UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

Maestría en

PSICOLOGÍA CON MENCIÓN EN INTERVENCIÓN CLÍNICA INDIVIDUAL Y GRUPAL

RPC-SO-05-NO.156-2021

Opción de Titulación:

Informes de investigación

Tema:

Estudio de los sesgos cognitivos en el proceso de toma de decisiones, en la detección de correos phishing en profesionales de ciberseguridad de la ciudad de Quito

Autor(es)

Daniel Badillo Santos

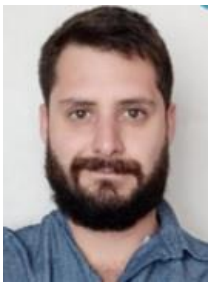
Director:

María Fernanda Cazares Zabala

QUITO – Ecuador

2023

Autor(es):



Daniel Andrés Badillo Santos
Psicólogo
Candidato a Magíster en Psicología con mención en intervención
Clínica Individual y Grupal por la Universidad Politécnica Salesiana
Sede Quito
andres.badillo@hotmail.com

Dirigido por:

María Fernanda Cazeres Zabala
Psicóloga Clínica
Magíster en Psicoterapia Integrativa
mcazares@ups.edu.ec

DANIEL ANDRÉS BADILLO SANTOS

ESTUDIO DE LOS SESGOS COGNITIVOS EN EL PROCESO DE TOMA DE DECISIONES, EN LA DETECCIÓN DE CORREOS PHISHING EN PROFESIONALES DE CIBERSEGURIDAD DE LA CIUDAD DE QUITO.

DECLARATORIA DE RESPONSABILIDAD

Yo, Daniel Andrés Badillo Santos, Candidato a Magíster en Psicología con Mención en Intervención Clínica Individual y Grupal por la Universidad Politécnica Salesiana – Sede Quito, declaro que soy el autor del "Estudio de los sesgos cognitivos en el proceso de toma de decisiones, en la detección de correos phishing en profesionales de ciberseguridad de la ciudad de Quito." En tal virtud, los conceptos desarrollados, el estudio y el análisis realizado, las encuestas elaboradas, aplicadas y practicadas; así como, las conclusiones establecidas y materializadas son de mi exclusiva responsabilidad.

Quito, D.M. 27 de abril de 2023

Psc. DANIEL ANDRÉS BADILLO SANTOS

DEDICATORIA

Dedico este trabajo a mis padres, a mis hermanos y a todas las personas que hacen de mi vida más llevadera con su amor, su apoyo incondicional y su presencia ya que me dan confianza y se constituyen en mi soporte permanente. También, dedico este trabajo a quienes han sido víctimas de correos phishing que cuenten con una guía para afrontar este problema.

Podemos estar ciegos para lo evidente, y ciegos además para nuestra ceguera.

¨

Daniel Kahnema¨

AGRADECIMIENTOS

Llegar a alcanzar una meta, más, en la vida es importante pues conlleva la culminación de un esfuerzo que da un importante fruto que a uno le permite crecer, profesionalmente, pero especialmente, como individuo y ser humano. Nunca en este caminar nos encontramos solos o sin un acompañamiento, siempre hay personas buenas que nos quieren y ayudan a avanzar brindándonos su aliento, sus consejos y su guía, a todas ellas mi más sincero agradecimiento.

No obstante, debo primero expresarles mi amor y gratitud a mis padres Manuel y Zenaida por estar siempre a mi lado alentándome, acompañándome y facilitándome los medios necesarios para mi preparación académica y siempre creyendo en mí lo que me hace motivarme y creer, igualmente, en todo lo que hago y sueño obtener.

En segundo, lugar a mis maestros de la Universidad Politécnica Salesiana por sus sabias enseñanzas y su entereza al orientarnos en cada una de las materias que nos impartieron, en este curso de formación en intervención clínica, tanto como en la parte del aprendizaje en grupo donde pude inter actuar y conocer más a mis compañeros quienes son excelentes profesionales y me permitieron el alcanzar a ser más flexible en mis forma de pensar y analizar los conceptos y conocimientos sobre psicología; Mención especial merece mi tutora de tesis, doctora María Fernanda Cazares, quien con sus conocimientos, talento, generosidad, paciencia e inteligencia me dirigió en la elaboración del presente trabajo hasta culminarlo exitosamente.

Mi gratitud y reconocimiento, a la par, a mi querido amigo Erick Espinoza quien estuvo, de manera permanente, alentándome para que culmine mi trabajo y dándome sus consejos y orientaciones siempre valiosas. También, mi gratitud a mi profesor Patricio Arias quien me ha encaminado y ha orientado en muchos temas de la psicología y me ha invitado a participar en Neurocorp. Sin duda, no puedo dejar de agradecer a la vida que ha puesto tantas personas y profesionales buenos en mi camino y me ha colmado de oportunidades.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Estudio de los sesgos cognitivos en el proceso de toma de decisiones, en la detección de correos phishing en profesionales de ciberseguridad de la ciudad de Quito.

Autor:

Daniel Badillo Santos.

RESUMEN

En la actualidad el término phishing se usa, ampliamente, en los medios tradicionales, las redes sociales y la literatura científica. Es un delito que emplea tanto la ingeniería social como un subterfugio técnico para robar los datos de identidad, las contraseñas y las credenciales de las cuentas financieras de los consumidores.

La muestra lo conformaron 44 profesionales de ciberseguridad de la ciudad de Quito. A los cuales se les aplicó el test de sesgos cognitivos, reflexibilidad cognitiva y phishing. Posteriormente, se realizó el análisis de correlación entre estas variables, obteniendo una alta asociación entre estas. Concluyendo que las características del perfil cognitivo de los usuarios de internet influyen en la tarea de detección de correos phishing.

Palabras clave: Sesgos cognitivos, Correo tipo phishing, Toma de decisiones.

ABSTRACT

Currently, the term phishing is widely used in traditional media, social networks and scientific literature. It is a crime that employs both social engineering and technical subterfuge to steal consumers' identity data, passwords and financial account credentials.

The sample was made up of 44 cybersecurity professionals from the city of Quito. To which the test of cognitive biases, cognitive reflexivity and phishing was applied. Subsequently, the correlation analysis between these variables was carried out, obtaining a high association between them. Concluding that the characteristics of the cognitive profile of Internet users influence the task of detecting phishing emails.

Keywords: Cognitive biases, Phishing email, Decision making.

INTRODUCCIÓN

El phishing es un ciberataque basado en la ingeniería social, cuyo objetivo es robar datos confidenciales, como números de tarjetas de crédito, credenciales de inicio de sesión y contraseñas. La mayoría de las veces, el atacante registra una dirección de dominio falsa, diseña un portal de internet que imita, cuidadosamente, el sitio web real de una organización y envía un correo electrónico masivo a miles de personas para inducir a que los destinatarios que lo reciben hagan clic en un enlace de la página web falsa. Estos tipos de correos electrónicos aplican diferentes tipos de amenazas, asustan a los usuarios o utilizan información ficticia para lograr que las personas realicen algunas acciones que los atacantes desean. El resultado de esta inducción es que los cyber delincuentes redirigen a los usuarios a una página web diseñada para sustituir al portal real y original haciéndose pasar por esa página de inicio de sesión (Alper et al., 2023).

