21	0.46	0.31	0.28	0.53	0.62

Tabla 7.8: Resultados de fijaciones en prueba de phishing en contenido de correo

AOI	Avg. TTFG	Avg. Time Spent	Gazes	Ratio
Asunto	4.28	1.5	757	0.92
Emisor	5.61	0.84	352	0.77
Contenido	3.65	6.99	3880	1
Link	7.21	0.73	332	0.85

Tabla 7.9: Resultados de miradas en prueba de phishing en contenido de correo

AOI	Clics	Avg. TTFC
Asunto	0	N/A
Emisor	0	N/A
Contenido	14	11.65
Link	9	4.38

Tabla 7.10: Resultados de clics en prueba de phishing en contenido de correo

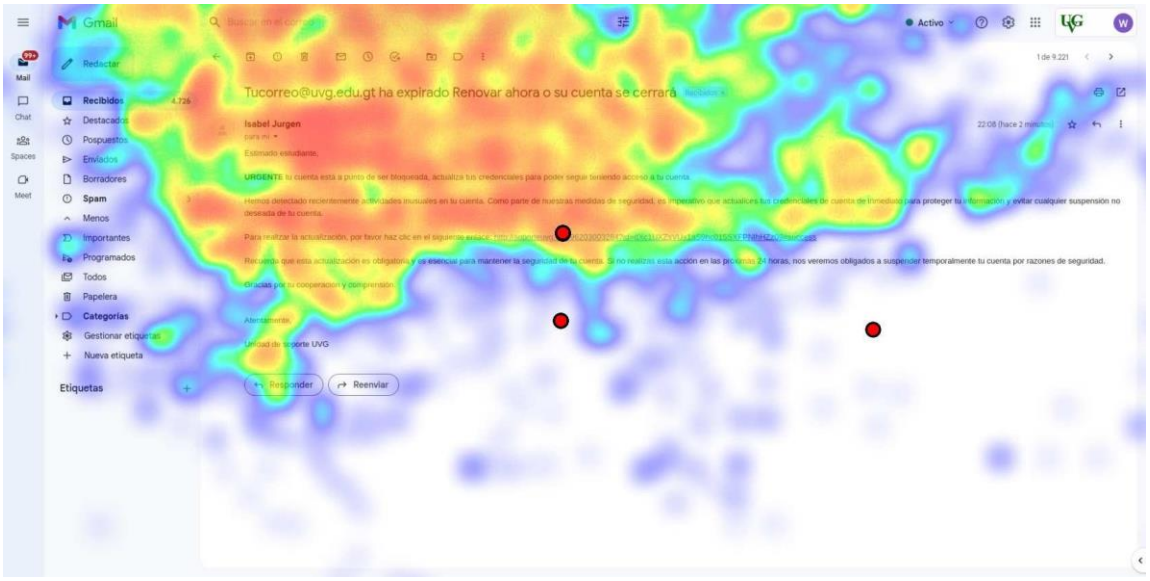


Figura 7.35: Heatmap de movimiento ocular en prueba de phishing en contenido de correo

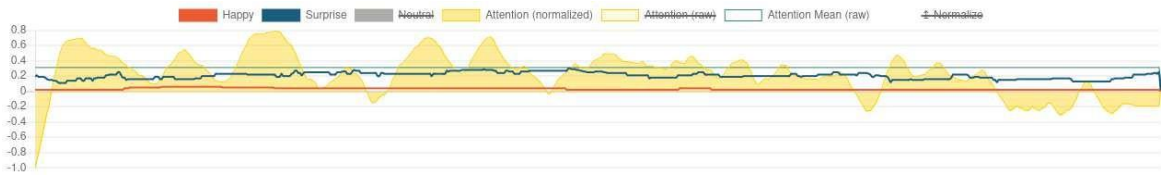


Figura 7.36: Atención y emociones captadas del movimiento ocular en prueba de phishing en contenido de correo

7.3.3. Prueba de bait

AOI	Avg. TTFF	Avg. Time Spent	Fixations	Ratio	Avg. Fixation Duration	Avg. FFD	Attention	Avg. Revisits
Emisor	4.45	0.51	21	0.62	0.2	0.19	-0.03	0.62
Link	5.88	0.44	12	0.38	0.2	0.2	-0.82	0.55
Preview	4.94	1	45	0.69	0.2	0.18	0.37	1.33

Tabla 7.11: Resultados de fijaciones en prueba de bait

AOI	Avg. TTFG	Avg. Time Spent	Gazes	Ratio
Emisor	2.47	0.78	307	0.69
Link	5.42	0.52	188	0.62
Preview	3.61	1.48	579	0.69

Tabla 7.12: Resultados de miradas en prueba de bait

AOI	Clics	Avg. TTFC
Emisor	0	N/A
Link	0	N/A
Preview	0	N/A

Tabla 7.13: Resultados de clics en prueba de bait

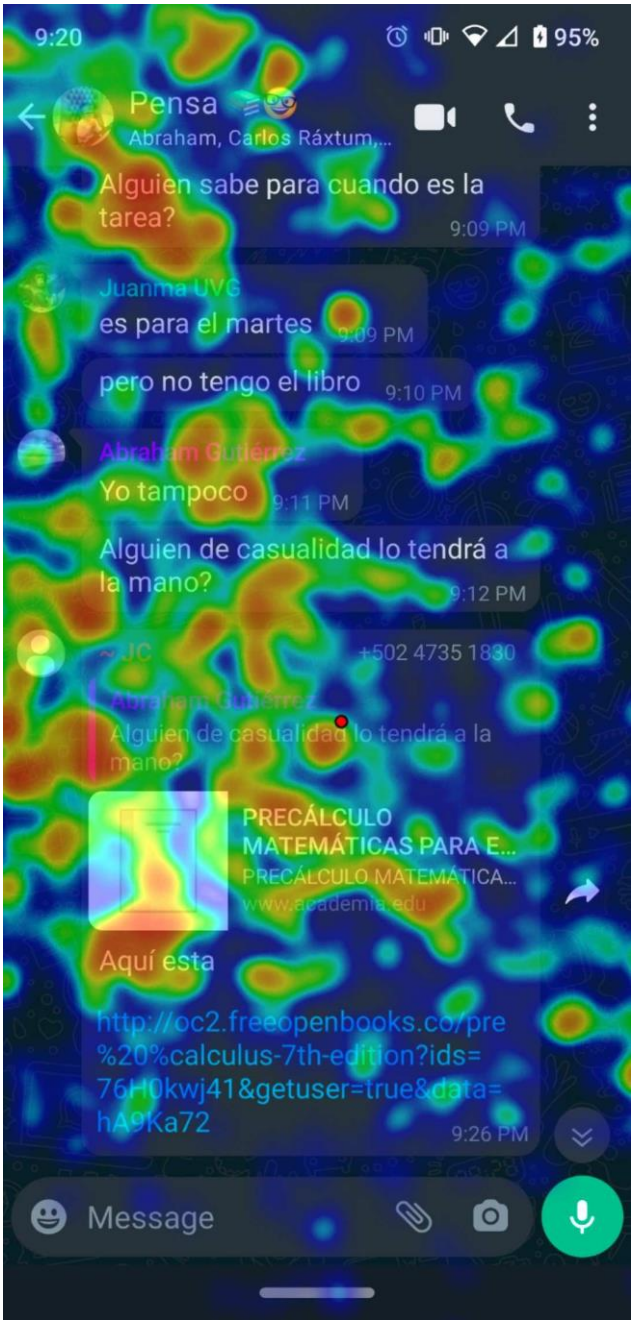


Figura 7.37: Heatmap de movimiento ocular en prueba de bait

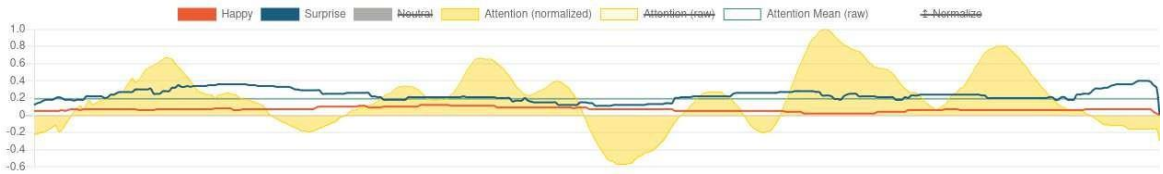


Figura 7.38: Atención y emociones captadas del movimiento ocular en prueba de bait

7.3.4. Prueba de password leak

AOI	Avg. TTFF	Avg. Time Spent	Fixations	Ratio	Avg. Fixation Duration	Avg. FFD	Attention	Avg. Revisits
Botón	4.61	0.64	11	0.38	0.32	0.35	0.23	0.31
Textfields	1.86	2.28	89	1	0.32	0.36	0.34	1.38
Términos y condiciones	3.81	1.06	36	0.92	0.36	0.39	0.8	0.77
Título	2.53	0.88	22	0.62	0.33	0.35	-0.01	0.42

Tabla 7.14: Resultados de fijaciones en prueba de password leak

AOI	Avg. TTFG	Avg. Time Spent	Gazes	Ratio
Boton	3.75	0.59	152	0.46
Textfields	0.86	2.62	1483	1
Terminos y condiciones	3.38	1.16	577	0.92
Título	0.91	0.8	279	0.62

Tabla 7.15: Resultados de miradas en prueba de password leak

AOI	Clics	Avg. TTFC
Boton	1	5.54
Textfields	2	2.82
Terminos y condiciones	0	N/A
Título	0	N/A

Tabla 7.16: Resultados de clics en prueba de password leak

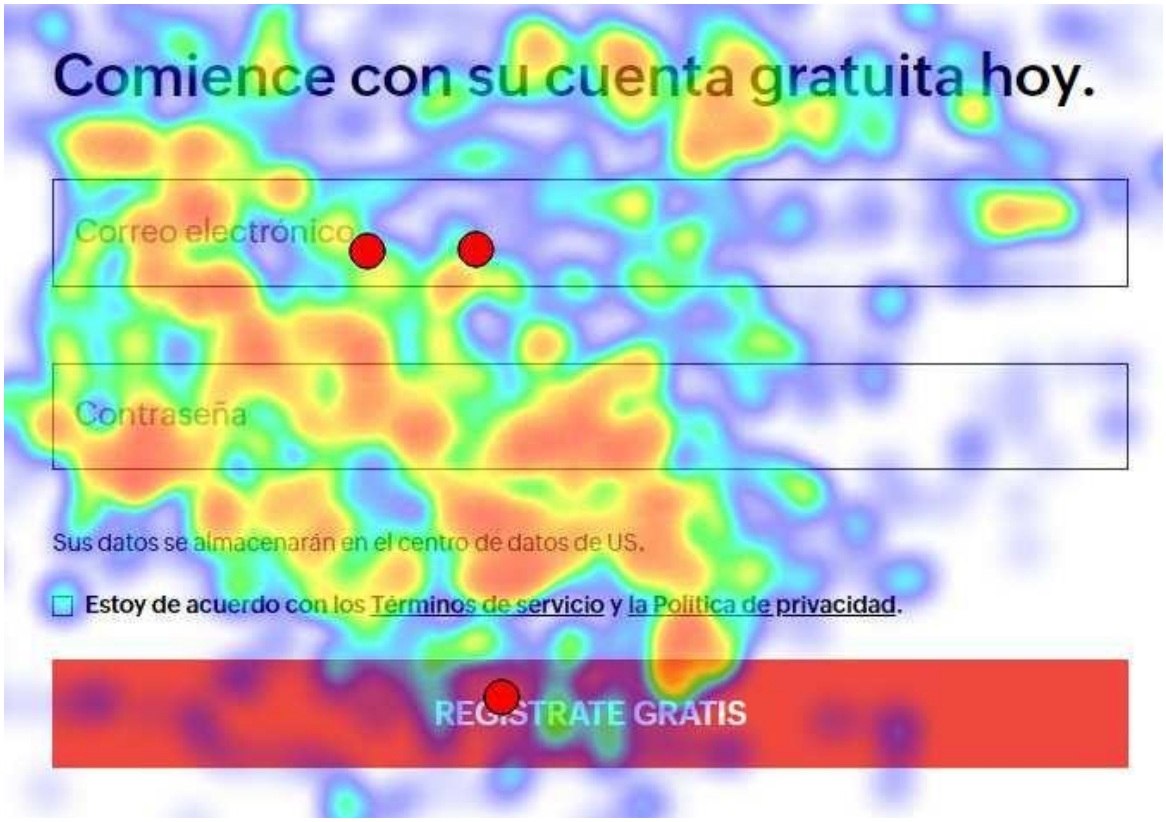


Figura 7.39: Heatmap de movimiento ocular en prueba de password leak

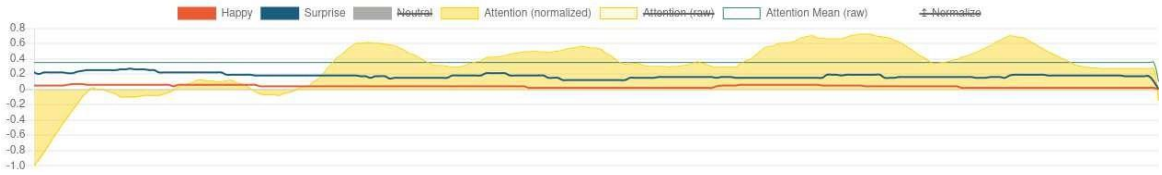


Figura 7.40: Atención y emociones captadas del movimiento ocular en prueba de password leak

7.4. Evaluación de desempeño de múltiples antivirus en un ambiente controlado

	Escenarios		
	Detección de virus	Detección de amenazas en página web que muestra spam, anuncios invasivos y abre pestañas sin permiso	Detección de phishing
AVG Free Antivirus			
Avast Free Antivirus			
Kaspersky Standard			
Bitdefender Security			

Figura 7.41: Calificación de desempeño de cada uno de los antivirus por escenario

CAPÍTULO 8

Discusión de resultados

8.1. Análisis estadístico de la población

En la primera fase, se pudo observar que en una escala de 1 a 10, el 43.1 por ciento de los estudiantes voto 10 y opinan que la seguridad informática es muy importante en sus vidas y en su futuro profesional, también, con un valor de 10 puntos, además el 19.4 por ciento votaron que 9, el 16.9 con un valor de 8. Lo que nos quiere decir que el 79.4 si cree que este es un tema relevante y al cual hay que prestar atención cómo se puede visualizar en el Gráfico 17 7.9. Sin embargo, si nos fijamos en el Gráfico 16 7.8 indican que el porcentaje de estudiantes que se autodefinen con un alto conocimiento en seguridad informática es considerablemente bajo, lo que sugiere una posible vulnerabilidad ante ataques de seguridad cibernética, destacando la importancia de abordar este aspecto en la comunidad estudiantil.

Por otro lado, al estudiar la relación entre las variables del formulario, se encontró como hallazgo más relevante que no existe correlación entre las variables demográficas y los sesgos (ver Figura 7.21). Esto implica que, para la población en cuestión, independientemente de la carrera, año, edad, o particularidades demográficas consideradas en esta investigación, un estudiante es igual de propenso a ser víctima de un ataque que explote cualquiera de esos sesgos. Este hallazgo puede ser controversial considerando que se esperaría que un estudiante fuera menos propenso a caer en estos sesgos mientras más avanzado sea su grado, o mientras más relacionado esté con la computación. Sin embargo, este resultado hace sentido al ser plasmado en la realidad cuando tomamos en cuenta la escasa cultura en ciberseguridad en el contexto de la población y el hecho que la UVG no fomenta una educación sólida en ciberseguridad a sus estudiantes en cualquier año y carrera y las pocas campañas que lanzan por medio del correo electrónico institucional no suelen ser efectivas en llegar a los estudiantes. Se reconoce que la excepción a este análisis son los estudiantes de computación con especialización en seguridad informática, sin embargo, estos representan una minoría en la población, además esto supone una brecha entre conocimientos técnicos de ciberseguridad y la puesta en práctica de los conceptos, pues como profesionales de la seguridad se nos hace más sencillo captar los errores de terceros que los nuestros, ya que esto involucra una carga emocional mayor.

Esta carencia en educación de ciberseguridad sin duda alguna afecta la respuesta cognitiva de los estudiantes frente a ataques informáticos, pues este conocimiento permite a los estudiantes reconocer las tácticas comunes utilizadas en los ataques. Al entender cómo operan estos ataques, los estudiantes pueden identificar señales de alerta que mitiguen el riesgo de convertirse en víctima.

8.2. Discusión de resultados de la fase 1

8.2.1. Hallazgos de psicología cognitiva

Lo primero que hay que tener en cuenta para entender los resultados de los sesgos, es el hecho de que los sesgos no son inherentemente malos, tienen el propósito de ayudar al cerebro a ahorrar energía liberándose del procesamiento de información selectiva. Dicho esto, si hay que tomar en cuenta que hay situaciones en las que estar sesgado puede conllevar a perjuicios, tal como lo es en un ataque de ingeniería social.

Los resultados muestran que los estudiantes son altamente susceptibles a los sesgos de confirmación (el 83.8% son alta o moderadamente susceptibles), anclaje (91.9% son alta o moderadamente susceptibles) y Dunning-Kruger (86.9% son alta o moderadamente susceptibles). En cuanto al sesgo de autoridad, está relativamente balanceado, con un 58.1% de estudiantes alta o moderadamente susceptibles. Y, por último, el sesgo al que menos fueron susceptibles fue al sesgo de optimismo donde el 55% de los estudiantes optó por la decisión menos sesgada.

La primera observación que se hace notable es la poca correlación entre el caso de Dunning-Kruger y el de optimismo, encontrándose en extremos opuestos donde el primero de estos ha demostrado que los estudiantes se ven altamente confiados en sus capacidades de mantenerse seguros y que consideran que el riesgo de ser víctimas es bajo, mientras que el segundo de estos nos plantea que los estudiantes no son del todo optimistas en pensar que una amenaza no les afectaría. No obstante, a pesar de la intuitiva correlación esperada, es válido considerar que estos resultados no sean mutuamente excluyentes, ya que el hecho de que una persona se sienta confiada en sus capacidades no implica que no tome acción ante el riesgo, más bien es lo contrario, la confianza en esa capacidad muchas veces viene de tomar acción ante la situación y no esperar a un evento de fortuna; por el otro lado el hecho que considere que el riesgo a que yo sea víctima sea bajo tampoco implica que no sea consciente de que el riesgo aún existe. Es importante destacar que la principal diferenciación entre el caso de Dunning-Kruger y el de optimismo, es que en el segundo de estos se plantea un caso en el que se requiere la decisión y acción del estudiante ante una amenaza presente que ya ha sido confirmada, por lo que esto pudo servir como incentivo para que el estudiante se haya sentido más optimista al hecho de que el también pudo haber sido una víctima del ataque que se plantea.

Respecto al sesgo de autoridad, es curioso notar que es uno de los que menos riesgo presentan a la población estudiada. Considerando que las edades de la muestra varían entre los 18 y 26 años, hay que enfatizar que son jóvenes que pertenecen a la generación Z, la cual es popularmente conocida por su tendencia a desafiar a la autoridad y el statu quo (Mundo, 2020). Esto pudo resultar en que la mayoría de los estudiantes no haya sentido urgencia o confiado plenamente en la figura de autoridad que le comunicaba en el caso.

Sobre esta misma línea de análisis, hay que agregar que la generación Z también se caracteriza por tener un alto apego a los recursos digitales, de hecho son “el grupo demográfico con el uso más intensivo de las redes sociales en todo el mundo"(Mundo, 2020). Este puede ser un factor que influyó directamente sobre los resultados del caso de sesgo de confirmación, pues es una población

que está muy acostumbrada a seguir tendencias y compartir abiertamente su opinión en redes sociales, lo cual al haber una inmensa cantidad de información en las redes sociales, se refuerza la necesidad del cerebro en filtrar cuál es la información más valiosa o más creíble pues sería muy costoso a nivel de procesamiento y memoria tener que evaluar cada post, comentario, mensaje, entre otros de forma individual, por lo que el cerebro tiende a sesgarse a aquellas opiniones o enunciados que se alineen con sus propias perspectivas.

Por otro lado, el sesgo de anclaje presentó resultados bastantes altos en susceptibilidad, sin embargo, hay que considerar que la mayoría fue moderadamente susceptible. Para este sesgo en particular los resultados no son muy conclusos, pues es muy probable que más que el sesgo de anclaje, influyera el sesgo de la experiencia reciente, pues si bien el caso realmente presenta un escenario en el que el sesgo del anclaje toma el papel principal, cabe destacar que la forma en la que se plantea simula que el individuo recibió la información del salario de su amigo tiempo atrás, sin embargo en la materialidad no es así pues mientras el participante lee el caso, tiene ahí mismo la información del anclaje, reforzando que tenga ese valor en la memoria de trabajo (la memoria de corto plazo) y no la memoria de largo plazo, lo cual es más la situación de un sesgo de experiencia reciente. Sin embargo, evaluar un sesgo meramente de anclaje es algo más elaborado de realizar y se sale del alcance de esta investigación, pues se requeriría de una de las siguientes opciones: encontrar un anclaje que todos o la mayoría de los participantes tenga en común; o inducir un anclaje de forma inconsciente en los participantes. A pesar de estos desafíos, el caso de anclaje aún sigue teniendo cierta validez, pues independientemente de que influya el sesgo de experiencia reciente, el sesgo de anclaje aún está presente en la decisión de los individuos.

8.2.2. Hallazgos para seguridad en sistemas de la información

En esta sección se analizarán y discutirán a detalle los resultados obtenidos de la primera encuesta realizada a los estudiantes de la Universidad del Valle de Guatemala con el fin de obtener datos relevantes para diseñar las pruebas controladas a la cual se someterán los voluntarios. El objetivo principal es examinar las respuestas que estos tuvieron para determinar su conocimiento sobre la seguridad informática y determinar su percepción inicial acerca de esta. Se analizarán las respuestas de las 5 preguntas sobre seguridad de la información.

Pregunta 1: Conocimiento sobre medidas de seguridad

En primer lugar, es importante destacar que en esta pregunta existe un 53% que expresa tener un conocimiento sobre las medidas de seguridad que deberían de implementar en sus dispositivos para proteger su información mientras que un 49% presenta un desconocimiento de estas medidas de seguridad para la protección de información en sus dispositivos electrónicos. Esto establece un enfoque sólido, en que un poco más de la mitad de los encuestados tiene conocimientos y el resto no lo tiene, respecto a la seguridad de la información.

El que la mayoría de los estudiantes presenten conocimiento sobre estas prácticas indica que existe concientización acerca de estos temas, sus dispositivos, y se puede inferir que posiblemente sepan de algunos ataques que pueden llegar a ser víctimas aunque implica que se necesita de más concientización respecto a las medidas, mejores prácticas y métodos de protección de la información.

La anterior pregunta es necesaria para tomarla en cuenta con respecto a la respuesta de las demás preguntas, las cuales evaluarán sus conocimientos con respecto a las medidas más comunes para

proteger su información, personas y datos.

Saber si las personas actualizan las aplicaciones a sus versiones más recientes, la cual puede considerarse parte de una medida de protección, debido a que estas son parches que mejoran la aplicación en varios sentidos y uno de ellos son bugs que permitan ataques cibernéticos y perjudican negativamente a los usuarios de estas. Determinar que tanta atención le brindan a la creación de contraseñas seguras, que palabras, frases, tipos usualmente contienen estas y sumándole a eso, si los encuestados reconocen los peligros de conectarse a redes abiertas, brindará un panorama y percepción del conocimiento general de los estudiantes de la Universidad del Valle de Guatemala y de esa forma presentar las mejores conclusiones.

Pregunta 2: Tiempo de espera para actualizaciones

Cabe destacar que en las respuestas de esta pregunta casi el 38% de personas recurre a que las aplicaciones, software, navegadores y tecnologías instalados en sus dispositivos tengan configurado para que se actualicen automáticamente, dando a entender que estos presentan influencia sobre el sesgo de automatización, donde las personas le tienen confianza a las tecnologías. Esto presenta y construye una base sólida respecto a que las personas encuestadas si presentan sesgos respecto al uso de tecnología y su juicio hacia ellas.

Luego, como dato interesante, se puede encontrar que hay opiniones divididas con respecto a cuándo actualizar las aplicaciones, softwares, navegadores y tecnologías con las opciones de; Espero a que haya revisiones de las actualizaciones para realizarse y la otra opción, cuando vuelvo a utilizar la aplicación me doy cuenta de las actualizaciones. Ambas opciones con un 21% de elección, donde se puede inferir que las personas hacen la tarea de investigar las versiones más recientes para saber si descargar e instalar la actualización, pues se ha visto muchas de las veces que existe el posible riesgo de que las actualizaciones puedan ser inestables y presentan mayor cantidad de exploits y bugs que pueden aprovecharse por atacantes cibernéticos. Aparte de realizar lo anterior con respecto a las actualizaciones, se puede observar que la mayoría de las personas dejan aplicaciones instaladas en su dispositivo y que hasta que vuelven a usarlas, la actualizan. Esto puede permitir que en caso el dispositivo ya haya sido comprometido con algún virus o similar, el ejecutar esta aplicación nuevamente y que esta esté infectada, mantendrá la infección incluso en la versión actualizada, por lo que perjudica negativamente al usuario.

Como últimas elecciones, el 16% de los usuarios instalan inmediatamente las actualizaciones cuando estas se encuentra disponibles, esto puede considerarse ser parte del sesgo de novedad, donde la persona por cualquier opción, función o característica diferente, realizan la actualización sin hacer revisiones e investigaciones previas acerca de la misma, ocasionando que en el caso de que la actualización sea inestable, quebrante el dispositivo hasta recibir el hotfix o parche. También se puede inferir que existe un sesgo de confirmación social, donde porque la mayoría opta por realizar la actualización de forma inminente, este también lo hace. La última elección con un 4% indica que nunca realizan la actualización sus aplicaciones, softwares, tecnologías, navegadores dándole cero importancias a que estos reciban un ataque o sean víctima de algún riesgo por no instalar la última versión. Esto presenta un sesgo de optimismo por parte de los estudiantes encuestados, ya que piensan que no recibirán la misma importancia o que no serán parte del radar de un atacante debido a que no tienen suficiente información de valor.

Pregunta 3: Tiempo de espera para cambio de contraseña

Lo destacable de analizar detalladamente los resultados de esta pregunta es que el 63% de los participantes cambian su contraseña sólo cuando la plataforma se los solicita. El sesgo de ilusión de seguridad se ve presente en este caso, pues creen que están seguros con las medidas de protección y "buenas" prácticas que estos implementan en su organización. Dando a entender que la mayoría de los estudiantes de la Universidad del Valle de Guatemala tienden a esperar que los recursos de la universidad, sus aplicaciones y plataformas les soliciten que hagan el cambio de contraseña sin ellos realmente colocarle importancia a realizarlo cada cierto tiempo, lo cual sería lo recomendado por varios expertos en ciberseguridad y soportado por una consultoría de tecnología tal que (JSM, 2023) lo menciona.

Otro dato destacable con respecto al tiempo el cual toman los encuestados para realizar un cambio de contraseña en sus tecnologías, aplicaciones, dispositivos, entre otros, es que el 17% opta por hacer un cambio de contraseñas cada año lo cual indica que están influenciados por el sesgo de disponibilidad donde mantienen la contraseña por un largo periodo de tiempo ya que esta es fácil de recordar y no pueden mantener un cambio constante de esta por la dificultad de su capacidad para hacerlo.

Lo último por decir es que sólo el 13% si realiza cambios de su contraseña entre 3 a 6 meses, lo cual es considerado lo óptimo y lo ideal, dando a conocer que existe un porcentaje muy bajo de que los estudiantes le colocan la importancia que se necesita para la protección de sus cuentas, dispositivos, softwares y tecnologías. Un porcentaje del 7% no realiza cambios en sus contraseñas dando a entender que están sesgados a ser optimistas, debido a que creen que nunca se le realizará un ciberataque, o querrán sus credenciales para obtener información personal y delicada para ellos.

Pregunta 4: Creación de contraseñas

Lo más destacable de esta pregunta es el porcentaje de personas que utilizan palabras de una larga cantidad de caracteres para crear su contraseña, tal que un 35% alteran estas palabras largas para que esta sea su método de validación para sus cuentas. Posteriormente, un dato interesante, es que el 31% de los estudiantes encuestados utilizan la combinación de su nombre con fecha de nacimiento para la generación de sus contraseñas. El utilizar contraseñas que tengan datos personales como nombre y fecha de nacimiento es una mala práctica debido a que se comparte estos datos personales en redes sociales, cuentas bancarias, creación de correos electrónicos por lo que se facilita a los atacantes el obtener estos datos mediante un ataque de fuerza bruta, según (Dominios Gt, 2020) existen varias recomendaciones para diferenciar una buena o mala contraseña. Esto evidencia un claro sesgo de sobre confianza, donde piensan que el colocar una contraseña de este tipo generará una mayor protección para acceder a sus cuentas.

Dentro de las opciones más escogidas, omitiendo las anteriores opciones, se encuentra un 20% el uso de palabras que los estudiantes utilizan en su día a día, por detrás de esta opción se encuentra el uso de nombres y personajes de series o películas con un 19%, y también se presentó la utilización del nombre de su mascota con un 16% y por último el uso de softwares para la creación de estas con un 16% nuevamente. Es importante saber que mediante ingeniería social se puede llegar a tener esta información, debido a que al generar confianza entablando conversaciones con estas personas, se puede saber las palabras que usan diariamente y el contexto en el cual las usan descubriendo así partes fundamentales de sus contraseñas. La utilización de preguntas sobre sus series, películas y personajes favoritos de estas puede dar indicaciones y guiar al atacante a obtener la contraseña de este tipo. El nombre de la mascota con simples preguntas puede obtenerse además de la especie, raza entre otros datos que pueden ser de interés para adivinar y crackear la contraseña. Nuevamente se puede ver expresado un sesgo de sobre confianza en elementos cotidianos para la creación y

generación de contraseñas. La utilización de software para la creación de contraseñas seguras puede ser un arma de dos filos, esto porque si puede llegar a generar una contraseña que tienen un alto nivel de seguridad pero si no se tiene el conocimiento de estas aplicaciones, se podría llegar a divulgar en internet estas contraseñas donde los atacantes procederán a obtenerlas debido a que son de dominio público y de esa forma colocarlas en un descifrador de contraseñas y obtener acceso a las cuentas vinculadas a la contraseña. Es un sesgo de automatización debido a la confianza que los estudiantes le brindan a las tecnologías debido a su facilidad de uso, pero con la existencia de posibles fallos debido a que esta no es perfecta.

Las menos escogidas que pueden ser relevantes para el estudio, son el nombre de su celebrity crush con un 7%, buscar ejemplos en internet con un 3% y cosas random con un 2%. Esto indica que los estudiantes no son muy propensos a escoger estos tipos de contraseñas para cuidar y proteger sus cuentas.

Pregunta 5: Conexión a Wi-Fi

En primer lugar, un 62% de los estudiantes encuestados se conectan a redes que prestan un servicio de conexión Wi-Fi abierto y de forma gratuita. Mientras que un 38% de los estudiantes no se conectan a estos servicios. Esto indica que la mayoría de los encuestados no prestan atención a los riesgos, amenazas y ataques que estos pueden recibir conectándose a la red de un lugar público o similar.

Se presenta un hallazgo muy importante, debido a que la falta de conocimiento sobre la seguridad en redes públicas debe de ser tratado con importancia, según el artículo (Pastor, 2017) pues existe el riesgo de transmitir la información ya sean credenciales, datos personales y en casos extremos el contagiarse de un malware con la conexión de estos. Los resultados de esta pregunta presentan que los estudiantes son susceptibles e influenciables a varios sesgos, tales como sesgo de optimismo, disponibilidad, anclaje.

El sesgo de optimismo se presenta cuando los estudiantes se conectan a estas redes abiertas sin tener conocimiento alguno de los efectos negativos que pueden tener en su persona, mostrando una actitud relajada al realizar la conexión que luego puede llegar a perjudicarlos. El sesgo de disponibilidad se presenta por el hecho de que ellos no han sufrido de ataques o riesgos al conectarse anteriormente a redes similares o no cuentan con experiencias pasadas que le haya hecho dudar el realizar la conexión, por lo tanto, llegan a subestimar he ignorar lo que realmente puede pasar en caso si suceda la vez que lo hagan, basando sus decisiones directamente he instantáneamente en lo ya vivido. Por último, el sesgo de anclaje influencia a los estudiantes a que tomen la decisión por necesidad o conveniencia, puede ser para no gastar sus datos móviles, porque no cuentan con estos o una alternativa que tenga mejor seguridad que una red pública, causando que tomen como principal y única opción la conexión gratis a internet que ofrece el lugar público.

El otro 38% que seleccionó no conectarse a redes abiertas puede inferirse que tienen conocimiento sobre los peligros que esto conlleva o cómo perjudica negativamente a su persona además de estar influenciados por el sesgo de confirmación. El sesgo de confirmación puede verse expresado cuando estos mediante investigaciones pasadas, información adquirida y conocimientos no realizan la conexión a estas redes, por lo que optan por otras alternativas para la navegación segura en estos lugares.

Pregunta 6: Medidas de protección

Destacable y con bastante diferencia respecto a las otras opciones se seleccionó el antivirus como medida de protección en los dispositivos por parte de los estudiantes con un 54% de preferencia sobre las otras. El que la mayoría de los estudiantes tenga antivirus indica que la mitad de los encuestados toman una de las protecciones esenciales para sus sistemas contra malwares, virus, entre otros según (The Bridge, 2023). Es importante resaltar que como lo menciona el blog, no es una solución infalible el tener un antivirus, lo que se traduce a que tenerlo está bien pero no es suficiente. Esto resulta en que la mayoría de los estudiantes que sólo utilizan antivirus como única medida de protección para sus dispositivos estén sesgados por anclaje, confirmación y norma social.

El sesgo de anclaje se expresa de la forma en que ellos tienden a pensar que el antivirus es suficiente para contrarrestar y proteger el dispositivo sobre cualquier tipo de ataque. Este sesgo influye de la misma manera a que estos no lleguen a explorar otras soluciones y medidas de protección debido a la elección precipitada e inicial de implementar un antivirus. El sesgo de confirmación se manifiesta cuando estos tienen una medida de protección escogida como lo es el antivirus y por más que tengan información que sustenta que podrían existir mejores medidas de seguridad, estos hacen caso omiso debido a la información presentada primero, que en este caso fue la del antivirus y medida de protección que tienen actualmente. Por último, el sesgo de norma social, se expresa cuando el entorno y personas como tal del estudiante cuentan sólo con esta medida de protección optando por seguir sus pasos y adquirir la misma posición con una un antivirus como protección.

Un 39% escogió el tener habilitado el Two Factor Authentication como medida de seguridad y el tener un gestor de contraseñas con un 31% como medida de seguridad. El 39% al tener como medida de protección el 2FA (Two Factor Authentication) es buena práctica, debido a que presenta que tienen conocimiento y están conscientes que el tener usuario y contraseña no les brinda la mayor protección a sus dispositivos, esto según el artículo (What Is Two-Factor Authentication (2FA)?, n.d.). El 39% utiliza un gestor de contraseñas para proteger sus dispositivos es lo esencial para proteger credenciales importantes y accesos a los sistemas, tal como se menciona en (Fernández, 2023). Los sesgos cognitivos que se manifiestan en el porcentaje de estudiantes que no escogieron estas medidas de protección para sus dispositivos son el sesgo de anclaje y sesgo de optimismo.