Actualmente, el término phishing se usa, ampliamente, en los medios tradicionales, las redes sociales y la literatura científica. Es un delito que emplea tanto la ingeniería social como un subterfugio técnico para robar los datos de identidad, las contraseñas y las credenciales de las cuentas financieras de los consumidores. Además, es un acto malicioso, escalable de engaño mediante el cual se utiliza la suplantación de identidad para obtener información de un objetivo o alcanzar un beneficio (Torre et al., 2020).

Un ataque de phishing generalmente se caracteriza por los siguientes tres aspectos: Una entidad legítima es suplantada. Se utiliza un sitio web para el proceso de suplantación de identidad. Se solicita y recupera información confidencial (Fan et al., 2020).

Estas herramientas dan como resultado principalmente la pérdida de información confidencial del cliente, pérdidas financieras, la pérdida de propiedad intelectual (PI) y el debilitamiento de la confianza y la seguridad nacional. La cantidad de ataques de phishing aumentó particularmente después de la pandemia de la enfermedad por coronavirus 2019 (COVID-19) (es decir, a mediados de marzo de 2020), y los ataques utilizaron los temas de COVID-19 contra instalaciones y más en los trabajadores de atención médica. Alrededor del 70 % de los ataques de atención médica se dirigieron a instalaciones que tienen menos de 500 empleados porque estas pequeñas instalaciones probablemente tienen sistemas de seguridad

más débiles debido a los presupuestos de seguridad más pequeños (Jing, 2021). Por tanto, es de gran importancia tener un nivel de conocimiento de los sesgos cognitivos debido a que esto depende en la toma de decisiones de los profesionales de ciberseguridad **ya que esto tiene gran influencia en los correos phishing. Además, que toda la información con la que se cuenta es de gran significancia debido a que en este sentido las decisiones pueden ser tomadas bajo certeza o con determinados riesgos.**

La psicología es fundamental en el estudio de phishing porque este tipo de ataques se basa en la manipulación de las emociones y la conducta humana para engañar a los usuarios y obtener información confidencial.

En este sentido, la psicología es fundamental para comprender cómo los usuarios perciben y procesan la información que reciben a través de los medios digitales, **cómo toman decisiones** en situaciones de incertidumbre y cómo se ven afectados por factores como la confianza, el miedo o la curiosidad. Estudiar estos aspectos es clave para diseñar estrategias efectivas de prevención y educación que permitan a los usuarios reconocer y evitar los ataques de phishing.

En resumen, la psicología es esencial en el estudio del phishing porque permite entender cómo los usuarios reaccionan ante los ataques de phishing y cómo los atacantes manipulan y explotan las debilidades humanas para obtener información confidencial.

CAPÍTULO I

1. PROBLEMA DE INVESTIGACIÓN

1.1. Antecedentes

El Phishing es un ataque informático en el cual el atacante, a través de técnicas de ingeniería social, explota a sus víctimas para el robo de su identidad y demás datospersonales. La forma tradicional de funcionamiento del phishing es mediante el envío de un correo electrónico falsificado, que imita un correo electrónico legítimo de bancos, subastas, sitios de premios o sitios de pago para guiar a los usuarios a una página web falsa que está diseñada de forma tan detallada que se parece al sitio original (Aleroud & Zhou, 2017).

El objetivo central de esta práctica maliciosa, que actualmente es muy frecuente, es recopilar datos confidenciales e información personal entre las que se encuentran nombres de usuario, contraseñas, números de tarjetas de crédito o débito, datos bancarios e incluso dinero, haciéndose pasar por una entidad legítima. Este tipo de ataquecibernético suele ser muy exitoso porque los usuarios en su mayoría no son conscientes de las vulnerabilidades que tienen o no comprenden los riesgos que ello implica (Desolda et al., 2021).

Los estudios que tratan de comprender los factores humanos que intervienen en el phishing también han ido en aumento a nivel mundial y regional para determinar los mecanismos mentales de los usuarios que son propensos a estos ataques tomando como base la psicología cognitiva, **aunque su vasta investigación haya sido desarrollada en su mayoría desde las ciencias de la computación e informática** (Cano, 2019). Esta ciencia cognitiva tiene comoobjeto de estudio los fenómenos mentales, con mayor énfasis en los mecanismos involucrados en el procesamiento de información, desde la percepción, la memoria y el aprendizaje hasta la toma de decisiones, la planeación de acciones y la generación de la conducta (Aleroud & Zhou, 2017).

A partir del abordaje de todos estos conceptos se puede determinar que los ciberataquesno son nada sencillos y se basan en una compleja ingeniería social que busca explotar las debilidades en las funciones cognitivas humanas, esos puntos infalibles en que la mayor cantidad de usuarios son víctimas potenciales. Una defensa exitosa ante estos ciberataquesrequiere conocer a profundidad los aspectos propios de la cognición humana que son más vulnerables y con ello crear

estrategias que minimicen o mitiguen el daño (Montañez et al., 2020). Sin embargo, uno de los problemas a los que se enfrentan se debe a que no solo mejoran los sistemas de detección o seguridad, sino que a la par también mejora la efectividadde las tecnologías utilizadas en estos ataques de ingeniería social. Una de las posibles explicaciones para ello es que la investigación se ha centrado en detectar o comprender los ataques desde un enfoque tecnológico, sin tener en cuenta que su éxito puede depender dela poca comprensión sistemática de los componentes psicológicos implicados (Gordon, 2022).

Algunas de las estrategias planteadas para tratar de conocer más a los usuarios, así comosus debilidades, han sido trazar modelos computacionales de todos los procesos cognitivos para hacer experimentos y simulaciones en ciberseguridad como una forma de mejorar la toma de decisiones para hacer más seguras las redes computacionales, es decir, un modelado cognitivo en base a cada usuario o atacante que se va actualizando con el tiempoen función del comportamiento registrado (Veksler et al., 2018). Algunas estrategias de los usuarios que tienen algunos conocimientos sobre estos ataques de ingeniería social han sidoel estar alerta a errores ortográficos en los correos electrónicos, tipo de información que les solicitan y si es muy confidencial, cambio en los datos personales que antes no les habían solicitado y demás tácticas fraudulentas que se pueden utilizar como medio de robo de información (Abroshan et al., 2021). Sin embargo, recalcan que en algunas situaciones es muy difícil estar alerta por la cantidad de información que se revisa a diario debido a actividades laborales o académicas, inclusive por la forma tan camuflada en que suelen esconderse estos ataques.