El sesgo de anclaje se expresa cuando estos prefieren la comodidad de sólo ingresar las credenciales e ingresar a sus sistemas y cuentas sin realizar un paso extra que en este caso sería el 2FA. Mientras que, en el caso de utilizar un gestor de contraseñas, los estudiantes prefieren no utilizar estos softwares y aprovechar sus beneficios porque les es más fácil recurrir a patrones familiares para la creación de contraseñas, que estas sean fáciles de recordar o una alternativa similar, por lo que no recurren a un cambio o lo subestiman. El sesgo de optimismo se manifiesta en ambas medidas, donde el implementar alguna de ellas no es necesario porque nunca van a estar amenazados, en riesgo o serán perjudicados por algún ataque que reciban.

Por último, las medidas de protección menos escogidas fueron ningún dato personal o credenciales guardadas en el dispositivo con un 21% y un 18% cuentan con una seguridad nula en sus dispositivos. El 21% el que como medida de seguridad no tengan datos personales e información importante en sus computadoras es una medida eficaz debido a que, si reciben un ataque o algo similar, no se recaba información importante sobre ellos. El 18% de los estudiantes que no tienen una medida de seguridad, indica una falta de concientización y conocimiento sobre los riesgos que se presentan día a día con respecto a los dispositivos que estos utilizan. Claramente, el sesgo de optimismo y sobre confianza se presentan en esta decisión. El no tener métodos de seguridad es ser optimista con respecto a que nunca se va a recibir un ataque o se estará en riesgo

alguno por parte de los ciberdelincuentes, ya que nuestra información no es de valor con respecto a la de otros estudiantes o frente a una organización. El sesgo de sobre confianza se presenta cuando los estudiantes que no tienen medidas de seguridad se creen mejores que los atacantes, ya que pueden pensar que el que ni siquiera necesita protección porque los atacantes no son lo suficientemente eficientes como para acceder a sus dispositivos.

Estos resultados de las encuestas establecen una base sólida para comprender las percepciones iniciales de seguridad de los estudiantes y el cómo se pueden desempeñar en las pruebas, planteando hipótesis y comprobando cada una de ellas. A continuación, se explicará cómo estas percepciones se traducen en el desempeño real en pruebas controladas de seguridad informática, desde la visualización de imágenes hasta la contestación de preguntas que guíen a la determinación de los sesgos cognitivos que pueden surgir durante la toma de decisiones de este tipo.

8.2.3 Hallazgos en UI/UX

Pregunta 1: Inicio de sesión

Para la primera pregunta del formulario, como se puede observar en la Figura 7.22, el 13.8% de los encuestados, alumnos de la Universidad del Valle de Guatemala, respondieron en una situación similar: ingresaron con sus credenciales sin sospechar nada. Este comportamiento está relacionado con los sesgos de normalidad y el sesgo de confirmación. Principalmente, el sesgo de normalidad sugiere que un grupo de estudiantes percibe esta situación como segura y aceptable debido a su familiaridad. Por ejemplo, podrían asumir que la interfaz se actualiza con frecuencia, lo que les brinda la confianza suficiente para proporcionar sus credenciales sin dudarlo mucho. Asimismo, el sesgo de confirmación se refleja en la confianza de los estudiantes que afirmaron que ingresarán sus credenciales. Estos se respaldan en creencias existentes, asumiendo que no existe ningún riesgo y que no están siendo víctimas de ningún ataque. Esto los convierte en un grupo expuesto a riesgos cibernéticos, ataques de *phishing* o de *baiting,* en donde el atacante busca aprovechar la confianza excesiva para suplantar una interfaz o correo pidiendo una verificación con el objetivo de robar información confidencial de la víctima.

Por su parte, el 33.8% respondió que, en una situación de este tipo, comprobarán si el URL es el correcto. Este comportamiento de confirmar si la situación es segura y se alinea con las expectativas de seguridad ya establecidas por los alumnos en experiencias pasadas está relacionado con el sesgo de confirmación, donde se valida que, en este caso, la URL valide y confirme nuestras creencias de seguridad pasadas. Así mismo, se puede ver que este grupo de estudiantes, a través del sesgo de la disponibilidad, recuerda la importancia de verificar que se encuentran en el URL correcto. Esto puede ser porque en el pasado ya han sido víctimas de ataques como phishing o pharming o tengan conceptos y estén conscientes sobre seguridad cibernética. Por último, el restante 52.5% de estudiantes respondió que, dada una situación de este tipo, cerraron la ventana y no ingresaron sus credenciales. Esta respuesta está relacionada con el sesgo de confirmación, ya que al ver que la página no confirma sus creencias preexistentes, desconfiaron inmediatamente de la página web y como medida de protección, la cerraron, independientemente de que los cambios no indiquen un problema de amenaza. Así mismo, al percibir que no les resulta familiar y sentirse en peligro, el sesgo de normalidad las llevó a desconfiar de la página, de manera que opten por no brindar sus datos.

Pregunta 2: Pop-Ups

En la segunda pregunta cómo se puede observar en la Figura 7.23, el 24.4% de los encuestados, respondió que cerraran cuidadosamente los *pop-ups,* aunque al hacer esto abran nuevas pestañas en el navegador. Esta acción indica que los sujetos ven la necesidad de realizar hacer algo frente al problema, en este caso el cerrar los *pops-ups* es una respuesta automática para controlar la situación, aunque la acción no resuelva la situación y genera más problemas, eso indica que el sesgo de acción controlar este posible accionar hipotético. Asimismo, el sesgo de aversión a la pérdida, ya que los estudiantes perciben que constante apertura de nuevas ventanas representa una pérdida de control en su experiencia como usuario, lo cual junto con el sesgo de acción los lleva buscar controlar la situación cerrando los *pop-ups,* aunque esto resulte afectándolos al final. Este posible accionar ante esta situación hace a este grupo, vulnerable a ataques de *baiting,* al estar abriendo muchas páginas en el navegador un pop-up podría abrir una página y descargar algún programa malicioso. Por su parte, el 25.6% de los encuestados, respondió que utilizan algún tipo de *add-blocker* mientras que el 21.9% de los estudiantes encuestados respondió que tienen su navegador configurado para no abrir ventanas emergentes sin permiso. Esto demuestra que ambos grupos valoran su experiencia de usuario y usabilidad por lo que no permiten que elementos extras les arrebaten esto. Ambos grupos también experimentan el sesgo de confirmación, donde buscan y adoptan soluciones que respalden su deseo de una experiencia de usuario sin interrupciones. Al elegir un bloqueador de anuncios o configurar el navegador para bloquear ventanas emergentes, están confirmando su creencia en la importancia de la usabilidad y la experiencia del usuario. Además, para el grupo que utiliza un *add-blocker* el sesgo de aversión al riesgo está presente en aquellos que utilizan algún tipo de bloqueador de anuncios. Prefieren prevenir la posibilidad de anuncios molestos en lugar de enfrentar la incertidumbre de encontrarse con *pop-ups* no deseados. Por último, el 28.1% de los estudiantes encuestados, respondió que cierran la página dada una situación como la que se planteó en la pregunta, esta respuesta está relacionada con el sesgo de disponibilidad, ya que cerrar la página es la opción más fácil de las 4, sin embargo, esta no busca una solución a largo plazo o el sesgo de acción, en donde se evita un problema con la acción rápida de cerrar la ventana. Otro sesgo presente sería el sesgo de la aversión a la pérdida donde se priorice la tranquilidad y no afectar la experiencia de usuario cerrando los *pop-ups.* El cierre de la página *web* podría ser una respuesta impulsiva motivada por la aversión a la pérdida, la preferencia por acciones inmediatas y la disponibilidad de esa opción en el momento del encuentro con *pop-ups* molestos.

Pregunta 3: Banca en línea

Para la tercera pregunta, cómo se puede observar en la Figura 7.24, el 11.9% de estudiantes indicó que en una situación de ese tipo se fijaron primero en los botones, esto porque confían (sesgo de familiaridad) en elementos de *UI* familiares para verificar la autenticidad de un sitio web. Por su parte el 18.8% de los estudiantes encuestados respondió que los campos del formulario son lo primero en lo que se fija para comprobar que se encuentran en la página oficial de su banca, este está relacionado con el sesgo de confirmación, donde verifican la presencia de formularios que recuerdan haber llenado con anterioridad al utilizar su banca o el sesgo de disponibilidad, ya que validar que estén los formularios para constatar que se encuentran en la página oficial. Con mayoría el 36.9% de los encuestados respondió que se fijan principalmente en la barra de navegación, esto está relacionado con el sesgo de confirmación ya que validan y confirman creencias de seguridad pasadas al ver que se encuentran en la *URL* correcta. Además, el 10.6% de los estudiantes contestó que se fijan en el tema de la página, así como en los colores, esta acción está relacionada con el sesgo de normalidad, ya que valida su experiencia de usuario pasada para determinar que se encuentren en la banca correcta. Por último, el 21.9% de los encuestados respondieron que se fija

en otro tipo de elementos del *UI,* multimedia *o fonts,* este enfoque está relacionado con el sesgo de la normalidad y la disponibilidad, ya que ambos sesgos buscan validar que elementos conocidos en experiencias pasadas se encuentren presentes. Los cinco grupos, de igual manera quedan expuestos a ataques cibernéticos, ya que ataques de phishing en donde los ataques puede replicar los botones, sobretodo si los botones son de alguna librería o replicar los formularios para hacer creer a las víctimas que están en la banca en línea oficial o ataques de *pharming o baiting* en donde pueden hacer creer a la víctima la información que refleja la barra de navegación es la oficial de manera que la víctima ingrese sus credenciales.

Pregunta 4: Descarga de material

Para la última pregunta del formulario, como se puede observar en la Figura 6.1, todas las opciones comparten la misma estética, diferenciándose únicamente en los elementos de cada botón. El propósito de esta evaluación es determinar cuál de estos elementos, en este caso, la flecha, se percibe como más confiable por parte de los estudiantes. En la Figura 7.25, se evidencia que tanto la Opción 2 como la Opción 3 fueron seleccionadas como la primera opción por un 9.4% de los estudiantes encuestados. En contraste, un considerable 21.9% optó por la Opción 1 como el botón al que darían clic para descargar el material solicitado por el catedrático.

Este fenómeno podría explicarse mediante el sesgo de normalidad, ya que la Opción 1 podría ser percibida como la elección estándar debido a su posición de liderazgo en la disposición de los botones. Los encuestados pueden haberse sentido inclinados a seleccionar el primer botón de manera predeterminada, sin considerar exhaustivamente las otras opciones.

En cuanto a la Opción 4, observamos que el 25% de los estudiantes la prefirió. Este sesgo de disponibilidad puede estar influyendo, ya que el elemento específico de la flecha en esta opción podría haber sido más familiar o llamativo para algunos encuestados, llevándolos a elegir de manera más activa.

Sin embargo, resulta intrigante que el 34.4% de los estudiantes indicaron que no darían clic en ninguna de las opciones de botones. Aquí entra en juego el sesgo de acción, ya que los encuestados podrían haber experimentado una falta de confianza general en las opciones presentadas. Es posible que la uniformidad en la estética haya creado una sensación de indiferencia, haciendo que un porcentaje significativo de participantes se abstuviera de tomar una decisión definitiva.

Los resultados de la encuesta revelan que los estudiantes de la Universidad del Valle de Guatemala muestran diferentes comportamientos y decisiones en situaciones relacionadas con la seguridad cibernética. La presencia de sesgos cognitivos, como el sesgo de normalidad, confirmación, disponibilidad entre otros anteriormente mencionados, influye en la experiencia de usuario de cada estudiante.

8.2.4. Hallazgos en tráfico de red

Pregunta 1: Visita a páginas que ofrecen contenido gratuito

El 45% de los 160 estudiantes encuestados acceden a páginas que ofrecen contenido de paga de manera gratuita. Esto indica que una muestra significativa de estudiantes no sabe de los peligros a los que están expuestos y actúan influenciados por los sesgos cognitivos de norma social y el de ilusión de control, por lo que vemos que los sesgos cognitivos llevan a los mismos usuarios y en este caso a los estudiantes a ser una vulnerabilidad para ser víctima de un ataque cibernético, debido

a que por la falta de conocimiento de técnicas de protección cibernética, actúan basados en sus pensamientos sin mayor análisis de riesgos cibernéticos. Muchas de estas páginas muestran una gran cantidad de anuncios dado a que es una de las maneras en que obtienen dinero para pagar por los servidores. Estos al ser muy invasivos, pueden llevar a los estudiantes a descargar algún tipo de servicio de adblock y de alguna manera bloquearlos. Sin embargo, esto sólo hará que el sesgo de la ilusión de control se active dado que el usuario tendrá la idea que usando un servicio externo podrá darle un mejor control de lo que desea ver. A este mismo sesgo se le suma que cuando la misma página empieza a abrir otras pestañas sin el permiso del usuario, este solamente debe cerrarlas y sigue creyendo que tiene control, pero es obvio que no es así, porque se está realizando algo sin su permiso. Aquí también entra el sesgo de optimismo, dado a que pueden tener el pensamiento que nada grave les sucederá, que probablemente mientras no den clic a un botón extraño de una ventana emergente o hablen con extraños, todo seguirá bien. Y por ello mismo, entra el sesgo de status quo el cual puede verse reflejado en "Sí nada grave o raro me ha sucedido, ¿por qué he de parar de visitar este tipo de páginas?".

Además, hoy en día gracias a las redes sociales se pueden encontrar varias publicaciones de diferentes usuarios que recomiendan paginas para ver contenido de paga de forma gratuita y esto puede aumentar el sesgo de norma social, donde el estudiante se percate que esas publicaciones tengan ciento, miles o millones de visitas con buenas reseñas lo cual lo haga pensar que entonces es común visitarlas y por lo tanto, seguir ese comportamiento de aceptación (y esto puede influenciar a aquellos que le rodean). Por esto último, al haber visitado una página y ver contenido sin ningún riesgo que el usuario vea como un peligro potencial, estará la posibilidad que visite otras páginas similares teniendo el mismo pensamiento que todo estará bien y nada fuera de lo normal sucederá, mostrando claramente el sesgo de resultado.

Es entonces el actuar de los usuarios basados en sesgos cognitivos que los hacen tomar decisiones peligrosas sin contemplar el riesgo que esto significa y haciéndolos vulnerables y que cualquier ciber- atacante pueda explotar esta vulnerabilidad y de esa forma lleven con éxito ataques por medio de software como el rasomware que permitirá encriptar toda la información de un dispositivo o de igual forma podrían verse infectados por algún tipo de spyware que espiar y obtener información personal o en el peor de los casos replicarse a la red del lugar de trabajo del usuario y provocar un ataque aún mayor.

Pregunta 2: Acceso a redes públicas

El 49.4% de los 160 estudiantes entrevistados se conectan pocas veces a redes públicas. Mientras que un 15% se conecta a menudo a estas. Estos dos grupos de estudiantes puede que se conecten a redes públicas dado a que son usualmente gratis, no requieren de contraseña y puedan ahorrar recursos propios (como los datos móviles), dando una "falsa" comodidad el cual es un claro ejemplo de la heurística de disponibilidad que los afecte psicológicamente y los lleve a en lugar de tomar la decisión analizando toda la información correspondiente y los riesgos que esto conlleva, y sólo actuar bajo percepciones y así convertirse el estudiante en la principal amenaza de un ataque cibernético. También puede verse reflejado el sesgo de ilusión de control, dado a que podrían tener la idea que siguen teniendo control sobre todo lo que hacen dentro de la red cuando en realidad sólo están generando tráfico que puede ser de interés para alguien con fines maliciosos como un ataque de Man-in-the-Middle en el que el atacante pueda intervenir todo o parte del tráfico que circula por esa red. Este mismo sesgo puede ser más común cuando a un grupo de estudiantes no les preocupa los riesgos de seguridad al usar redes Wi-Fi públicas (un 20.6% de los 160 estudiantes encuestados). A este grupo mencionado, se le puede sumar que un 45% de los 160 estudiantes encuestados le preocupan este tipo de riesgos sólo para ciertos casos, lo que refleja el sesgo de status quo dado a

que seguirán manteniendo su línea de pensamiento de que está bien conectarse a una red pública en situaciones en específico debido a que no han sido víctimas de ataques cibernéticos en ocasiones anteriores que han tomado el mismo comportamiento, que es precisamente lo que hace el sesgo de status quo y que puede ser un factor importante en una falla de seguridad cibernética provocada por parte de los mismos estudiantes. Y con todo esto mencionado, puede ser que como no es común escuchar noticias de robo de información proveniente de lugares públicos, exista el sesgo de sobre confianza porque el estudiante puede pensar que será poco probable que sea víctima de uno, sin embargo, posiblemente ya ha sido víctima de un ataque y no se ha dado cuenta por actuar basado en sus sesgos cognitivos y no en conocimiento sobre técnicas de defensa y buenas prácticas al navegar en cualquier red sea pública o privada.

Pregunta 3: Phishing

El Phishing es una de las técnicas más utilizadas de ataques cibernéticos por personas que desean obtener información como contraseñas, números de tarjeta de crédito, entre otras. Y es una técnica muy utilizada ya que los ciber atacantes saben que una de las principales falles de seguridad informática son los usuarios, y por ello hacen uso de ingeniería social para engañar a los usuarios presentando por medio de phishing sitio web y mensajes que son personalizados para que parezcan verídicos y así influir a que el usuario caiga en la trampa y no tome en cuenta medidas de defensa como el análisis de los mensajes y sitios web que se les solicita abrir, si no que al contrario el usuario se vea influenciado por los sesgos cognitivos ya mencionados y así llegué a ser víctima de un ciberataque que podría traer graves consecuencias. Sería posible mitigar estos ataques y reducir las fallas de seguridad cibernética si se contara con el conocimiento necesario y oportuno sobre seguridad informática y cibernética.

Pregunta 4: Descargas

Lo destacable de la encuesta es que un 68.1% de 160 estudiantes no hace análisis de descargas. Y se pueden observar los mismos sesgos del caso anterior: la obtención de contenido de manera rápida y sencilla bajo presión o una urgencia (heurística de disponibilidad); si es una página la cual tiene reseñas positivas por parte de diferentes usuarios puede que el usuario se sienta confiado en descargarlo también (sesgo de norma social); si se visita constantemente una página la cual ofrece diferentes servicios o productos para descargar y no ha tenido ningún problema, pueda que el usuario se sienta confiado en seguir usándolo (sesgo de resultado); tener la idea de que es poco probable que le suceda algo grave después de la descarga (sesgo de optimismo). A estos también se le puede unir el sesgo de anclaje debido a que el usuario pueda buscar “algo” en específico y quedarse con el primer resultado que se le presente, omitiendo el resto de las opciones que podrían ser más seguras.

Estos sesgos llevan a influir fuertemente en caer en un error de seguridad informática provocado por el usuario ya que la seguridad no es un objetivo principal para los usuarios, y es por eso que debido a la falta de conocimiento de los riesgos de un ataque cibernético y las consecuencias que esto le podría generar, con frecuencia para los usuarios es más fácil hacer caso omiso de los mecanismos de seguridad si esto facilita la obtención de su objetivo principal como podría ser la descargar de una archivo que es importante para él. Sin embargo, esto podría llevar al usuario a ser víctima de un ataque con malware como el más común que es el ransomware.

Pregunta 5: Contraseñas

Distintos sesgos cognitivos llegan influir en generar una potencial vulnerabilidad de seguridad cibernética, ya que le dan al usuario la ilusión de tener todo bajo control y estar correctamente protegidos utilizando una misma contraseña, que en la mayoría de casos ni siquiera cumple con los parámetros necesarios para considerarse una contraseña segura ya que utiliza información personal como la fecha de cumpleaños, nombres o nombres de mascotas, y dichos datos son los primeros que los atacantes buscan obtener por medio de ingeniería social y posteriormente descifrar mediante diversas técnicas. Dejando así expuesto al usuario a ser víctima de robo de información o suplantación de identidad. Esto podría ser mitigado haciendo uso de contraseñas fuertes con combinaciones de números, letras y símbolos, así como con el uso de un gestor de contraseñas.

Pregunta 6: Huella digital

Los sesgos cognitivos ejercen un impacto significativo en que tipos de rastros dejamos en Internet. Estos sesgos, como la ilusión de control, la sobre confianza, la norma social y otros, influyen en las decisiones que tomamos en línea de maneras a menudo sutiles pero importantes. Por ejemplo, la ilusión de control puede hacer que se subestimen los riesgos y se crea la falsa ilusión de que se es capaz de mantener nuestra información segura, lo que podría llevar a la elección de contraseñas débiles o a compartir datos sensibles sin precaución. La norma social puede influir en las acciones del individuo, haciendo que se siga comportamientos comunes en línea, incluso si no son los más seguros. La sobre confianza en habilidades de seguridad puede llevar a una falta de precaución y una sensación exagerada de invulnerabilidad en línea. Estos sesgos pueden contribuir a la creación de una huella digital que refleje la influencia de las percepciones sesgadas, lo que potencialmente pone en riesgo la seguridad y privacidad del estudiante en un entorno cibernético cada vez más complejo. Reconocer y abordar estos sesgos es esencial para tomar decisiones más informadas y proteger la identidad y datos personales.

Evaluación de desempeño de múltiples antivirus en un ambiente controlado

Como se puede observar el Cuadro 6 de Resultados, los 4 antivirus cumplieron con los objetivos de detectar la ejecución del virus y eliminarlo inmediatamente del sistema dado a que todos lo detectaron como un archivo potencialmente peligroso, además la detección que la página que redirigiría la pestaña de phishing no era de confiar y bloquearon el acceso a este. Lo cual es bueno dado a que esto significa que hay herramientas que son gratuitas y son capaces de detectar amenazas en las descargas y ejecución de programas que se pueden pasar por "inofensivos". Lo mismo en el caso de phishing, el cual estos programas son capaces de identificar si alguna página se está dirigiendo a un sitio web no confiable que puede ser una estafa o robo de información (esto se puede ver en la Figuras 42, 43, 45-48 de la sección de Anexos). Sin embargo, únicamente los antivirus AVG y Avast bloquearon el acceso a la página web que ofrecía contenido de paga de forma gratuita de manera inmediata (Figuras 42 y 43 de la sección de Anexos). Por otro lado, Kaspersky Standard permitió la entrada a la página, pero detectó y bloqueó una descarga de manera inmediata y bloqueaba cualquier sitio web de pestañas emergentes (Figura 44 de la sección de Anexos). Por último, el antivirus Bitdefender tuvo el peor desempeño durante esta escena, porque no bloqueó en ningún momento el acceso a la página, nunca detectó alguna descarga inmediata y no bloqueaba algunos de los sitios web que aparecían de manera espontánea en pestañas emergentes.

8.3. Discusión de resultados de la fase 2

8.3.1. Resultados de las pruebas de ataques

Prueba de open Wi-Fi

Para entender lo sucedido en la prueba de open Wi-Fi es importante destacar el hecho de que ninguna de las redes era realmente segura, incluyendo dentro de las redes maliciosas la red UVG Student", dado que en el campus de la universidad no existe ninguna red con ese nombre, sin embargo, fue la más elegida por los estudiantes, con el 100% de respuestas positivas, como la opción más segura a la cual conectarse entre el resto de redes (ver A.1). Esto puede ser resultado de un sesgo de autoridad, pues al ver el nombre de UVG los individuos lo asocian como algo de confiar, y esto se confirma en las justificaciones que dan los estudiantes luego de seleccionar dicha red (ver A.2) donde la mayoría indica que la han elegido por el mero hecho de que tiene el nombre de la universidad y eso les da más confianza.

Además, otra red común seleccionada entre los estudiantes fue la red del café que se encuentra en el campus con un 31% de respuestas positivas (ver A.1). Interesantemente, si bien esta no fue la más seleccionada, esta generó bastante interacción en las métricas del eye tracker. La Tabla 7.2 nos muestra que con un tiempo promedio de fijación de 0.84s, siendo esta la red en la que más tiempo se fijaron los estudiantes, aunque considerando que no es la que tiene más fijaciones en cantidad, puede haber sido porque el nombre tenía más caracteres y símbolos que el resto. La razón principal por la que esta red pudo haber sido altamente seleccionada, también pudo haber sido por el conocimiento previo de que los cafés suelen tener redes abiertas, creyendo por sesgo de autoridad que al ser el internet de una empresa reconocida su internet debería ser seguro (tal como lo indican en A.2), ignorando que el riesgo se encuentra en los otros individuos que también se conectan a dicha red.

Con respecto al flujo de la vista de los participantes, el eye tracker nos muestra que el flujo de atención fue el siguiente: un escaneo visual de las redes y posteriormente una fijación con alta atención en la red de UVG Student, esto nos dice que primero los estudiantes evalúan sus opciones y luego le prestan atención a la red en la que más confían. Dicho punto de atención en la red UVG Student es el punto de atención más alto en toda la visualización (ver B.1).

Detallando los datos destacables de los resultados de esta prueba pueden observarse en las columnas de Avg. TTFF de la Tabla 7.2 donde en primera instancia la red con el nombre del restaurante Go Green tiene el mayor tiempo de espera para que se haya realizado la primera fijación, con un tiempo de espera de 3 segundos, detrás de ella la red con el nombre de la universidad con 2.3 segundos y por último la red de café barista con 2.08 segundos. Esto indica que los estudiantes recurrieron de forma inmediata a observar las redes que no eran comunes con respecto a encontrarse en el entorno de la universidad.

Luego analizando la columna de Avg. Time Spent del mismo cuadro, se puede ver que los estudiantes se fijaron mucho más tiempo en las redes con el nombre de Claro, Go Green y Iphone de Rodrigo con 1.25, 1.01, 1.15 segundos respectivamente. Esto puede deberse a que encontraron interesantes o sospechosas estas redes debido a la inexistencia de las mismas en la universidad, mientras que la red con el nombre de la universidad y café barista tienen menor tiempo de fijación debiéndose a un sesgo de disponibilidad, dado a que toman la decisión de no fijarse en ellas, ya que se les hace conocidos los nombres.

Otros datos interesantes, abarcan la columna de Fixations de la Tabla 7.2. La red con más

fijaciones es la de Go Green con 30 fijaciones, segundo la red de Claro con 27 fijaciones y por último la red de Café Barista 26 fijaciones. Esto indica que los voluntarios pasaron el mayor tiempo de la prueba fijándose en estas redes comparado a las otras que tienen menos fijaciones con un tiempo menor a 0.40 segundos cada fijación como lo indica la columna Avg. Fixation Duration del mismo cuadro.

Analizando la columna de Gazes del mismo cuadro, se puede observar que las redes de UVG_Student, Go Green y Claro tuvieron una mayor cantidad de miradas y escaneo, confirmando que eran las que brindaban un mayor interés.

De esta forma, se hace evidente que el principal factor que influye en que los estudiantes sean víctimas de un ataque por open Wi-Fi, es su susceptibilidad al sesgo de autoridad y de disponibilidad. Aquí es pertinente realizar una aclaración, pues la sección anterior demostró que los estudiantes no eran demasiado susceptibles a ser víctimas de este sesgo, pero hay una diferencia crucial entre ambas situaciones y es la autoridad que toma papel en cada caso: en el caso de la sección anterior, la autoridad era un padre, mientras que en este caso la autoridad es una empresa o institución. Esto nos da a entender entonces el tipo de autoridad a la que los estudiantes suelen mostrar más sesgo y a cuáles más rechazo.

8.3.2. Prueba de password leak

Una gran vulnerabilidad encontrada en los estudiantes es que suelen acceder a recursos de la memoria para crear sus contraseñas, por ejemplo, utilizando el nombre de sus mascotas, fechas importantes entre otros, como se puede observar en la figura A.8, donde se ve una tendencia de utilizar fechas importantes, tu nombre o nombre de algún conocido, nombre de mascota y alguna actividad que les guste, estas con 23%, 15%, 8% y 23% respectivamente. Note que esta vulnerabilidad es altamente explotada por los crackers para vulnerar accesos. Y es que los estudiantes exponen que la razón de esto es porque utilizan contraseñas que sean fáciles de recordar, hacen uso de un atajo mental, además que la mayoría afirma que utilizan una misma contraseña para varias plataformas, confirmando un sesgo de anclaje, ya que los estudiantes al no verse vulnerados en un principio con dichas credenciales se aferran a una idea errónea de que esta es lo suficientemente segura como para ser descubierta y por lo tanto optan por utilizarla en la mayoría o todos los casos. Esto se refuerza con el hecho de que una gran parte, el 46%, de los encuestados, afirma que se sienten confiados en que su contraseña es lo suficientemente segura como para no ser vulnerada (ver A.11), lo cual claramente provoca en consecuencia un sesgo de Dunning-Kruger, que como se explicó en la sección anterior es de los que más influyen en la población, y este presenta un caso materializado de cómo los estudiantes caen en este tipo de efecto.

Es importante mencionar que en dado caso el estudiante reciba un ataque donde su contraseña de algún lugar se filtre, el atacante tendrá acceso a todas las cuentas vinculadas, por lo tanto, se considera una práctica peligrosa, pues puede perjudicar en gran medida a los usuarios como se menciona en (Samsung, 2023).

Volviendo al hecho de que la generación Z se ve envuelta en una gran variedad de plataformas digitales, es intuitivo pensar que busquen atajos mentales para crear credenciales para todos los accesos que utilizan en internet, pues de lo contrario aprenderse esa gran cantidad de contraseñas presupondría una gran carga mental. Es interesante observar que, a pesar de eso, una gran parte no explora alternativas de *passwords managers,* lo cual se ve relacionado al hecho de que la mayoría se siente confiado, por el sesgo de Dunning-Kruger, de que sus credenciales ya son seguras.

A la hora de ingresar sus credenciales, es interesante notar que los estudiantes se fijan en las

políticas de privacidad, de hecho, es el área al que más atención le pusieron como de ver en la Tabla 6.3, con un índice de atención de 0.8. La cuestión es que el hecho que le presten atención a dicha área no implica que en un contexto real se detuvieran a leer las políticas de privacidad de sus credenciales con detenimiento, pues la misma tabla nos demuestra que no hubo ningún evento de mouse sobre dicha área.

8.3.3. Prueba de phishing

La gran mayoría de los estudiantes logró identificar correctamente que había un correo sospechoso que no formaba parte de la institución como exponen en A.12. Sin embargo el eye tracker no mostró una diferenciación significativa entre las métricas de fijaciones o miradas de ese punto, únicamente una gran concentración de atención en al nombre del emisor del correo de phishing (ver B.4).

Lo preocupante de este caso, es que, dentro del correo, hubieron 9 clics (de 13 participantes, aunque hubieron clics repetidos por participante) en el link malicioso. Cabe destacar que el eye tracker no muestra que los participantes le hayan puesto atención especial al link, lo cual indica que para aquellas personas que no hicieron el clic, les bastó únicamente el emisor y el contenido del correo para identificar que era malicioso (pues fueron los AOI's con mayor nivel de atención, donde para el caso del emisor se obtuvo un índice de atención de 0.48, y para el caso del contenido, se tuvieron hasta 3880 miradas, lo que implica que lo estuvieron leyendo como se observa en B.5), esto es bueno considerando que muchas veces los links pueden ser procesados con *link shorteners* lo que dificulta decir a simple vista si un link es genuino o no. No obstante, para aquellos que, si hicieron clic en el link, implica que no están prestando suficiente atención a los componentes que dan alertas de riesgo en casos de phishing, y esto se ve reflejado en el 31% de los estudiantes que afirmó no identificó la amenaza, y el 15% que estuvo dispuesto a proceder con las instrucciones del atacante (ver A.4).

Esta falta de preocupación y atención puede implicar que los estudiantes se hayan visto sesgados por optimismo, creyendo que las probabilidades de que un correo malicioso le llegara directamente a el sería casi nula y por lo tanto no se esperan una amenaza en su bandeja de entrada. Este análisis propone refutar los resultados de la sección anterior sobre el sesgo de optimismo donde se presumía que era el sesgo al que menos propensos son los estudiantes, sin embargo hay que tomar en cuenta el hecho de que no fue la mayoría de los estudiantes los que clic en el enlace malicioso, sino que fue, como se mencionó anteriormente, el 31% de los estudiantes los que no identificaron la amenaza, y son estos estudiantes que estadísticamente no representan al resto de la población los más propensos a verse sesgados por optimismo.

En el caso de aquellos que hicieron clic en el link, no se puede afirmar que haya sido por la urgencia del mensaje, dado que ellos estaban conscientes de que se estaba realizando una simulación y por lo tanto no existiría ninguna necesidad real de cambiar sus credenciales.

8.3.4. Prueba de bait

Los resultados muestran que el punto de mayor atención en el ataque de bait fue el preview del archivo malicioso, con un índice de atención de 0.37 frente al resto de índices que se encuentran por debajo de 0 y tiene más tiempo promedio entre revisitas, con 1.33 segundos lo que indica que se volvió a visitar un par de veces y se tomó mayor tiempo para hacerlo. Además, el link recibió atención casi nula, con una cantidad de miradas que es menor entre los tres campos, con 188,

confirmando que fue en lo que menos se fijaron, lo cual es alarmante considerando que en esta situación es un gran indicio de las malas intenciones del emisor, indicando un sesgo de ilusión de seguridad, debido a que este parecía estar correcto por el formato del link, el cual parecía "verídico" desde un principio y resultó ser un link de una página no confiable.

Claramente al tomar esta decisión se manifestaron los sesgos de confirmación y de automatización. El sesgo de confirmación se activa, debido a que al observar por bastante tiempo lo que es el preview del libro, por sus experiencias pasadas observando contenido similar, generan confianza hacia este. El sesgo de automatización surge debido a que se confía en la aplicación de mensajería, pues a pesar de que el link tiene cambios, esta sigue mostrando el preview del libro, lo cual no debería de pasar si esta aplicación cuenta con medidas de seguridad.

El principal protagonista de que el 85% de los estudiantes fueran víctima de este ataque fue el sesgo de autoridad, pues como indica el 54% de los mismos en A.16, les ha dado confianza el hecho de que se haya enviado en el grupo de la clase donde están sus compañeros. Es importante aclarar que el para el sesgo de autoridad, la autoridad no necesariamente debe ser una persona u organización, sino que también puede ser un grupo de personas en quién deposito mi confianza por el mero hecho de ser quienes son, en este caso, sus compañeros son una imagen de autoridad entre ellos mismos, de forma que como estamos en el mismo contexto bajo los mismos objetivos (del curso), ellos tienen cierta autoridad de influir en mis decisiones. Este vuelve a ser otro ejemplo de cómo ciertas autoridades tienden a influir más que otras en la población estudiada, donde los compañeros de clase se suman al grupo de las organizaciones e instituciones en las que estos mismos confían sus decisiones.

Otro sesgo importante de mencionar es el sesgo de norma social, pues el aquí existe presión social de aceptar el archivo malicioso por el hecho de que los demás estudiantes lo han aceptado previamente. Por otro lado, la urgencia juega un papel crucial en este escenario, dado que el 54% de los participantes afirma que la motivación de descargar el archivo es que lo requieren lo antes posible para finalizar su tarea tal cual se estipula en el caso planteado.

8.4. Propuestas de seguridad

Dado los resultados de las pruebas podemos recomendar que los estudiantes eviten el uso de contraseñas débiles y predecibles, como secuencias numéricas sencillas, y en su lugar, utilicen contraseñas fuertes y únicas para cada cuenta. Deben adoptar la práctica de no reutilizar contraseñas entre diferentes servicios en línea para evitar que un posible compromiso de una cuenta ponga en riesgo otras. También es importante que cambien sus contraseñas regularmente y utilicen gestores de contraseñas seguros para facilitar la gestión de contraseñas fuertes y únicas.