Latinoamérica no ha sido la excepción, así como ninguna región del mundo, por ello se han aplicado diversas estrategias de seguridad cognitiva como el uso de bigdata, machine learning y analítica de datos encaminados a mejorar los tiempos de respuesta de la detecciónde ataques. En consonancia con estos datos el estudio de Ortiz-Garcés et al., (2019) presentan en su investigación un análisis del comportamiento anómalo relacionado con los ataques web de phishing y en qué forma las técnicas de aprendizaje automático pueden aplicarse para enfrentarse a este problema o que minimicen su impacto (p. 366). Este y otros enfoques de la academia han sido muy elaborados y efectivos para combatir los ataques de ingeniería social, todos deben conocerlos por su importancia pero que

lastimosamente la gran mayoría de usuarios los ignoran o simplemente no son conscientes de sus vulnerabilidades, por ende, no hacen nada por protegerse.

Una de las posibles soluciones necesarias y más relevantes para la seguridad de los usuarios en internet es trazar perfiles de usuarios susceptibles o que suelen ser víctimas de este tipo de ataques repetidamente, desarrollar programas informáticos que permitan asesorar y capacitar a estos usuarios de forma general y ayudarles a abordar este problema de seguridad para que sean más eficientes en la detección de ataques de phishing. Una de las estrategias que han propuesto García y Padilla (2022) es un marco centrado en el usuario que tiene como base cuatro perspectivas: socio-psicológica, habitual, socio-emocional y perceptiva; combinados en un solo modelo que facilite una compresión global de la susceptibilidad del usuario (p. 1). Con estas estrategias lo que se busca es evitar que los ciberdelincuentes se aprovechen de la brecha débil, fácil y vulnerable de los usuarios, e incluso de grandes empresas o corporaciones, que puede ser explotado a través de los diversos métodos de ingeniería social, que no solo afectan a los correos electrónicos sino también en páginas webs fraudulentas, las redes sociales y aplicaciones de mensajería instantánea.

Se ha explicado y escrito bastante sobre el peligro que conllevan estos ataques fraudulentos a través de los correos electrónicos donde los ciberdelincuentes utilizan diversas estrategias para obtener datos confidenciales pero muy poco sobre la vulnerabilidad que los mismo usuarios tienen al tener constante interacción en las redes sociales, donde no hace falta utilizar métodos para robar información personal y se la puede obtener sin mucho esfuerzo debido a que son los mismos usuarios los que comparten su información personal completa, fotografías, información familiar, etc., de forma voluntaria, sin darse cuenta del peligro inminente que esto representa. Por esta razón los modelos de predicción y modelado tomando como referencia las propias perspectivas del usuario se están tornando como las soluciones más efectivas a aplicar. Uno de los modelos que han sido desarrollados incluyen interacciones entre diferentes factores orientados a las redes sociales, nivel de participación, motivación para usar la red y la competencia o conocimiento para hacer frente a las amenazas de cada red social (Albladi & Weir, 2018).

Lo necesario en cuanto a estos ataques de robo de información es tomar en

cuenta los perfiles de los usuarios, la interacción y las actividades realizadas en internet para tratar de predecir un ataque basado en ingeniería social, pero sobre todo fortalecer la seguridad cognitiva que va orientado específicamente desde la psicología cognitiva en base a como el cerebro procesa la información y como se aplica en el comportamiento del usuario en internetpara mejorar las estrategias de protección.

1.2. Justificación

Los sesgos cognitivos son importantes y necesarios en nuestro día a día al momento detomar las decisiones, mismas que también tienen un componente emocional. Están inmersosen cada acción que realizamos, en cada decisión sea esta pequeña o muy grande.

Es por ello que se recalca la importancia de este tipo de investigaciones donde se puedencrear estrategias, modelos, perfiles y enfoques para que las personas estén protegidas mientras navegan por internet y realizan cualquier actividad. Debido a que estamos conectados todos los días debido a las actividades en general. Si se pueden aportar con datospara mejorar la vulnerabilidad de los usuarios en nuestro país y región encaminados en proteger el bigdata que vamos creando constantemente.

Este al ser un importante tema de investigación hay poca información al respecto desde en nuestro país, lo es aún más desde la psicología tomando en consideración que se considera un tema que se aborda de las ciencias computacionales y la informática, con sistemas que suelen considerarse complejos por su aprendizaje continuo, pero también presentan fallos. En escasas ocasiones se toma en consideración el factor humano que interactúa con estos sistemas para poderlos ejecutar correctamente. Tampoco se ha tomado la importancia necesaria que tienen la forma en que estos sistemas influyen en el comportamiento humano sin que las personas se den cuenta.

Al haber retroalimentación constante no se toman en cuenta muchos factores al momento de navegar en internet, sin embargo, debería ser una de las actividades en las cuales más nociones y conocimientos se deben tener para tener seguridad. Otro dato que también se debe considerar es que cada vez las personas que acceden a internet tienen edades más cortas o avanzadas, desde pequeños niños

hasta ancianos que tienen conocimientos al respecto, peor aún una guía de sitios maliciosos a los que no deben entrar o información quedeben o no compartir. Algo que los convierte en objetivos fáciles de estafar. Con esto se pueden brindar estrategias modeladas cognitivamente para asesorar y capacitar a los usuarios en general.

Los sesgos cognitivos cuando son utilizadas heurísticas y se llegan a rápidas conclusiones, los individuos pueden llegar a tomar equivocadas decisiones o decisiones que se desvían de la racionalidad. Los ciberdelincuentes elaboran ataques de ingeniería social personalizados que explotan el sesgo cognitivo, según un nuevo informe de Security Advisor, que utiliza el aprendizaje automático para personalizar la capacitación de concientización sobre seguridad para empleados individuales.

El sesgo cognitivo hace referencia a los atajos mentales que los humanos toman inconscientemente al procesar e interpretar información antes de tomar decisiones. El sesgo es un intento de simplificar el procesamiento de la información para acelerar la toma de decisiones y puede explotarse de manera efectiva en ataques de phishing, dijo a VentureBeat el director ejecutivo de SecurityAdvisor, Sai Venkataraman. Los ciberdelincuentes manipulan los pensamientos y las acciones de un destinatario para convencer a esa persona de que participe en un comportamiento arriesgado, como hacer clic en un enlace en el que normalmente no haría clic o ingresar información confidencial en un sitio web (Butavicius et al., 2015).

Los correos electrónicos de phishing son correos electrónicos enviados con intenciones maliciosas que intentan engañar a los destinatarios para que proporcionen información o acceso al remitente. Por lo general, el remitente se hace pasar por una entidad legítima y manipula el correo electrónico para tratar de persuadir al usuario para que realice una acción. Esta acción puede implicar revelar información sensible (por ejemplo, contraseñas) y / o proporcionar acceso inadvertidamente a su computadora o red (por ejemplo, a través de la instalación de malware) (APWG, 2014). En una encuesta reciente de organizaciones australianas, el incidente de seguridad más común reportado (45%) fue el de los empleados que abrieron correos electrónicos de phishing. Mientras que los costos financieros de tales ataques cibernéticos en 2013 se estiman en la asombrosa cifra

de 5900 millones de USD, también hay una variedad de otras consecuencias negativas para las organizaciones que pueden ser simplemente como perjudicial. Estos incluyen daños a la reputación, pérdida de propiedad intelectual e información sensible y la corrupción de datos críticos (Alavi et al., 2015).

1.3. Objetivos

1.3.1. Objetivo General

- Identificar los sesgos cognitivos predominantes que influyen en la toma de decisiones y detección de los ataques de ingeniería social al momento de identificar correos tipo phishing.

1.3.2. Objetivos Específicos

- Establecer el tipo de relación que existe entre los sesgos cognitivos y la detecciónde ataques cibernéticos basados en ingeniería social.
- Definir los usuarios con un buen nivel de detección de los ataques cibernéticos y sus características cognitivas, del proceso de toma de decisiones.
- Evaluar a los usuarios que presentan más vulnerabilidades a través de tareas de ensayo-error para establecer un perfil cognitivo que modele dichoscomportamientos.
- Desarrollar un modelo de estrategias enfocadas en la capacitación y asesoramiento a los usuarios para mejorar la detección y toma de decisiones antelos distintos ciberataques de tipo phishing.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Sesgos cognitivos

2.1.1. Definición

Los investigadores en este campo han tenido en cuenta varios aspectos de los factores relacionados con la cognición. Uno de los subconjuntos de factores cognitivos es el concepto de errores cognitivos (Gomroki et al., 2021). Los sesgos cognitivos son aquellos que le pueden ocurrir a todas las personas al juzgar y tomar decisiones por limitaciones cognitivas, factores motivacionales o adaptación al medio y condiciones situacionales. Al analizar, interpretar y juzgar los hechos, estos errores atrapan a los individuos y les impiden poder evaluar adecuadamente la situación actual y elegir la mejor opción. El hecho es que algunas decisiones tomadas por parte de los individuos son ilógicas y, en algunos casos, utilizan automáticamente un mecanismo llamado error cognitivo (Wilke & Mata, 2016).

Los **errores** cognitivos tienen muchos subconjuntos que a veces no tienen límites claros, pero pueden superponerse entre sí. Entre las varias divisiones y términos en el campo de los errores cognitivos, los dos términos de "sesgos cognitivos" y "distorsiones cognitivas", así como las "falacias cognitivas" pueden ser más comunes. A pesar de serias discrepancias en cuanto a la definición y separación del concepto y la división de estos tres términos, son más comunes que el resto (Afzal & Thompson, 2017).

El sesgo cognitivo se puede definir como un conjunto de errores mentales predecibles que surgen de nuestra capacidad limitada para procesar la información de manera objetiva. Puede resultar en decisiones ilógicas e irracionales, y puede hacer que usted juzgue mal los riesgos y las amenazas (Behimehr, 2018).

Los investigadores explicaron que el sesgo cognitivo es la tendencia a tomar decisiones o actuar de forma ilógica, provocada por nuestros valores, memoria, socialización y otros atributos personales. Existen numerosos sesgos que afectan una amplia gama de comportamientos, incluida la toma de decisiones, el juicio, las creencias y las interacciones sociales (Berthet, 2022).

El sesgo cognitivo es una forma de procesamiento de la información en la que las personas prestan más atención a ciertos estímulos e ignoran otros. De

hecho, este tipo de sesgo se debe a la falta de comprensión adecuada de conceptos o eventos (estímulos del entorno) por parte de una persona, en la que no logra identificar la importancia o el peso de cada factor en el proceso de análisis. Por lo tanto, muchas personas padecen este problema debido a este enfoque cognitivo incorrecto y desequilibrado (falta de procesamiento equilibrado de la información). De hecho, un sesgo cognitivo es un tipo de vulnerabilidad cognitiva en el procesamiento de la información en mente, es decir, ciertas condiciones que hacen que los procesos cognitivos se dirijan de manera incompleta hacia estímulos específicos (Baddeley & Hitch, 2016).

En general, el sesgo se define como el apartamiento y la imperfección como una curva defectuosa en la percepción, medición, juicio u otras actividades cognitivas que resultan de no ver o descuidar algunos aspectos en favor de otros (Wilke & Mata, 2016). Existen diferentes tipos de sesgos cognitivos que afectan a casi todos los aspectos de la vida humana. Estos sesgos afectan nuestras habilidades de comunicación social diaria, relaciones e incluso nuestras actividades científicas. El proceso de búsqueda y recuperación de información no escapa a esta regla, y los usuarios, en algunos casos, experimentan estos sesgos cognitivos durante el proceso de recuperación de información en el entorno web (Behimehr, 2018).

Los sesgos cognitivos hacen que las personas saquen conclusiones más rápidamente y tomen decisiones equivocadas. Si una persona se ve obligada a analizar muchas variables a la vez, el cerebro está sobrecargado y por lo tanto la persona trata de elegir el camino más corto y rápido para responder (Ehrlinger et al., 2016). Beck et al. (1979) creen que las personas generalmente no interpretan los eventos como realmente son. Por lo tanto, el objetivo de los especialistas es identificar las distorsiones cognitivas y aportar soluciones que les den una visión real y positiva del mundo alrededor de ellos. El tema de la identificación de posibles sesgos en el campo de la recuperación de información sólo puede ser identificado por especialistas en este campo (Berthet, 2022).

La terapia cognitiva desarrollada por Aaron Beck en la década de 1960 fue un ejemplo de la capacidad de cambiar patrones mentales (Tagg, 2018). Hasta ahora, se han realizado pocas investigaciones para identificar los sesgos cognitivos que pueden ocurrir durante la recuperación de información, por ejemplo, la investigación de Lau y Coiera (2017) es uno de los pocos estudios en este campo.

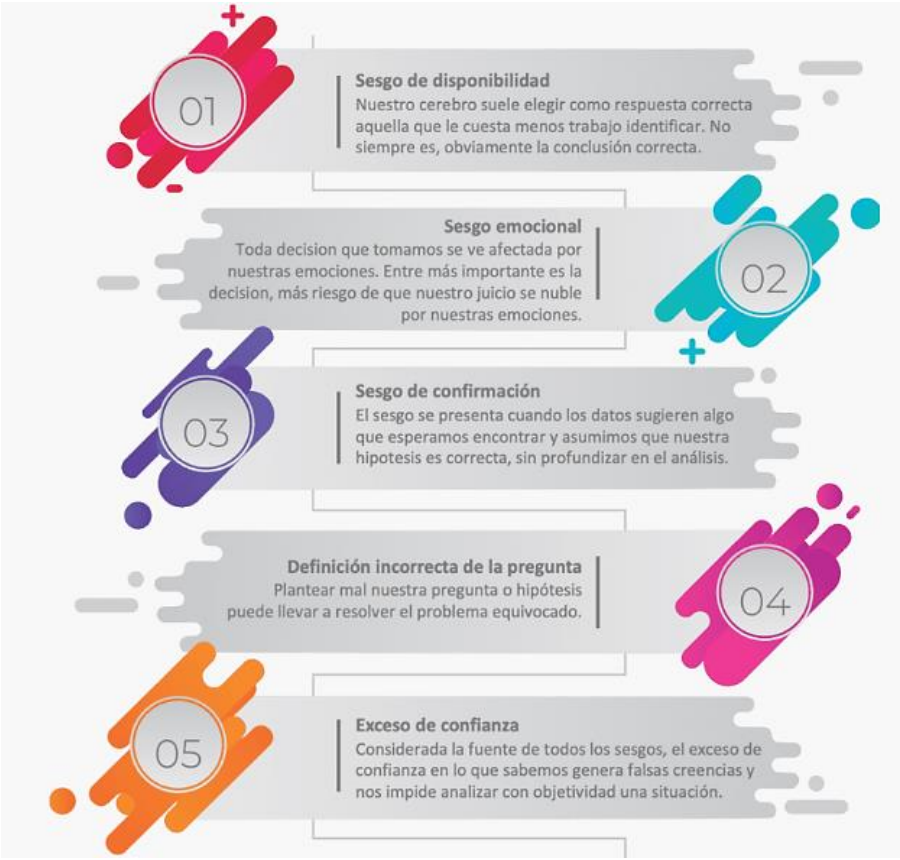
Sin embargo, en su estudio, las opiniones de expertos no se han considerado en el campo de la recuperación de información. Esta investigación argumenta que evaluar la relación entre los sesgos cognitivos y la recuperación de información requiere más estudios para abordar las generalizaciones relevantes.