Se recomienda que los estudiantes deben de ser cautelosos al conectarse a redes Wi-Fi públicas y, siempre que sea posible, utilizar redes seguras y de confianza, como las proporcionadas por la universidad.

Para proteger su privacidad y datos, es recomendable que utilicen una red privada virtual (VPN) al conectarse a redes Wi-Fi públicas. Esto cifrará su tráfico de Internet y reducirá el riesgo de que sus datos sean interceptados por posibles atacantes en la red.

En cuanto al phishing es vital que los estudiantes sean escépticos ante los correos electrónicos no solicitados y que eviten hacer clic en enlaces o descargar archivos adjuntos de remitentes desconocidos. Deben verificar la autenticidad de los remitentes y ser cautelosos ante correos que

prometen ofertas o premios sorprendentes.

Es altamente recomendable el mantener actualizado el software de seguridad y antivirus para detectar y bloquear correos electrónicos maliciosos. Además, que deben aprender a reconocer señales de correos electrónicos sospechosos, como errores de ortografía y gramática, así como remitentes desconocidos o direcciones de correo electrónico que no coinciden con las conocidas. Es fundamental verificar cuidadosamente la autenticidad de los correos electrónicos antes de tomar cualquier acción en respuesta a ellos, y deben informar inmediatamente de cualquier correo electrónico sospechoso a las autoridades de seguridad de la universidad.

Por último, los estudiantes deben desarrollar el hábito de verificar y confirmar la autenticidad de cualquier contenido en línea antes de interactuar con él, incluso si parece legítimo a primera vista. Esto significa detenerse y considerar si un mensaje, enlace o archivo adjunto coincide con sus expectativas antes de hacer clic o descargar.

También es importante que los estudiantes estén al tanto de las últimas tácticas de engaño en línea y se eduquen sobre cómo identificarlas para protegerse de posibles amenazas.

Para minimizar el impacto negativo provocado por ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques. Uno de los pasos más importantes en seguridad, es la educación.

Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas.

En cuanto a temas de UI/UX: Enseñar a los usuarios a cuestionar cambios inesperados en interfaces y a desarrollar una actitud de desconfianza constructiva y no asumir automáticamente la seguridad, incluso en entornos familiares. Modificar elementos del UI, en las listas de redes disponibles y diferenciar aquellas redes a las cuales ya no hemos conectado en el pasado. Considerar mejoras en la interfaz de usuario para resaltar visualmente elementos críticos que ayuden a los estudiantes a identificar correos sospechosos. Educar a los usuarios sobre las tácticas utilizadas en ataques de phishing, especialmente la replicación de elementos familiares como botones y formularios. Evitar el uso de librerías de componentes con elementos de UI genéricos a la hora de desarrollar aplicaciones web. Idear elementos de interfaz visual distintivos que aporten una experiencia única para los usuarios, dificultando así la capacidad de los atacantes para imitarlos.

CAPÍTULO 9

Conclusiones

- Se lograron cumplir los objetivos de la investigación: se implementaron amenazas informáticas controladas orientadas al ataque de sistemas de la información a los jóvenes para entender su respuesta cognitiva, se identificó efectivamente cuáles serían los ataques más comunes a los sistemas de información y los que con más frecuencia los estudiantes pueden ser víctimas, y se hizo la investigación de las recomendaciones y estrategias que más funcionan para la mitigación de estos ataques cibernéticos con justificación en los hallazgos cognitivos encontrados.
- Los individuos de la población del estudio son igual de susceptibles a sesgos independientemente de su información demográfica como edad, carrera, nivel académico, entre otros, por una parte, porque no hay mayor diferenciación entre la variedad de perfiles demográficos entre los estudiantes, y por otra parte porque una característica que la mayoría de los estudiantes comparten es la falta de capacitación seria sobre seguridad. El conocimiento sobre las medidas de seguridad necesarias para proteger la información en sus dispositivos electrónicos que presentan los estudiantes encuestados demuestra una necesidad de concientización y educación sobre amenazas cibernéticas y las medidas de protección disponibles.
- Los estudiantes en cuestión son muy susceptibles a los sesgos de confirmación, anclaje y Dunning-Kruger. Mientras que el sesgo de autoridad y optimismo son más moderados y presentan un menor riesgo para esta población. Estos son los sesgos que se utilizaron como referencia para el marco de análisis y efectivamente fueron los que más incidencia tuvieron en la respuesta de los estudiantes al realizar las pruebas controladas de los ataques, sin embargo, como se esperaba, durante la investigación surgieron otros sesgos que complementaron la perspectiva de los ataques de forma individual para la población estudiada, como lo fue el caso del sesgo de la norma social y urgencia en el ataque de bait.
- La principal razón por la que los estudiantes son víctimas de ataques de open Wi-Fi es por el sesgo de autoridad que tienen frente a la empresa que se supone provee la conexión a la red, de forma que una las redes que incluyen el nombre de una institución reconocida suelen verse como más confiables. En cuanto a la seguridad en redes Wi-Fi, es esencial que los estudiantes ejerzan precaución al conectarse a redes públicas y den preferencia a aquellas proporcionadas por la universidad. La implementación de una red privada virtual (VPN) se presenta como

una medida adicional para proteger la privacidad y los datos en entornos Wi-Fi públicos.

- Los estudiantes se ven influenciados de distinta forma por distintos tipos de figuras de autoridad. Bajo este contexto, las organizaciones, empresas, y compañeros de clase tienen más agencia en influir sobre las decisiones de estos que sus padres o tutores legales, aunque en otros contextos esto puede variar.
- Hay un gran riesgo en los estudiantes a ser víctimas de un password leak dado que utilizan atajos mentales para la creación y uso de sus credenciales, como el uso de fechas especiales, el nombre de su mascota, y patrones comunes que pueden ser fácilmente descifrados con un esfuerzo de ingeniería social.
- La mayoría de los estudiantes tiende a utilizar la misma contraseña para múltiples cuentas, lo que presenta sesgos de disponibilidad, anclaje y optimismo. Esto puede llevar a una falsa sensación de seguridad y aumentar la vulnerabilidad en caso de una brecha de seguridad en uno de los sitios vinculados a esa contraseña.
- En el caso de bait los sesgos de autoridad, rebaño, y la urgencia han llevado a los estudiantes a confiar en un archivo malicioso de un emisor al que no conocen, y no hubo ningún indicio de esfuerzos por evaluar la credibilidad del mismo.
- El phishing tuvo baja efectividad en los estudiantes, pero aun así hubo un 31% de los cuales fueron víctima por no prestar atención a los componentes clave que pueden dar indicios de peligro, esto como muestra de un sesgo de optimismo. En el ámbito de la seguridad en correos electrónicos, se debe ser precavidos al enfrentarse a correos no solicitados y enlaces desconocidos. Mantener actualizado el software de seguridad y antivirus también es importante para mitigar el riesgo, junto con la identificación de señales de posibles correos sospechosos, como errores gramaticales o remitentes desconocidos.
- El sesgo de confirmación es evidente en la mayoría de las pruebas y preguntas de la encuesta, ya que no consideran e ignoran señales de advertencia, características maliciosas u sospechosas a la hora de tomar ciertas decisiones.
- En el desarrollo y diseño de interfaces de usuario, se destaca la necesidad de mejoras específicas, desde resaltar visualmente elementos críticos que ayuden a identificar correos sospechosos hasta la implementación de prácticas que fomenten una actitud de alerta, se busca fortalecer la seguridad desde la experiencia del usuario.

CAPÍTULO 10

Recomendaciones

- Si bien para esta investigación se realizó sólo sobre una muestra diversa, una muestra mayor revelaría datos más precisos. Lamentablemente por cuestiones de recursos esto no fue posible en esta oportunidad.
- Como se plantea en la discusión de resultados, una excepción al análisis demográfico es los estudiantes con especialización en seguridad informática. Por lo tanto, en futuras investigaciones valdría la pena analizar por separado el sesgo de optimismo, extrema confianza y Dunning-Kruger sobre esta subpoblación bajo la hipótesis de que son igual de vulnerables al resto de estudiantes dado que suelen tener más confianza en sus habilidades de seguridad informática debido a su experiencia en el campo.
- Para la obtención de datos más precisos sobre los procesos cognitivos, se recomienda el uso de un encefalograma. Esto permitiría monitorear en tiempo real la actividad cerebral del participante para comprender de forma objetiva, y no del todo heurística como se realizó en el presente, las regiones del cerebro que se activan a ciertos estímulos y cómo eso se refleja en la toma de decisiones del individuo.
- Para mitigar la pérdida de atención de los participantes que puede ser producto de variables no controladas como estrés, falta de sueño, ansiedad, entre otras, se les puede ofrecer a los participantes té o café dependiendo de la necesidad del participante y medir su pulso y presión.
- Realizar más pruebas controladas con el apoyo de psicólogos para comprender mejor los sesgos.

CAPÍTULO 11

Bibliografía

7 types of cyber security threats. (2020, January). https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/.

Alanazi, M., Freeman, M., y Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*, 107376. doi: 10.1016/j.chb.2022.107376

Authy. (s.f.). *What is two-factor authentication (2fa)?* Descargado de https://authy.com/what-is-2fa/ (Retrieved October 31, 2023)

Bautista García, I. J. (2021, Mar). *Backend y frontend, ¿qué es y cómo funcionan en la programación?* servnet. Descargado de https://www.servnet.mx/blog/backend-y-frontend-partes-fundamentales-de-la-programacion-de-una-aplicacion-web

Belcic, I. (2023, January 19). *¿qué es el malware y cómo funciona? | definición.* Descargado de https://www.avast.com/es-es/c-malware (Retrieved October 31, 2023)

The bridge. (s.f.). https://www.thebridge.tech/blog/los-mejores-tipos-de-proteccion-contra-malware.

Chavez, J. (s.f.). *¿qué es un sistema informático? componentes, características y ejemplos.* https://www.ceupe.com/blog/sistema-informatico.html.

Continental, R. (2021, October). *En qué consiste el 'sesgo de automatización' que nos hace confiar en las máquinas.* https://www.continental.com.ar/sociedad/ en-que-consiste-el--sesgo-de-automatizacion--que-nos-hace-confiar-en-las-maquinas_a6171a5d74fc47c11dd35c5b2.

Cybersecurity for electronic devices. (s.f.). https://www.cisa.gov/news-events/news/cybersecurity-electronic-devices.

Definition of information (knowledge) assets - gartner information technology glossary. (s.f.). https://www.gartner.com/en/information-technology/glossary/information-knowledge-assets. (Retrieved February 25, 2023)

De Gregorio, M. (2021a, Jul). *Qué es ui o user interface.* OpenWebinars. Descargado de https://openwebinars.net/blog/que-es-ui-o-user-interface/

De Gregorio, M. (2021b, May). *Qué es ux o user experience.* OpenWebinars. Descargado de https://openwebinars.net/blog/ux-que-es/

de Normalización, O. I. (2016, December 16). *Iec 27004:2016 - information technology — security techniques — information security management — monitoring, measurement, analysis and evaluation.* Descargado de https://www.iso.org/standard/64120.html (Retrieved October 31, 2023)

de Normalización, O. I. (2022a, Agosto 1). *Iec 15408-5:2022 - information security, cybersecurity and privacy protection — evaluation criteria for it security — part 5: Pre-defined packages of secu-*

rity requirements. Descargado de https://www.iso.org/standard/72917.html (Retrieved October 31, 2023)

de Normalización, O. I. (2022b, Octubre 1). *Iec 27001:2022 - information security, cybersecurity and privacy protection — information security management systems — requirements*. Descargado de https://www.iso.org/standard/27001 (Retrieved October 31, 2023)

de Normalización, O. I. (2022c, Febrero 1). *Iec 27002:2022 - information security, cybersecurity and privacy protection — information security controls*. Descargado de https://www.iso.org/standard/75652.html (Retrieved October 31, 2023)

de Normalización, O. I. (2022d, Octubre 1). *Iec 27005:2022 - information security, cybersecurity and privacy protection — guidance on managing information security risks*. Descargado de https://www.iso.org/standard/80585.html (Retrieved October 31, 2023)

de Normalización, O. I. (2023, Junio 1). *Iec 27032:2023 - cybersecurity — guidelines for internet security*. Descargado de https://www.iso.org/standard/76070.html (Retrieved October 31, 2023)

Doan, M. (2020, Apr). *Ux design for cyber strategy*. Medium. Descargado de https://matthewdoan.medium.com/ux-design-for-cyber-strategy-9a60806c8c7c

Eldridge, S. (2016, August 1). *Confirmation bias | definition, examples, psychology, facts*. Descargado de https://www.britannica.com/science/confirmation-bias (Retrieved October 31, 2023)

Fitzgibbons, L. (2019, February 1). *States of digital data*. Descargado de https://www.techtarget.com/searchdatamanagement/reference/states-of-digital-data (Retrieved October 31, 2023)

Gate, R. (2021a). Practice and investigation of information security education with development of web-based learning materials at short-term educational institute. *ResearchGate*.

Gate, R. (2021b). Vulnerable young people and their experience of online risks. *ResearchGate*.

Hoover, A. M., Burden, S., Fu, X.-Y., Sastry, S. S., y Fearing, R. S. (2010). Bio-inspired design and dynamic maneuverability of a minimally actuated six-legged robot. En *Biomedical robotics and biomechatronics (biorob), 2010 3rd ieee ras and embs international conference on* (pp. 869–876).

INCIBE. (2020). *Glosario de términos de ciberseguridad*. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf. (Fecha de acceso: 21/10/2023)

Ingeniería social: Definición. (2018, October). https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering.

Internet security center | online protection | kaspersky. (s.f.). https://latam.kaspersky.com/resource-center.

is an information asset? | Information security, W. (2023, October 6). *What is an information asset? | information security*. Descargado de https://aptien.com/en/kb/articles/what-is-information-asset (Retrieved October 31, 2023)

Kim, C. (2016, April 19). *I am fine but you are not: Optimistic bias and illusion of control on information security*. Descargado de https://www.researchgate.net/publication/221599035_I_Am_Fine_but_You_Are_Not_Optimistic_Bias_and_Illusion_of_Control_on_Information_Security (Retrieved October 31, 2023)

Kumar, P. C., O'Connell, F., Li, L., Byrne, V. L., Chetty, M., Clegg, T. L., y Vitak, J. (2023). Understanding research related to designing for children's privacy and security: A document analysis. En *Proceedings of the 22nd annual acm interaction design and children conference* (p. 335–354). New York, NY, USA: Association for Computing Machinery. Descargado de https://doi.org/10.1145/3585088.3589375 doi: 10.1145/3585088.3589375

La guía esencial del malware: Detección, prevención y eliminación. (s.f.). https://www.avast.com/es-es/c-malware#:~:text=Malware%20es%20un%20t%C3%A9rmino%20general.

Li, P. (2022, July 19). *Availability bias: the tendency to use information that easily comes to mind*. Descargado de https://nesslabs.com/availability-bias (Retrieved October 31, 2023)

Mifsud, E. (2022, March 26). *MonogrÁfico: Introducción a la seguridad informática - seguridad de la información / seguridad informática*. Descargado de

http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1 (Retrieved October 31, 2023)

Mind, E. Y. (2021, June 18). *Social norms - biases, eflects, history, and examples.* Descargado de https://exploringyourmind.com/social-norms-biases-effects-history-and-examples/ (Retrieved October 31, 2023)

Morgan, L. (2021, November 1). *Authority bias: when we irrationally trust the judgement of experts.* Descargado de https://nesslabs.com/authority-bias (Retrieved October 31, 2023)

Mundo, B. N. (2020). *Generación z: Quiénes son los zoomers y por qué le causan dolores de cabeza a trump.* Descargado 2020-06-23, de https://www.bbc.com/mundo/noticias-53156753

Nadeem, M. S. (2022, Sep). *Ingeniería social: ¿qué es el baiting?* Mailfence. Descargado de https://blog.mailfence.com/es/que-es-baiting-ingenieria-social/

NICCS. (2023). *Explore terms: A glossary of common cybersecurity words and phrases.* Disponible en: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary. (Fecha de acceso: 19/10/2023)

Nikolopoulou, K. (2022, December 16). *What is anchoring bias? | definition examples.* Descargado de https://www.scribbr.com/research-bias/anchoring-bias/ (Retrieved October 31, 2023)

Nikolopoulou, K. (2023a, March 5). *What is conformity bias? | definition examples.* Descargado de https://www.scribbr.com/research-bias/conformity-bias/ (Retrieved October 31, 2023)

Nikolopoulou, K. (2023b, January 27). *What is optimism bias? | definition examples.* Descargado de https://www.scribbr.com/research-bias/optimism-bias/ (Retrieved October 31, 2023)

Nikolopoulou, K. (2023c, February 10). *What is recency bias? | definition examples.* Descargado de https://www.scribbr.com/research-bias/recency-bias/ (Retrieved October 31, 2023)

of Technology, M. I. (s.f.). *Information security asset risk level definition.* Descargado de https://security.calpoly.edu/content/policies/asset-risk-definition (Retrieved October 31, 2023)

Pastor, J. (2017, August). *Por qué es peligroso conectarse a wifis públicas y qué debes hacer para protegerte.* https://www.xataka.com/seguridad/por-que-es-peligroso-conectarse-a-wifis-publicas-y-que-debes-hacer-para-protegerte.

Public wifi risks and what you can do about it. (2023). Kaspersky. Descargado de https://usa.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

Qué es el sesgo cognitivo y por qué es importante en los negocios. (2020, January). https://www.brainvestigations.com/neurociencia/sesgo-cognitivo-negocios/#:~:text=Un%20sesgo%20cognitivo%20es%20una.

Qué es un virus troyano | definición de virus troyano. (s.f.). https://www.kaspersky.es/resource-center/threats/trojans.