Otro problema que debe abordarse es que, si bien las personas han estado tratando de comprender el mundo desde la infancia con la ayuda de modelos, no pueden procesar todos los estímulos ambientales de inmediato; en este caso, ellos pueden utilizar directamente la información obtenida de los sesgos cognitivos, sin asegurarse de su validez. Como resultado de esta desviación, el individuo se ve privado del proceso de pensamiento lógico (Ruiz et al., 2018).

Este problema puede afectar todos los aspectos de la vida de una persona. Por lo tanto, los individuos no pueden seguir el proceso lógico en el proceso de recuperación de información, que es una de las partes más importantes de la vida cotidiana de cada persona en la sociedad de la información actual, y como resultado, enfrentan problemas en este proceso. Sin embargo, si los sesgos son efectivos en la recuperación de información, que puede ser influenciada por variables demográficas, se puede ver que los usuarios si son consciente del proceso de recuperación de información y puede corregirse después de la observación de tales sesgos ya que las personas tienen el poder de cambiar sus patrones mentales. Esta cuestión puede generalizarse en el proceso de recuperación de la información, de tal forma que al reconocer los sesgos cognitivos de los usuarios sería posible eliminar o corregir algunos de estos sesgos.

2.1.2. Tipos de sesgos cognitivos

Los siguientes son solo algunos tipos de sesgos cognitivos que tienen una poderosa influencia **en cómo piensas, cómo te sientes y cómo te comportas**.



Anclaje

Este sesgo es la tendencia a sacar conclusiones precipitadas, es decir, basar su juicio final en la información obtenida al principio del proceso de toma de decisiones. Piense en esto como un sesgo de "primera impresión". Una vez que haya escuchado "el ancla", es probable que lo interprete y emita juicios basados en él (Kumar & Goyal, 2016).

El anclaje es cuando alguien se adhiere a un bit de información inicial. En la toma de decisiones, implica que las personas pongan demasiado énfasis en la información única. Esto puede hacer que el tomador de decisiones no considere otra información importante.

Sesgo de exceso de confianza

Esto sucede cuando pones demasiada fe en tu propio conocimiento y opiniones. También puede creer que su contribución a una decisión es más valiosa de lo que realmente es. Puede combinar este sesgo con el anclaje, lo que significa que actúa según sus corazonadas, porque tiene una visión poco realista de su propia capacidad para tomar decisiones (Behimehr, 2018).

Los investigadores han descubierto que los empresarios son más propensos a mostrar un sesgo de exceso de confianza que la población en general (Wilke & Mata, 2016). Pueden no detectar los límites de su conocimiento, por lo que perciben menos riesgo. Algunos tienen éxito en sus empresas, pero muchos no.

Las personas sobrestiman o tienen una confianza excesiva en su capacidad para predecir o prever eventos futuros. Esto hará que el tomador de decisiones tome decisiones sin fundamento o arriesgadas.

Falacia de planificación

La falacia de planificación se refiere a la tendencia de las personas a subestimar el tiempo necesario para completar una tarea. Incluso en los casos en que la tarea era familiar (es decir, el participante la había completado antes) y la persona que hacía la estimación tenía mucha experiencia, incluso experta, en la tarea en cuestión, las subestimaciones son extremadamente comunes. El sesgo está presente en innumerables tipos de tareas, desde la tarea hasta la construcción, desde tareas técnicas (altas habilidades) hasta tareas mundanas, y desde proyectos a pequeña escala (5 minutos) hasta programas gubernamentales a gran escala (Berthet, 2022).

Sin embargo, desde entonces se ha revisado la falacia de la planificación para extenderla no solo al tiempo, sino también al costo y los beneficios de la tarea que se está evaluando. Más precisamente, cuando las personas hacen predicciones sobre su propia tarea (es decir, una que planean completar por sí mismos), tienden a subestimar sistemáticamente el tiempo que llevará, subestiman el costo del proyecto y sobrestiman los beneficios potenciales del proyecto. Sorprendentemente, el sesgo solo está presente cuando se emiten juicios sobre las propias tareas. Los observadores que no están involucrados en la ejecución de la tarea tienden a ser demasiado pesimistas frente al abundante optimismo de la persona que planea realizar la tarea (Lilienfeld, 2019).

Error fundamental de atribución

Esta es la tendencia a culpar a los demás cuando las cosas van mal, en lugar de mirar objetivamente la situación. En particular, puede culpar o juzgar a alguien en función de un estereotipo o un defecto de personalidad percibido. El error de atribución fundamental es la tendencia a echar la culpa a hechos externos (Weems et al., 2017).

La tendencia de las personas a enfatizar demasiado las explicaciones basadas en la personalidad de los comportamientos observados en otros, mientras que subestiman el papel y el poder de las influencias situacionales en el mismo comportamiento.

Sesgo de representación

Esta es la tendencia a creer que una situación es indicativa de una tendencia mayor. Es decir, está relacionado con los estereotipos. El tomador de decisiones cree que la situación representa todas las características de la población de la que forma parte. Provoca una falla en la percepción de la capacidad de uno para predecir un resultado o resultado dado (Berthet, 2022).

Sesgo de aleatoriedad

Esta es la tendencia a ver un patrón en datos o información aleatoria. Buscamos cada vez más aprovechar nuevas fuentes de información en el proceso de toma de decisiones. Nuestra búsqueda de significado en la información conduce a una confianza irrazonable en resultados insignificantes (Franco, 2018).

Sesgo de autoservicio

Esta es la tendencia de atribuir los resultados positivos de una decisión o situación a las propias acciones o decisiones. Asimismo, hace que los individuos atribuyan consecuencias negativas a factores fuera de nuestro control. Esto puede causar una incapacidad para evaluar con precisión o afectar una situación a través de la toma de decisiones (Haselton et al., 2017).

Un sesgo egoísta es aquel que promueve su autoestima y lo ayuda a sentirse mejor acerca de la posición en la que se encuentra para tomar una decisión. Cuando se involucra en un sesgo egoísta, es posible que sin querer tome decisiones que lo beneficien a usted mismo sobre otros empleados, clientes, proveedores o la organización y sus objetivos (Behimehr, 2018).

Sesgo de impacto

El pronóstico afectivo es simplemente el proceso de hacer juicios sobre los propios estados emocionales futuros. Esto ocurre a lo largo de nuestras vidas y tiene una tremenda influencia en nuestro juicio y toma de decisiones, tanto a gran como a pequeña escala. Uno puede considerar muy razonablemente los sentimientos futuros al decidir si casarse, tener un hijo o cambiar de trabajo y cuándo, y las expectativas sobre el impacto de estas decisiones en la felicidad, por

ejemplo, probablemente jugarán un papel muy importante en el camino tomado (Berthet, 2022).

Al mismo tiempo, uno puede preguntarse si tomar o no una segunda copa de vino o comprar una nueva marca de detergente para la ropa. Las expectativas sobre los efectos de estos comportamientos en las emociones futuras también desempeñarán un papel en nuestra toma de decisiones diaria. La previsión afectiva es una habilidad importante, entonces, pero se ve afectada por varios sesgos, quizás el más destacado de los cuales es el sesgo de impacto. El sesgo de impacto es la tendencia de las personas a sobreestimar la duración y la intensidad de las emociones futuras, esperando que los eventos actuales tengan un mayor impacto en los estados emocionales futuros de lo que en última instancia tienen (Afzal & Thompson, 2017).

Sesgo de apoyo a la elección

Una vez que hemos tomado una decisión, tendemos a sentirnos bastante satisfechos con nosotros mismos. Es otra cosa fuera de la lista de "cosas por hacer" y podemos empezar a pensar en un plan de acción para el futuro. Este encanto del sentimiento posterior a la decisión también es un factor influyente (Arévalo & Valarezo, 2022).

Sesgo de información

No toda la información es relevante y, a menudo, los tomadores de decisiones absorben información irrelevante que no tiene relación con la decisión en sí. No se distraiga con montones de hechos que en realidad no tendrán relevancia para la decisión (Behimehr, 2018).

Sesgo a favor de la innovación

El sesgo a favor de la innovación describe cualquier situación en la que enfatizamos lo bueno de algo y descartamos lo malo, por ejemplo, cuando informamos un alto número de registros para una nueva herramienta de redes sociales pero las tasas de uso son realmente bajas. Las organizaciones centradas en el rendimiento son particularmente propensas a esto, ya que las personas exageran su propio éxito por razones de avance profesional (Afzal & Thompson, 2017).

2.1.3. Errores en la toma de decisiones relacionados con el sesgo

En cualquier lugar de trabajo, es probable que haya muchas situaciones en las que los gerentes o empleados necesiten tomar una decisión comercial informada. Tanto el pensamiento crítico como una evaluación de los diferentes resultados de varias decisiones son necesarios para tomar una decisión que produzca el resultado deseado. Sin embargo, a veces, sin darse cuenta, los tomadores de decisiones tienen cierto sesgo durante su proceso de toma de decisiones (Arévalo & Valarezo, 2022).

Cuando tiene un sesgo en la toma de decisiones, significa que toma su decisión en función de lo que suele ser un procesamiento subconsciente de sus experiencias y conocimientos previos. Estos atajos mentales pueden afectar la forma en que toma sus decisiones y pueden dar como resultado una decisión diferente de la que tomaría si no hubiera prejuicios. Los sesgos difieren según el individuo y sus personalidades y experiencias únicas (Tagg, 2018).

Hay varias razones por las que la toma de decisiones empresariales es difícil. Por lo general, más de una parte interesada está involucrada en el proceso; esto complica el proceso desde el punto de vista logístico y emocional y, a veces, agrega aspectos políticos y de carrera a la mezcla (Behimehr, 2018).

Cuando una empresa es global, a menudo ocurre que las partes involucradas en la toma de decisiones se encuentran en diferentes lugares del

mundo. Acordar una hora y un lugar para tomar la decisión en sí puede requerir una clase magistral en la gestión del diario. Múltiples oficinas pueden significar comprometer objetivos diferentes, incluso competitivos. Esto es notoriamente complicado cuando las decisiones las toman personas de diferentes países (Behimehr, 2018).

Algunas culturas son notoriamente lentas en la toma de decisiones. En Japón, que tiene aversión al riesgo, por ejemplo, muchos grupos diferentes dentro de una organización tienden a reflexionar sobre las cosas antes de que la empresa acuerde una nueva dirección. Esto significa que la toma de decisiones puede ser muy lenta (Ehrlinger et al., 2016).

El miedo a las implicaciones de tener que rendir cuentas por las decisiones puede hacer que los trabajadores se muestren reacios a comprometerse con una decisión. Las organizaciones que han desarrollado una cultura de la culpa a menudo descubren que los trabajadores son reacios a tomar decisiones si pueden ser contraproducentes para ellos individualmente. Esto puede volverse muy perjudicial para la organización a largo plazo si la empresa se paraliza por la falta de toma de decisiones (Afzal & Thompson, 2017).

Además de las razones culturales internas por las que una organización puede no tomar buenas decisiones, también existen muchos sesgos cognitivos que pueden afectar la toma de decisiones. Cuando estos factores cognitivos están en juego, es posible que ni siquiera nos demos cuenta. Comprender estos sesgos que influyen en nuestras decisiones es una buena manera de superarlos y, con suerte, tomar mejores decisiones a largo plazo (Arévalo & Valarezo, 2022).

Las personas pueden tomar muchas decisiones rápidas y eficientes todos los días, a menudo de manera inconsciente, basándose en esquemas cognitivos o atajos. Estos atajos permiten a las personas emitir juicios que son "suficientemente buenos" y, con frecuencia, correctos. Dicho esto, también dejan a las personas propensas a sesgos cognitivos predecibles (Ehrlinger et al., 2016).

Como categoría, los sesgos cognitivos en la toma de decisiones abarcan una amplia gama de desviaciones de lo que comúnmente se considera juicio y decisiones puramente racionales. En su libro de 2011, Daniel Kahneman abogó por una distinción entre diferentes modos en los que la gente piensa. Específicamente, se pueden distinguir entre el pensamiento que es rápido (a menudo denominado como Sistema 1 o pensamiento automatizado), y pensamiento que es lento

(Sistema 2, o consciente, pensamiento deliberado). El pensamiento del sistema 2 (es decir, lento) implica sopesar formalmente las opciones y valores de utilidad que forman parte de la toma racional de decisiones; es consciente, esforzada y particularmente útil para calcular y dibujar conexiones entre conceptos, el inconveniente al pensamiento del Sistema 2 es que requiere tener tiempo disponible, información y motivación para participar en una lenta reflexión consciente (Albladi & Weir, 2018).