Redes informáticas - concepto, tipos de red y elementos. (s.f.). https://concepto.de/redes-informaticas/.

Rodríguez, M. J. (2022, Mar). *Accesibilidad en ux: Experiencias de usuario para todas las personas: Blog.* Merkle. Descargado de https://www.merkle.com/es/es/blog/accesibilidad-ux-experiencias-usuario

Saeed, S. (2023). Education, online presence and cybersecurity implications: A study of information security practices of computing students in saudi arabia. *Sustainability*, *15* (12), 9426. doi: 10.3390/su15129426

Saideep, S. (2020, Nov). *Enhancing cybersecurity by providing better user experience.* The Startup. Descargado de https://medium.com/swlh/some-thoughts-and-ideas-blog1-d78e7237eac

Salahdine, F., y Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11* . doi: 10.3390/fi11040089

Seguin, P. (s.f.). *¿qué es el spyware? | definición de spyware.* Descargado de https://www.avast.com/es-es/c-spyware (Retrieved October 31, 2023)

Sesgos cognitivos: Tipos y descripciones. (2022, May). https://www.psyciencia.com/sesgos-cognitivos-tipos-y-

descripciones/#:~:text=Desde%20que%20fueron%20descritos%20por.
Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N., y Diakopoulos, N. (2016). *Designing the user interface: Strategies for eflective human-computer interaction* (6th ed.). Pearson.
Spam y phishing | amenazas asociadas a las estafas de phishing. (s.f.). https://latam.kaspersky.com/resource-center/threats/spam-phishing.
Stanleigh, M. (2011, March). *Risk management...the what, why, and how.* https://bia.ca/risk-management-the-what-why-and-how/.
Suplantación de identidad (phishing) y comportamiento sospechoso. (s.f.). https://support.microsoft.com/es-es/office/suplantaci%C3%B3n-de-identidad-phishing-y-comportamiento-sospechoso-0d882ea5-eedc-4bed-aebc-079ffa1105a3.
Taylor, H. (2021, June). *What are cyber threats and what to do about them.* https://preyproject.com/blog/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them.
Thorndike, E. L. (1932). Stimulus-response theory. *Journal of Educational Psychology* , *23* (6), 459–482.
Truitte, K. (2019). An unpatchable exploit: The human vulnerability in cybersecurity. *Georgetown Security Studies Review* .
Veksler, V. D., Buchler, N., LaFleur, C. G., Yu, M. S., Lebiere, C., y Gonzalez, C. (2020). Cognitive models in cybersecurity: Learning from expert analysts and predicting attacker behavior. *Frontiers in Psychology*, *11* . doi: 10.3389/fpsyg.2020.01049
Vicente, K. J., y Rasmussen, J. (1992). Ecological interface design: Theoretical foundations. *IEEE Transactions on Systems, Man, and Cybernetics*, *22* (4), 589–606.
Wang, Z., Sun, L., y Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE Access*, *8* , 85094-85115. doi: 10.1109/ACCESS.2020.2992807
¿qué es el adware? | definición de adware. (s.f.). https://www.avast.com/es-es/c-adware.
¿qué es el phishing? (s.f.). https://www.ibm.com/es-es/topics/phishing.
¿qué es el spyware? | definición de spyware. (s.f.). https://www.avast.com/es-es/c-spyware.
¿qué es la ciberseguridad? - explicación de la ciberseguridad. (s.f.). https://aws.amazon.com/es/what-is/cybersecurity/.
¿qué es un ciberataque? | definición de ciberataques. (2021, November). https://www.unisys.com/es/glossary/what-is-cyber-attack/.
¿qué es un virus informático? (s.f.). https://lam.norton.com/blog/malware/what-is-a-computer-virus.
¿qué son las amenazas informáticas y cómo protegerte de ellas? (2023, August). https://arrobasystem.com/blogs/blog/que-son-las-amenazas-informaticas-y-como-protegerte-de-ellas.
¿usas la misma contraseña en todas tus cuentas? enterate por qué no es recomendable y cómo evitarlo. (s.f.). https://news.samsung.com/ar/usas-la-misma-contrasena-en-todas-tus-cuentas-enterate-por-que-no-es-recomendable-y-como-evitarlo.

CAPÍTULO 12

Anexos

ANEXO A

Respuestas a las preguntas de las diapositivas del eye tracker

A.1. Respuestas a las preguntas de la prueba de open Wi-Fi

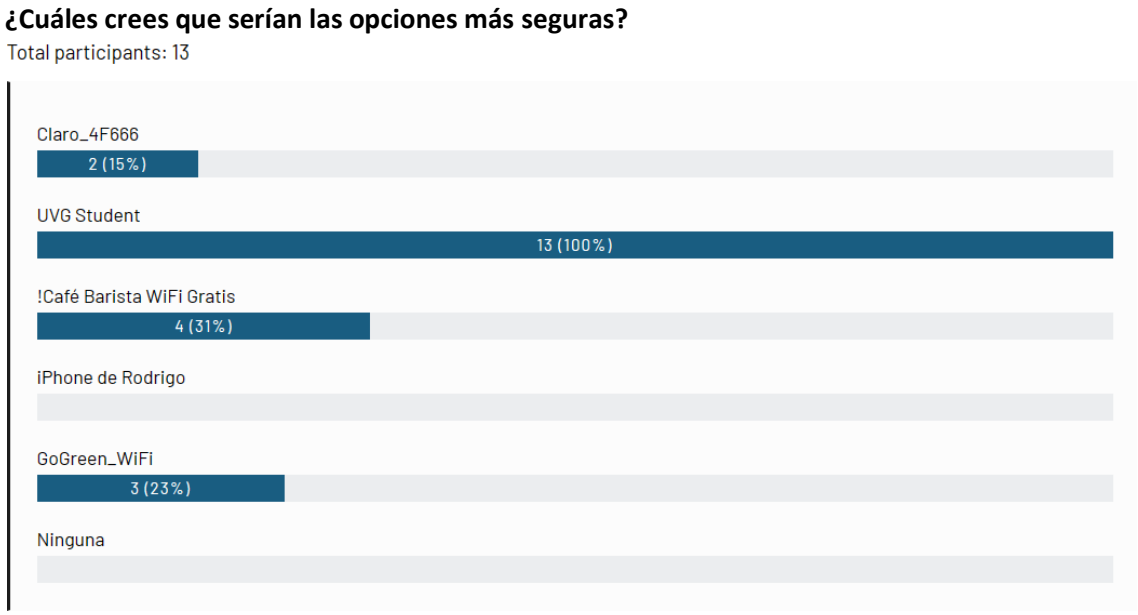


Figura A.1: Respuestas a la pregunta: "¿Cuáles crees que serían las opciones más seguras?"

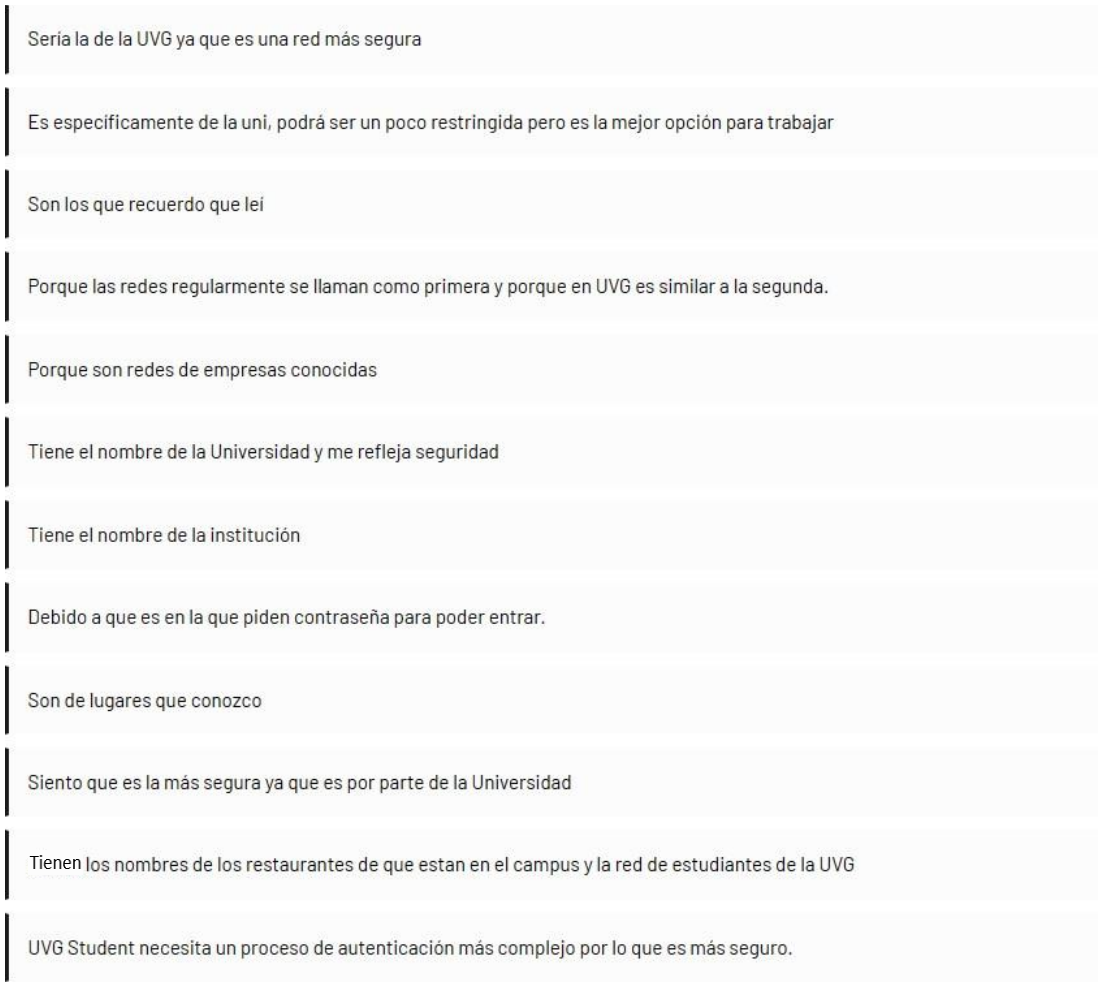


Figura A.2: Respuestas a la pregunta: "Justifique su elección"

Pregunta "¿Qué importancia le da a cada criterio para conectarse a la red?"

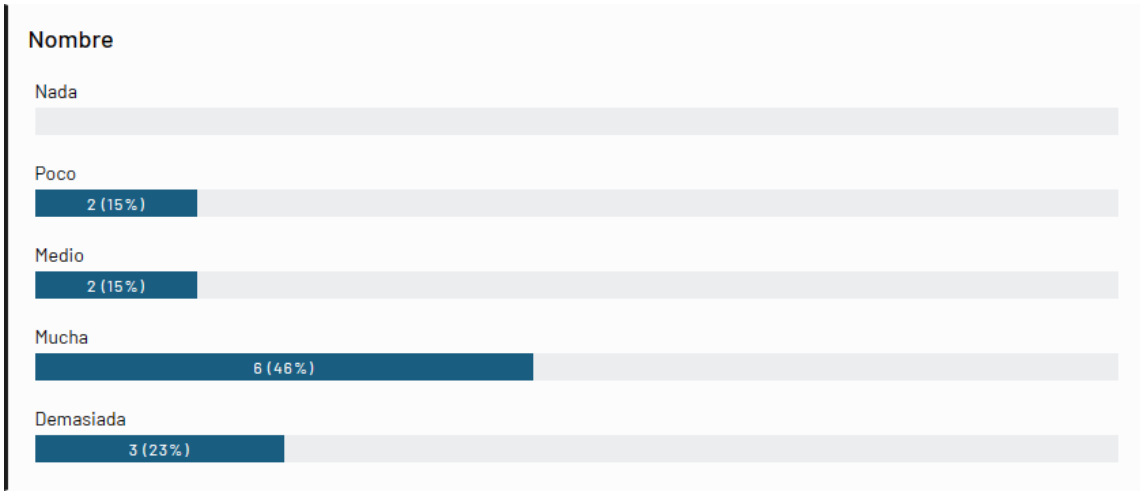


Figura A.3: Respuestas a la selección: "Nombre"

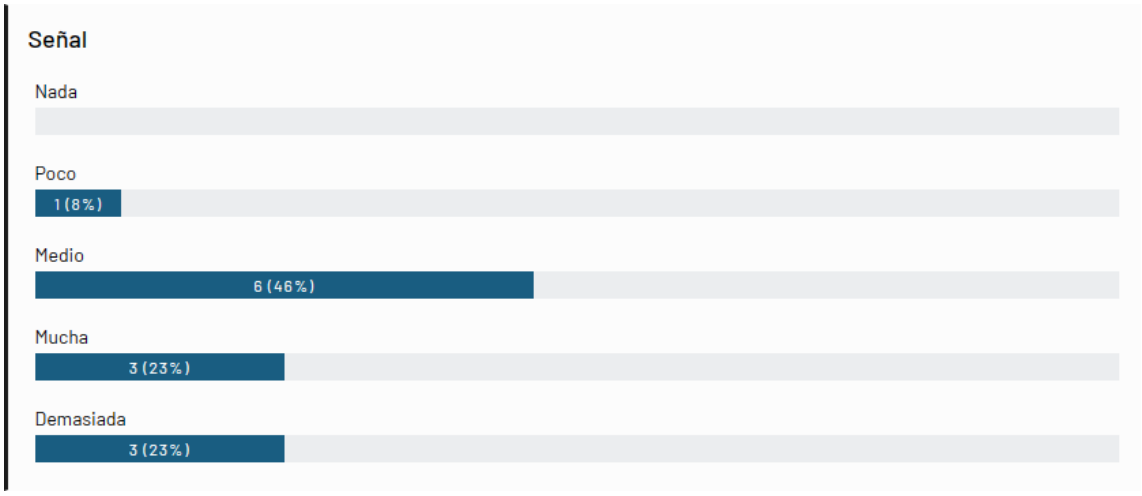


Figura A.4: Respuestas a la selección: "Señal"

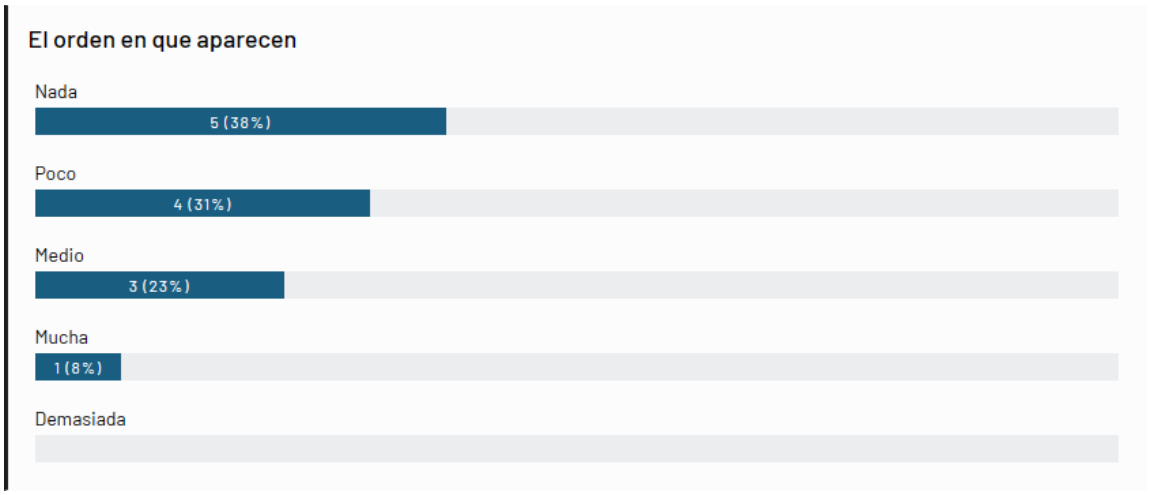


Figura A.5: Respuestas a la selección: “El orden en que aparecen"

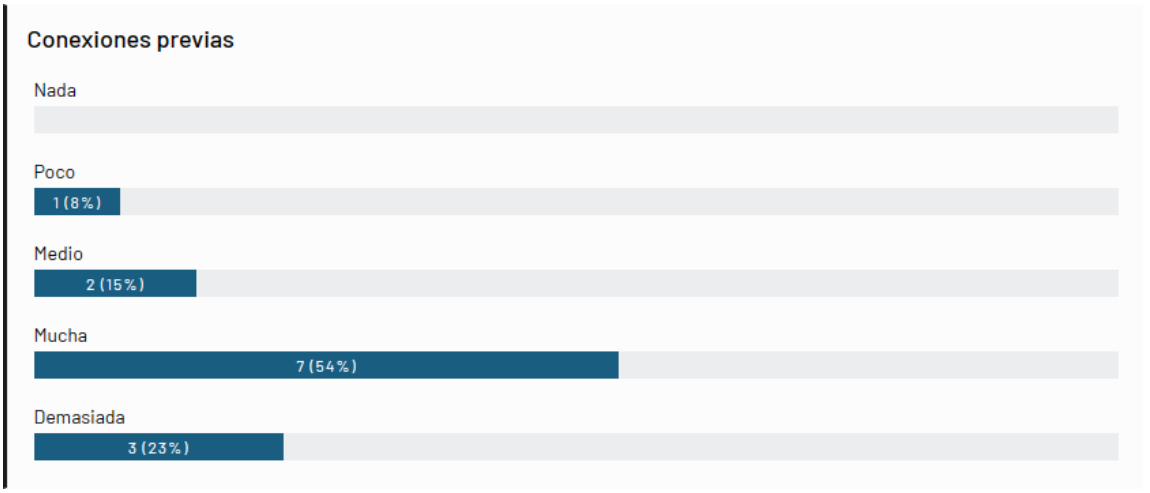


Figura A.6: Respuestas a la selección: “Conexiones previas"

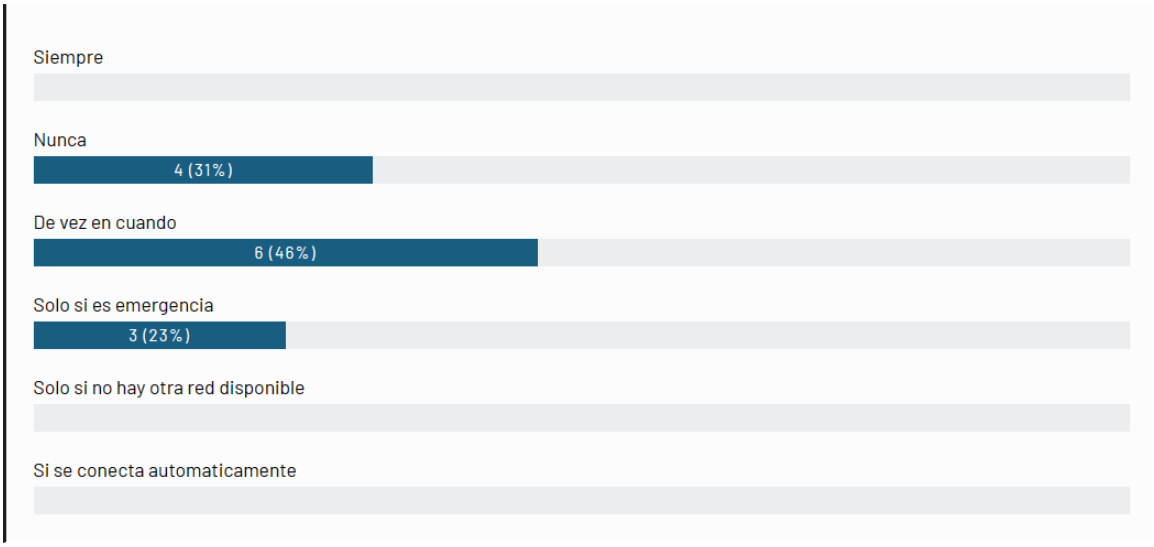


Figura A.7: Respuestas a la pregunta:"¿Usualmente se conecta a redes abiertas?"