Los sesgos cognitivos y de toma de decisiones existen porque el pensamiento rápido del Sistema 1 es inconscientemente para evaluar cualquier situación dada e intentar hacer coincidir un patrón con una situación anterior a partir de experiencia pasada. Este procesamiento basado en esquemas es notablemente eficiente, pero falla en las pruebas de teoría de la utilidad tradicional (bernouliana) de manera predecible. Estos atajos, como tales, son herramientas valiosas para navegar el complejo panorama social y cognitivo. Tomado como un conjunto, ofrecen una idea de las diferencias en el juicio y la toma de decisiones que existen entre pensamiento consciente y deliberado y procesamiento automatizado basado en heurísticas (Ehrlinger et al., 2016).

El cerebro humano es poderoso, pero está sujeto a limitaciones. Los sesgos cognitivos a menudo son el resultado del intento de su cerebro de simplificar el procesamiento de la información. Los sesgos a menudo funcionan como reglas generales que lo ayudan a comprender el mundo y tomar decisiones con relativa rapidez (Berthet, 2022).

Algunos de estos sesgos están relacionados con la memoria. La forma en que recuerda un evento puede estar sesgada por varias razones y eso, a su vez, puede conducir a un pensamiento y una toma de decisiones sesgados. Otros sesgos cognitivos pueden estar relacionados con problemas de atención. Dado que la atención es un recurso limitado, las personas tienen que ser selectivas sobre a qué prestan atención en el mundo que les rodea (Afzal & Thompson, 2017).

Si tuviera que pensar en todas las opciones posibles al tomar una decisión, tomaría mucho tiempo tomar incluso la opción más simple. Debido a la gran complejidad del mundo que te rodea y la cantidad de información en el entorno, a veces es necesario confiar en algunos atajos mentales que te permitan actuar rápidamente (Albladi & Weir, 2018).

Los sesgos cognitivos pueden ser causados por una serie de cosas diferentes, pero son estos atajos mentales, conocidos como heurísticas, los que a menudo juegan un papel importante. Si bien a menudo pueden ser sorprendentemente precisos, también pueden conducir a errores de pensamiento (Bertino & Ferrari, 2018).

Los sesgos cognitivos pueden conducir a un pensamiento distorsionado. Las creencias de la teoría de la conspiración, por ejemplo, a menudo están influenciadas por una variedad de sesgos. Pero los sesgos cognitivos no son necesariamente del todo malos. Los psicólogos creen que muchos de estos sesgos tienen un propósito adaptativo ya que permiten tomar decisiones rápidamente. Esto puede ser vital si nos enfrentamos a una situación peligrosa o amenazante (Ehrlinger et al., 2016).

2.1.4. Teoría de la perspectiva: un análisis de la decisión bajo riesgo

La teoría de la utilidad esperada ha dominado el análisis de la toma de decisiones bajo riesgo. Ha sido generalmente aceptado como modelo normativo de elección racional, y ampliamente aplicado como modelo descriptivo del comportamiento económico. Por lo tanto, se supone que todas las personas razonables desearían obedecer los axiomas de la teoría, y que la mayoría de las personas lo hacen la mayor parte del tiempo (Park, 2023).

La toma de decisiones bajo riesgo puede verse como una elección entre perspectivas o apuestas. Una perspectiva (x1, p1; …; xn, pn) es un contrato que produce un resultado xi con probabilidad pi, donde p1 + p2 + … + pn = 1. Para simplificar la notación, omitimos los resultados nulos y usamos (x, p) para denotar la perspectiva (x, p; 0, 1 – p) que produce x con probabilidad p y 0 con probabilidad 1 – p. La perspectiva (sin riesgo) que produce x con certeza se denota por (x). La presente discusión está restringida a prospectos con las llamadas probabilidades objetivas o estándar (Kahneman & Tversky, 2017).

La teoría de la perspectiva es una teoría de la psicología que describe cómo las personas toman decisiones cuando se les presentan alternativas que involucran riesgo, probabilidad e incertidumbre. Sostiene que las personas toman decisiones basadas en pérdidas o ganancias percibidas (Park, 2023).

La teoría de la perspectiva a veces se conoce como la teoría de la aversión a la pérdida. La teoría fue presentada por dos psicólogos, Daniel Kahneman y Amos Tversky, para describir cómo los humanos toman decisiones cuando se les presentan varias opciones (Kahneman & Tversky, 2017).

La teoría estaba contenida en el artículo "Teoría de la perspectiva: un análisis de decisión bajo riesgo" que se publicó en la revista "Econometrica" en 1979. Desde que se desarrolló, la teoría de la perspectiva se ha utilizado en varias disciplinas. Se utiliza para evaluar varios aspectos de la toma de decisiones políticas en las relaciones internacionales (Park, 2023).

Fases de la teoría de la perspectiva

La teoría describe el proceso de toma de decisiones en dos fases, que incluyen:

1. Fase de edición

La fase de edición se refiere a cómo las personas involucradas en la toma de decisiones caracterizan las opciones de elección o los efectos de encuadre. Los efectos explican cómo la elección de una persona se ve influenciada por la redacción, el orden o el método en el que se presentan las opciones.

Un ejemplo para demostrar el efecto de encuadre pueden ser las opciones que se les dan a los pacientes con cáncer. Por lo general, a los pacientes con cáncer se les presenta la opción de someterse a cirugía o quimioterapia para tratar sus enfermedades, y toman una decisión en función de si las estadísticas de resultados se presentan en términos de tasas de supervivencia o tasas de mortalidad. Una vez que las opciones se han enmarcado y están listas para la toma de decisiones, la teoría entra en la segunda fase.

2. Fase de evaluación

En la fase de evaluación, las personas tienden a comportarse como si tomaran una decisión en función de los posibles resultados y eligieran la opción con mayor utilidad. La fase utiliza el análisis estadístico para medir y comparar los resultados de cada prospecto. La fase de evaluación comprende dos índices, es decir, la función de valor y la función de ponderación, que se utilizan para comparar las perspectivas (Park, 2023).

Características de la teoría de la perspectiva

La teoría de las perspectivas viene con las siguientes características:

1. Certeza

Cuando se les presentan varias opciones para elegir, los humanos muestran una fuerte preferencia por la opción con certeza. Están dispuestos a sacrificar la opción que ofrece más ingresos potenciales para lograr una mayor certeza. Por ejemplo, suponga que una lotería ofrece dos opciones, A y B.

La opción A ofrece una ganancia garantizada de $100 mientras que la opción B brinda la posibilidad de ganar $200, con un 70 % de posibilidades de ganar y un 30 % de posibilidades de perder. La mayoría de la gente elegirá la opción A, ya que ofrece una ganancia garantizada, aunque ofrece un rendimiento menor en comparación con B.

2. Pequeñas probabilidades

La gente tiende a descontar probabilidades muy pequeñas incluso si existe la posibilidad de perder toda su riqueza. Al descontar las probabilidades pequeñas, las personas terminan eligiendo opciones de mayor riesgo con mayores probabilidades.