A.2. Respuestas a las preguntas de la prueba de password leak

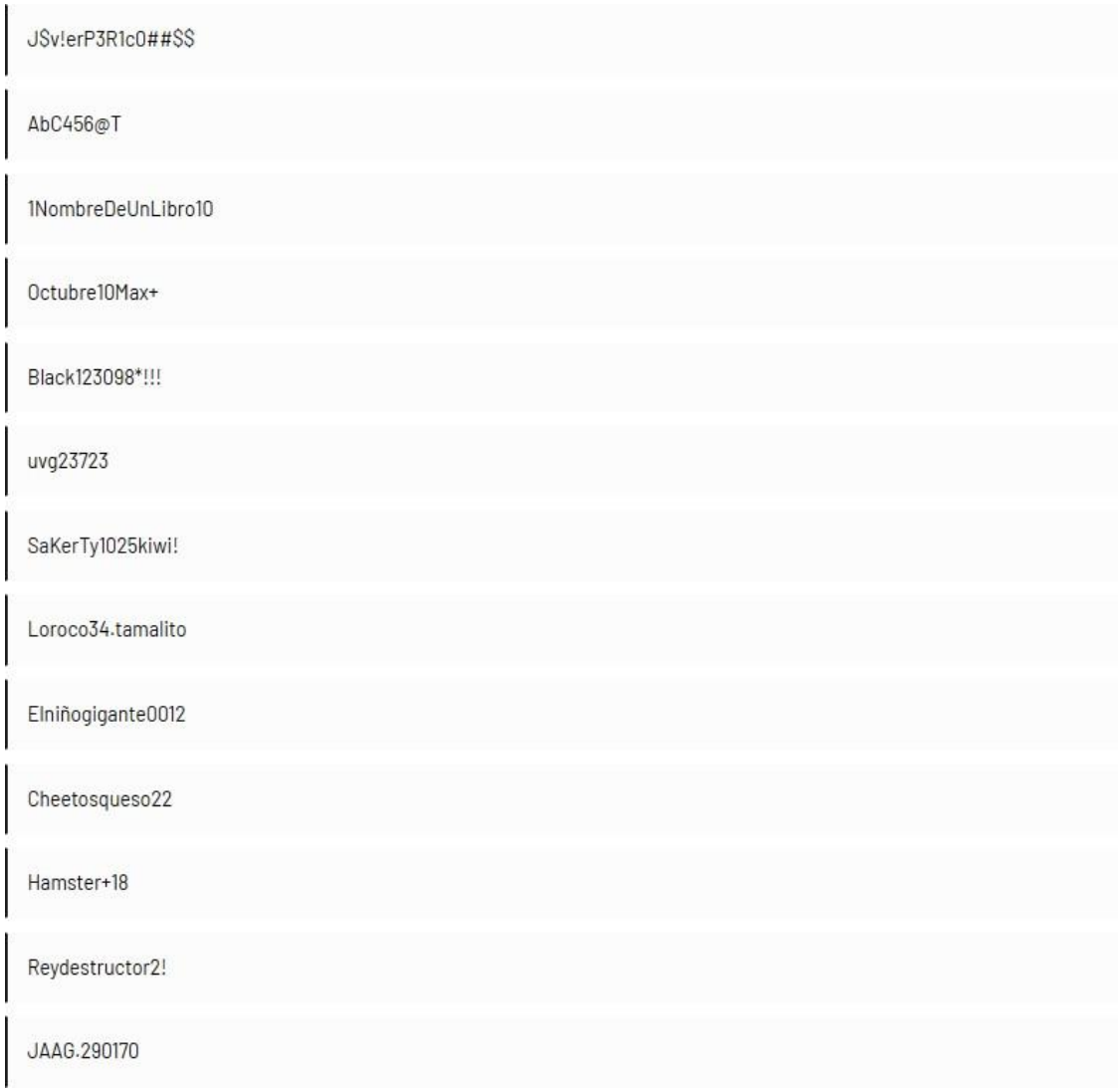


Figura A.8: Respuestas a la pregunta: “Escriba una contraseña que considere segura (no escriba credenciales reales o en uso)"

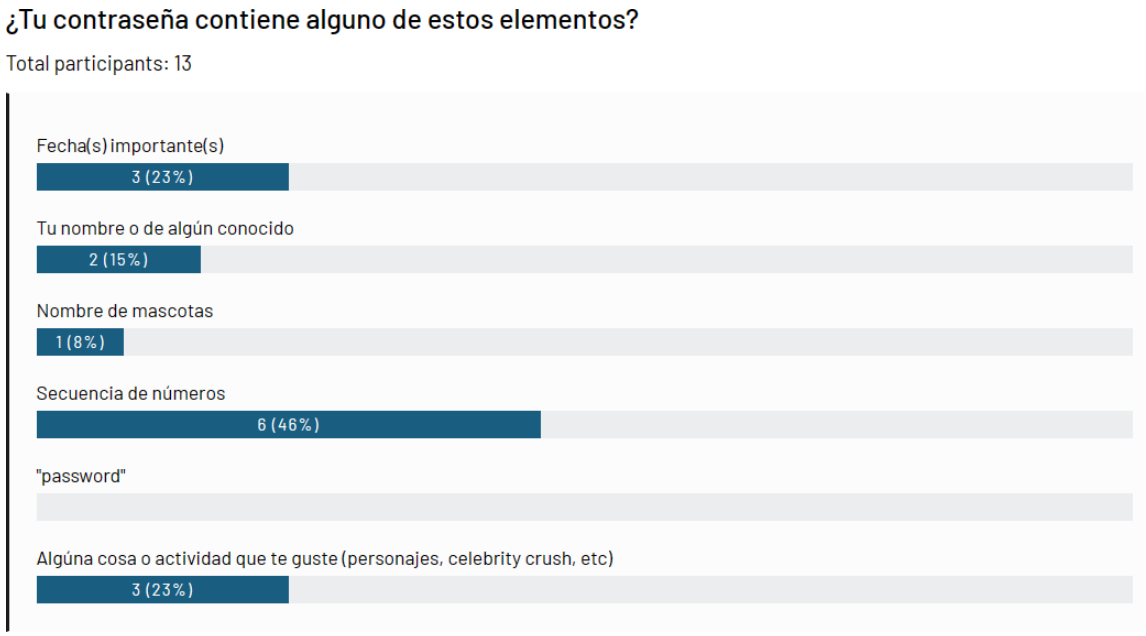


Figura A.9: Respuestas a la pregunta: "¿Tu contraseña contiene alguno de estos elementos?"

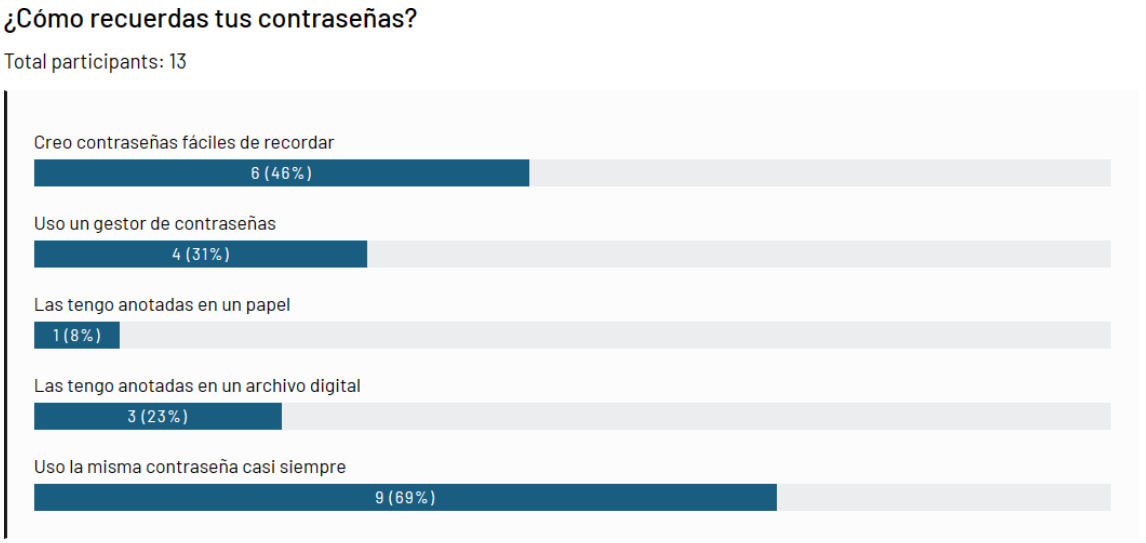


Figura A.10: Respuestas a la pregunta:"¿Cómo recuerdas tus contraseñas?"

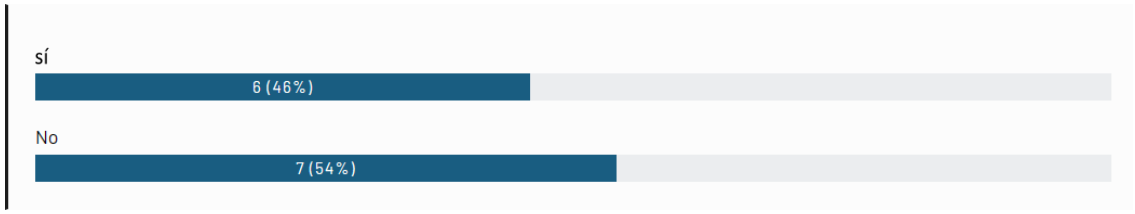


Figura A.11: Respuestas a la pregunta: "¿Cree que sus contraseñas son lo suficientemente seguras como para no ser descubiertas?"

A.3. Respuestas a las preguntas de la prueba de phishing en bandeja de entrada

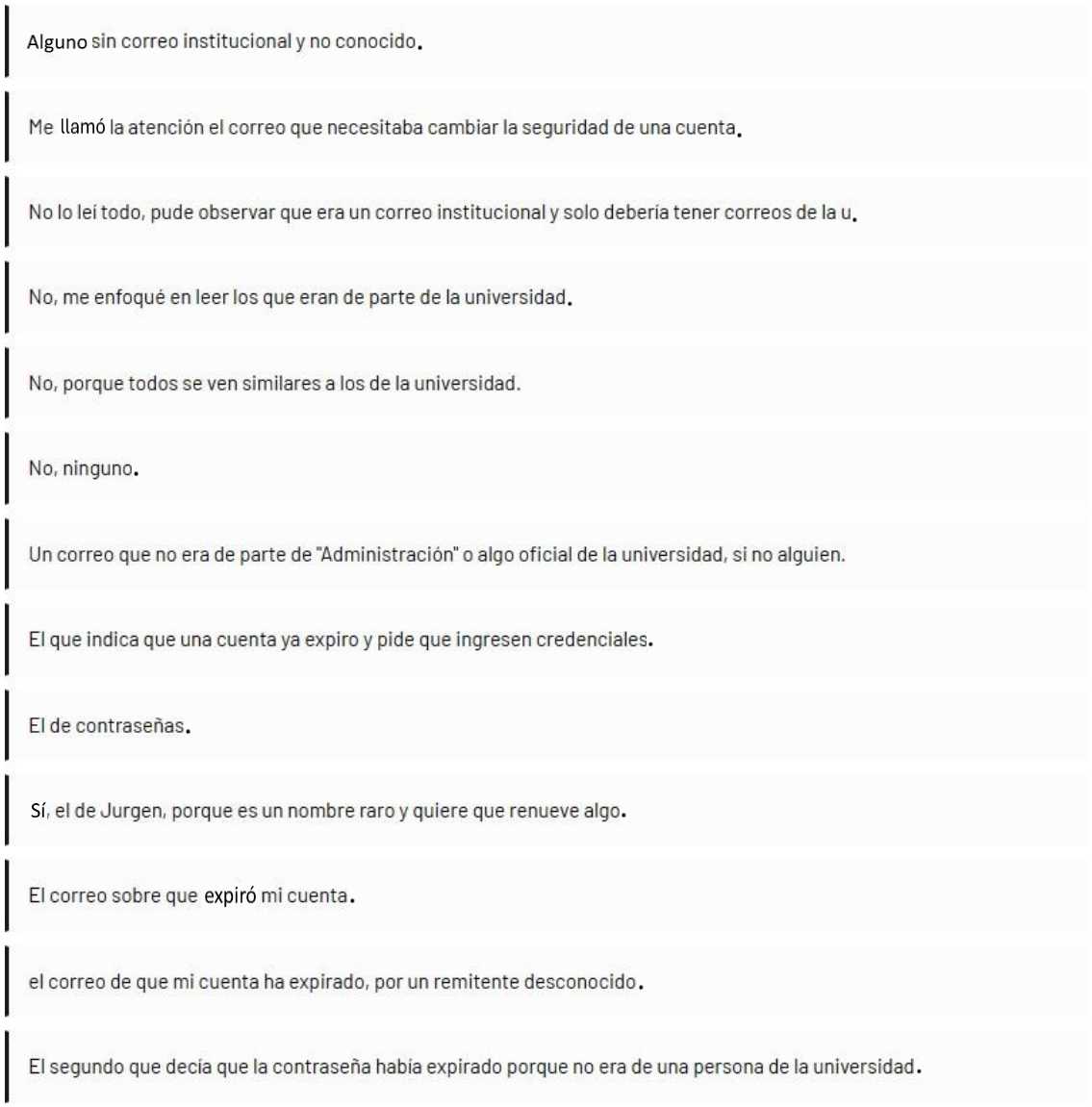


Figura A.12: Respuestas a la pregunta: "¿Algún correo llamó su atención por fuera de lo normal? Explique"

A.4. Respuestas a las preguntas de la prueba de phishing en contenido de correo

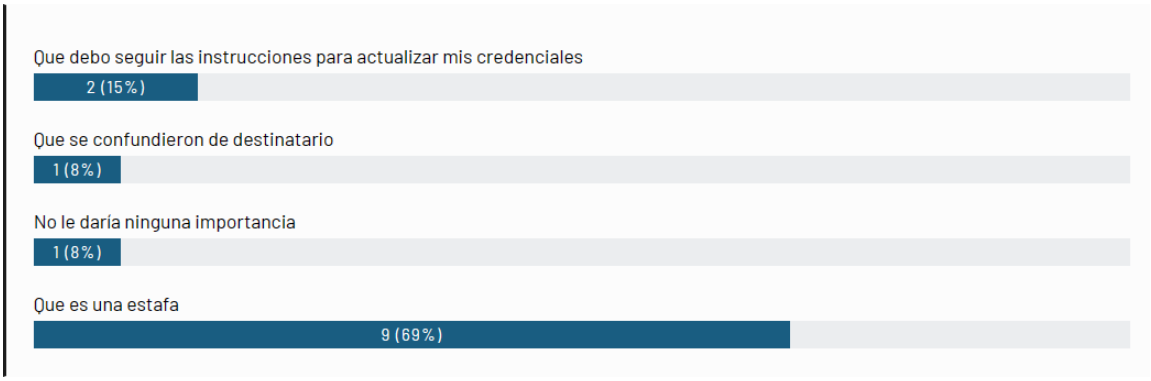


Figura A.13: Respuestas a la pregunta: "Si ese correo efectivamente le hubiera llegado a su bandeja de entrada, ¿qué pensaría al respecto?"

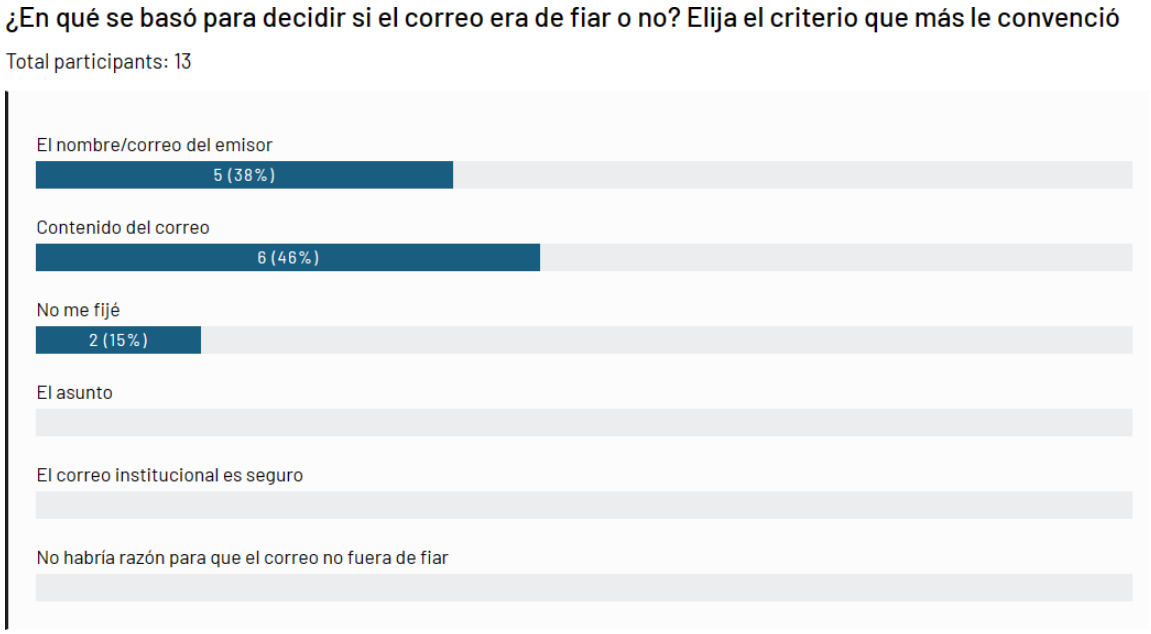


Figura A.14: Respuestas a la pregunta: "¿En qué se basó para decidir si el correo era de fiar o no? Elija el criterio que más le convenció"

A.5. Respuestas a las preguntas de la prueba de bait

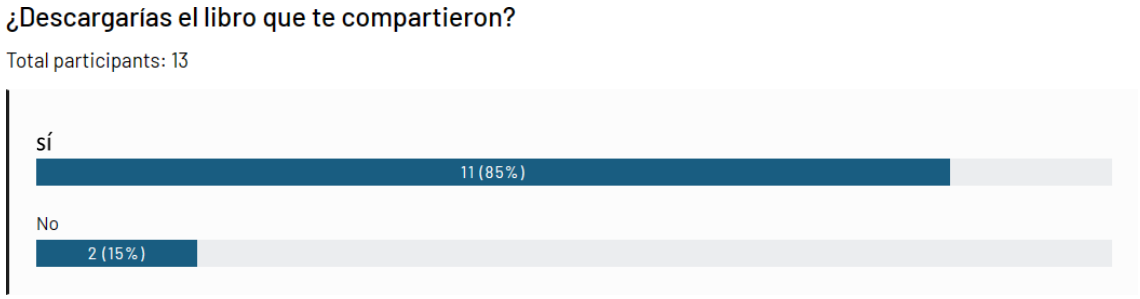


Figura A.15: Respuestas a la pregunta: "¿Descargarías el libro que te compartieron?"

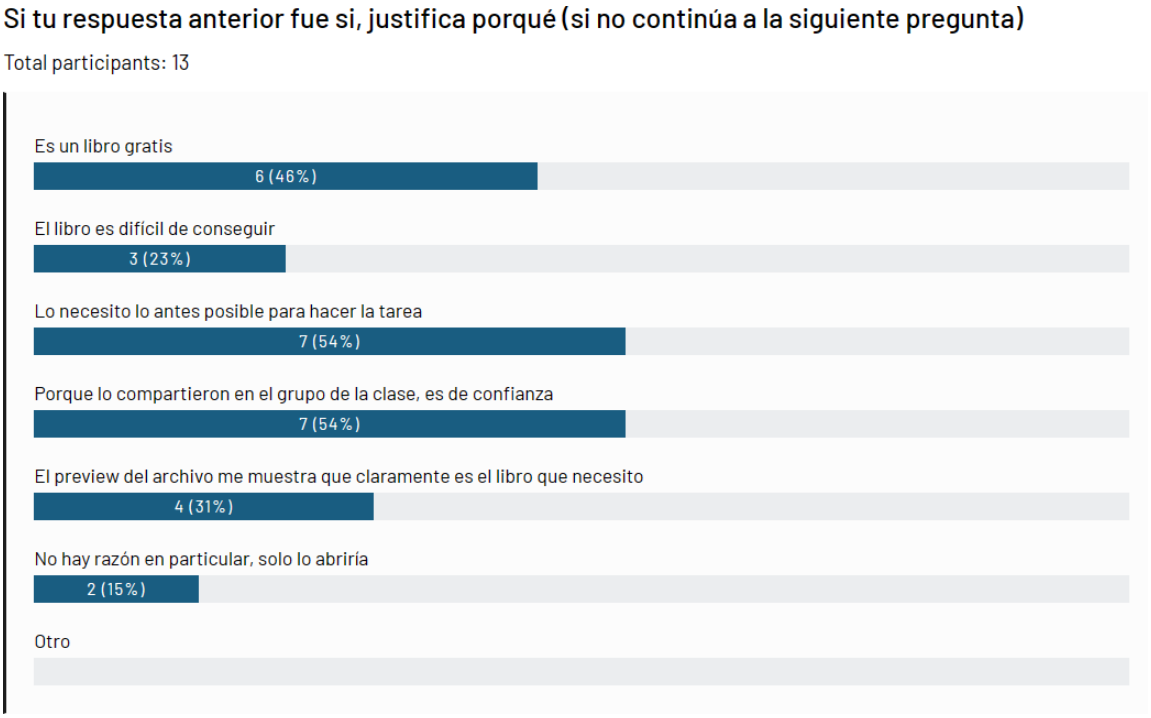


Figura A.16: Respuestas a la pregunta "Si tu respuesta anterior fue si, justifica porqué (si no continúa a la siguiente pregunta)"

Si su respuesta fue no, ¿por qué no lo abriría? (si su respuesta fue sí deje en blanco esta pregunta)

Total participants: 13

Figura A.17: Respuestas a la pregunta: "Si su respuesta fue no, ¿por qué no lo abriría? (si su respuesta fue sí deje en blanco esta pregunta)"

ANEXO B

Áreas de mayor atención en las diapositivas de las pruebas

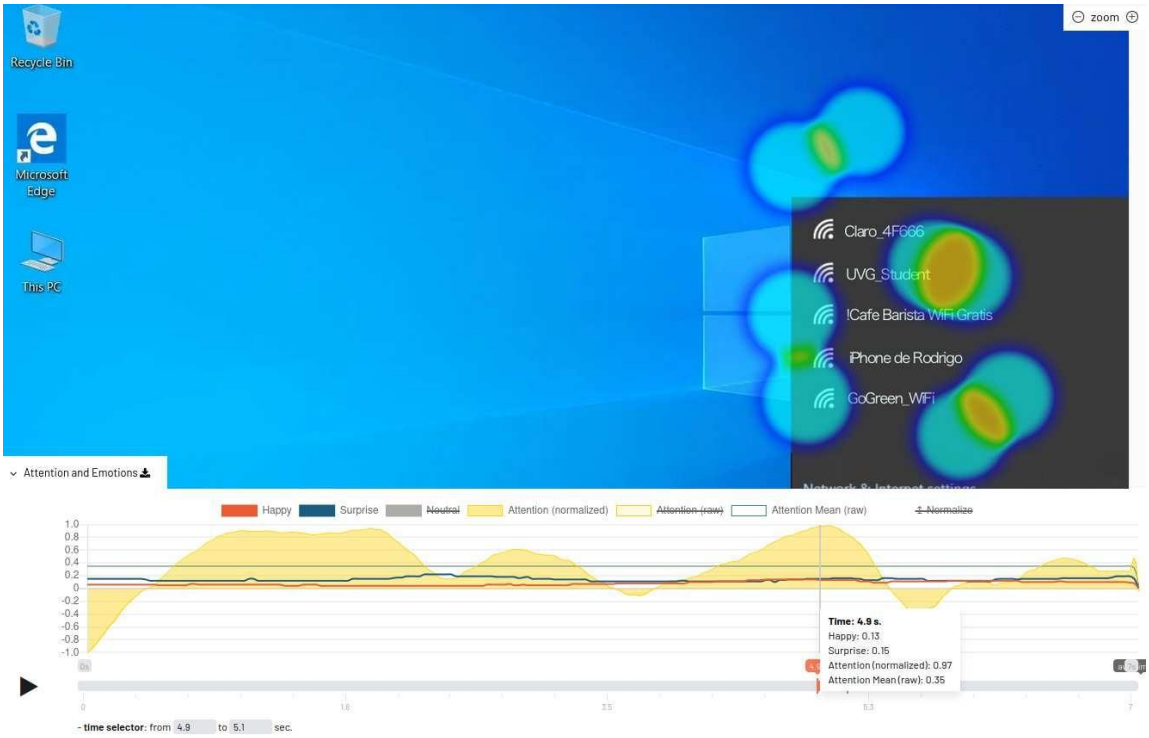


Figura B.1: Área de mayor atención en prueba de open Wi-Fi

Figura B.2: Área de mayor atención en prueba de password leak

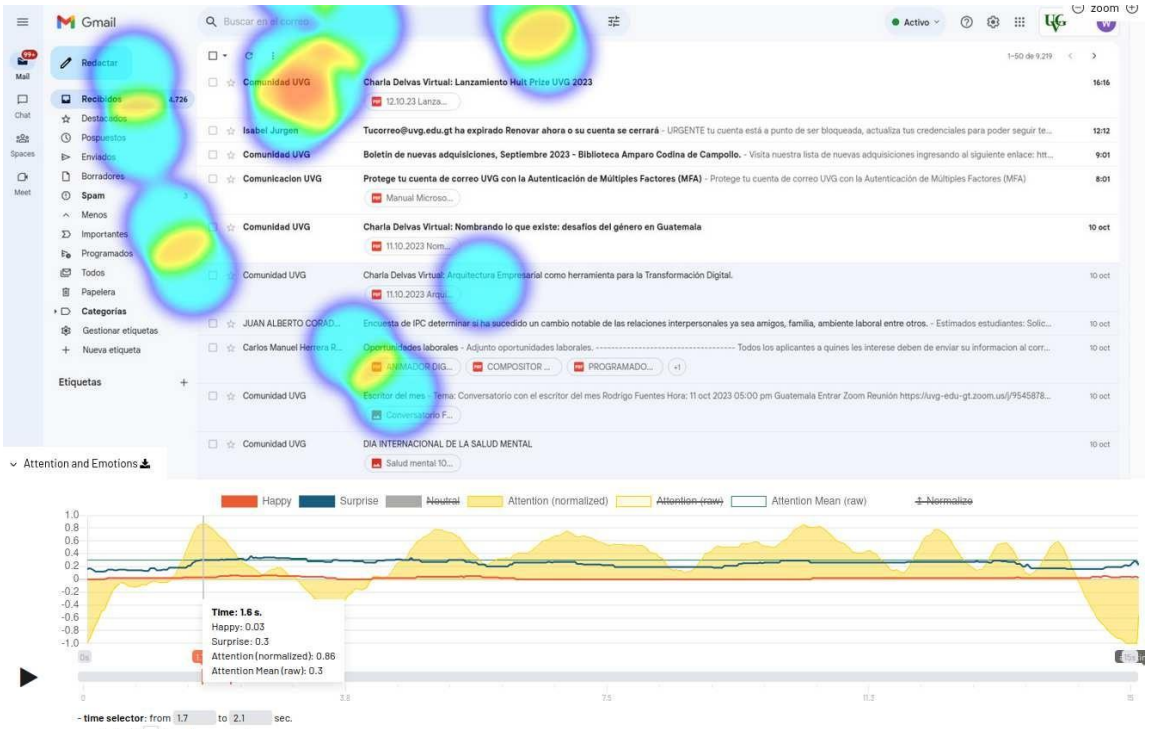


Figura B.3: Área de mayor atención en prueba de phishing en bandeja de entrada

Figura B.4: Atención en nombre del emisor en prueba de phishing en bandeja de entrada

Figura B.5: Área de mayor atención en prueba de phishing en contenido de correo

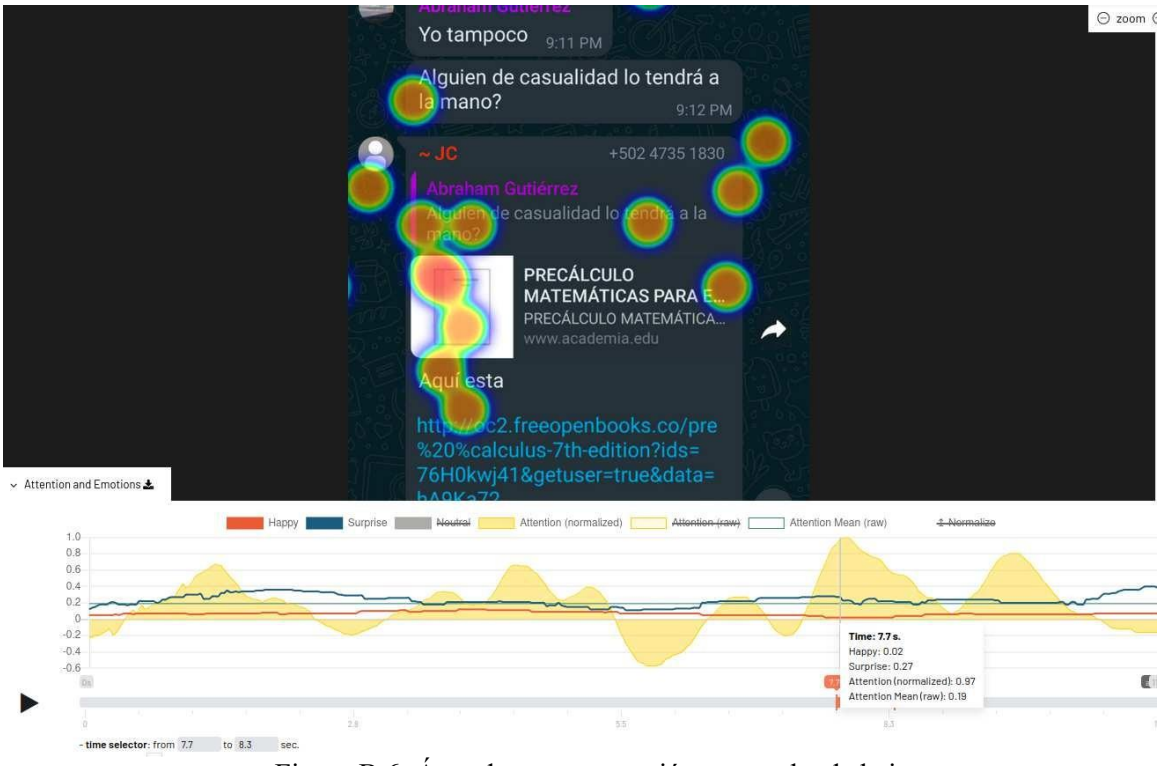


Figura B.6: Área de mayor atención en prueba de bait

ANEXO C

Glosario

AOI *Area Of Interest:* herramienta analítica que permite calcular medidas cuantitativas del movimiento ocular. Se selecciona un límite alrededor de un área de una imagen elegida de interés y se mostraran las métricas. 36

AOI Size: AOI se refiere a "Area of Interest". El tamaño de AOI puede mostrarse como un porcentaje del total de estímulos en RealEye. Esto se refiere al tamaño relativo del área dentro del contenido visualizado que está siendo observado o analizado. 51

Attention: La atención es un proceso cognitivo que nos informa sobre la concentración de alguien y su capacidad para procesar activamente información específica. En el contexto del seguimiento ocular, la atención se refiere a parámetros del movimiento ocular (duración de la fijación y amplitud de la sacada) para definir la trayectoria de la dinámica de atención de una persona examinada. 51

Avg. FFD: FFD se refiere a "First Fixation Duration". Esta métrica mide la duración de la primera fijación en un área de interés (AOI). 51

Avg. Fixation Duration: Esta métrica se refiere a la duración promedio de las fijaciones en un área de interés (AOI). Una fijación se considera válida para el rango de tiempo AOI si ha comenzado exactamente cuando comienza el rango de tiempo AOI o después, y si ha comenzado antes del final del rango de tiempo AOI. 51

Avg. Revisits: Promedio de veces que el participante devuelve la mirada a un AOI en particular, al haber sido visto anteriormente. 51

Avg. TTFC: TTFC se refiere a "Time to First Clic". Esta métrica mide el tiempo promedio que tarda un usuario en hacer el primer clic en un área de interés (AOI). 51

Avg. TTFF *Average Time To First Fixation:* Tiempo promedio que les tomó a los participantes fijarse en un AOI primera vez. 51

Avg. TTFG: TTFG se refiere a “Time to First Gaze”. Esta métrica mide el tiempo promedio que tarda un usuario en mirar por primera vez un área de interés (AOI). 51

Clics: Las interacciones del usuario con el contenido visualizado, como hacer clic en ciertas áreas o elementos. RealEye.io puede rastrear los movimientos y clics del mouse. 51

fijación *Fixation:* evento en el que el usuario detiene su mirada enfocándose en un punto en particular. 51

Fixations Avg. Time Spent: Métrica del eye tracker que indica el tiempo promedio que los participantes dedicaron a fijarse en un AOI. 51

Fixations Ratio: Proporción de participantes que se detuvieron a fijarse en el AOI. 51

Gazes Avg. Time Spent: Esta métrica se refiere al tiempo promedio que los usuarios pasan mirando un área de interés (AOI). 51

Gazes Ratio: Proporción de participantes que miraron el AOI. 51

Mirada *Gaze*: evento continuo en que el usuario recorre la pantalla con su vista sin detenerse en algún punto en particular. 51