3. Posicionamiento relativo

El posicionamiento relativo significa que las personas tienden a centrarse menos en su ingreso o riqueza final y más en las ganancias o pérdidas relativas que obtendrán. Si su posición relativa no mejora con el aumento de los ingresos, no se sentirán mejor. Esto significa que las personas tienden a compararse con sus vecinos, amigos y familiares, y están menos interesadas en saber si están mejor que hace algunos años.

Por ejemplo, si todos en la oficina obtienen un aumento del 20%, nadie se sentirá mejor. Sin embargo, si la persona obtiene un aumento del 10% y otras personas no obtienen un aumento, esa persona se sentirá mejor y más rica que los demás.

4. Aversión a la pérdida

La gente tiende a dar más peso a las pérdidas que a las ganancias obtenidas al tomar una determinada opción. Por ejemplo, si una persona gana $200 en ganancias y $100 en pérdidas, la persona se centrará en la pérdida, aunque haya obtenido una ganancia neta de $100. Esto muestra que las personas están más preocupadas por las pérdidas que por las ganancias (Park, 2023).

Crítica de la teoría de la perspectiva

Una de las críticas a la teoría de las perspectivas es que carece de explicaciones psicológicas para el proceso del que habla. La crítica proviene de otros psicólogos que señalan que factores como las respuestas emocionales y afectivas humanas que son importantes en el proceso de toma de decisiones están ausentes en el modelo. La teoría también es criticada por la teoría del marco inadecuado que explica por qué los actores generan los marcos que utilizan. Los tomadores de decisiones a menudo necesitan lidiar con marcos competitivos en varios temas (Kahneman & Tversky, 2017).

2.1.5. Los cinco sesgos cognitivos más populares que resultan en ataques de phishing

Tabla 1: *Sesgos cognitivos que influyen en la detección de correos phishing*

Sesgos cognitivos	Características
Sesgo de omisión	Preferencia por la omisión/inacción que puede llevar a los tomadores de decisiones a elegir los riesgos y beneficios del statu quo incluso cuando los riesgos y beneficios relativos (RR) de cambiar el statu quo a través de la acción son objetivamente superiores.
Sesgo de exceso de confianza	Las decisiones basadas en predicciones erróneas pueden generar expectativas incorrectas para el paciente y la familia, y un tratamiento, asesoramiento o planificación del alta potencialmente inapropiados.
Sesgo de resultado	La propensión a culpar más fácilmente cuando el resultado es malo.
Sesgo de anclaje	Este sesgo es la tendencia a sacar conclusiones precipitadas, es decir, basar su juicio final en la información obtenida al principio del proceso de toma de decisiones. Piense en esto como un sesgo de "primera impresión". Una vez que haya escuchado "el ancla", es probable que lo interprete y emita juicios basados en él.

Sesgo de confirmación	El sesgo de confirmación ocurre cuando busca información que respalde sus creencias existentes y rechaza los datos que van en contra de lo que cree. Esto puede llevarlo a tomar decisiones sesgadas, porque no tiene en cuenta toda la información relevante.
Sesgo de representatividad	Se juzga la probabilidad de que algo ocurra, a la causa de otro suceso basándose en cuánto representan o se parecen a creencias previas, ignorando otra información útil, este sesgo actúa cuando las personas tienen que predecir una conducta o atribuir una pertenencia categorial.
Sesgo de simulación	Representa la facilidad con que se puedan construir mentalmente ejemplos o escenarios de juicios sociales, lo que implica que mientras más fácil sea para las personas imaginar un escenario para un cierto resultado alternativo, creerán que es más probable que éste se produzca.
Sesgo de positividad	Se refiere al hecho de que las personas atribuyen sus conductas positivas a sí mismo o a sus disposiciones, mientras que las conductas negativas se atribuyen a causas externas. Este sesgo de positividad ha mostrado ser bastante fuerte cuando se han realizado experiencias con predicciones opuestas.
Sesgo de falsa unicidad	Las personas se autodefinen como superiores en base a sus atributos positivos como habilidades y capacidades personales, por lo que tienden a declararse superiores a sus pares o una persona similar a ellas en atributos deseables socialmente.
Sesgo de Optimismo Ilusorio	Predisposición de los sujetos a apreciar mayores probabilidades que el resto de individuos de que les sucedan acontecimientos positivos.

Sesgo de Ilusión de Invulnerabilidad	Percepción de las personas a sentir menor probabilidad de la ocurrencia de acontecimientos negativos.
Sesgo de Correspondencia	Proceso por el cual se explica una conducta por un rasgo ignorando causas situacionales. Este sesgo ocurre en parte porque la persona es saliente perceptivamente, se da con similar intensidad en culturas individualistas y colectivistas.
Sesgo de Atribución de causalidad	Proceso psicológico para explicar la conducta social mediante un esquema de antecedente-consecuente. Se atribuye la causa a un atributo interno de la persona si ésta muestra baja distinción, alta consistencia y bajo consenso.
Sesgo de Autoservicio	Tendencia a tomar el crédito para éxitos, y culpar a otros por el fracaso.
Sesgo de Confirmación	Es un tipo de parcialidad dirigido a la tendencia a buscar o interpretar información en una manera que se afirma las ideas preconcebidas, lo cual predispone al sujeto a modificar la percepción de opiniones previas de los hechos, a beneficio del resultado final.

Nota: Sesgos cognitivos **que influyen en el correo phishing** de acuerdo a Beldhuis et al., (2021)

Según Carpenter (2022) los cinco sesgos cognitivos más populares son:

Efecto halo

Tu impresión general de una persona influye en cómo te sientes y piensas sobre su carácter. Esto se aplica especialmente al atractivo físico que influye en cómo calificas sus otras cualidades.

La tendencia a tener una impresión positiva de una persona, empresa, marca, producto o servicio. Los ciberdelincuentes a menudo se hacen pasar por entidades confiables como un banco o una organización de renombre que lleva a las personas a abrir archivos adjuntos maliciosos, hacer clic en direcciones URL maliciosas o visitar sitios web maliciosos (Carpenter, 2022).

2.1.6. Descuento hiperbólico

El descuento hiperbólico, también llamado "sesgo presente", es un sesgo cognitivo, en el que las personas eligen recompensas inmediatas más pequeñas en lugar de recompensas posteriores más grandes. El valor presente descontado de la recompensa futura sigue una curva matemática llamada "hipérbola".

La inclinación a elegir recompensas más pequeñas en lugar de recompensas más grandes que vendrán más adelante en el futuro. Por ejemplo, la mayoría de nosotros tendemos a caer en las "pruebas gratuitas" o los "cupones gratuitos" y regalamos felizmente la información de nuestra tarjeta de crédito sin considerar los posibles resultados negativos a largo plazo (Carpenter, 2022).

Sesgos de curiosidad

Efecto de la curiosidad: Las personas son curiosas por naturaleza y, a menudo, se entregan a comportamientos arriesgados para satisfacer un antojo. Los ciberdelincuentes manipulan a los lectores en el correo electrónico y las redes sociales mediante la elaboración de mensajes (titulares de noticias, anuncios y otras campañas de clickbait) que despiertan la curiosidad (Carpenter, 2022).

Efecto de actualidad

Efecto de actualidad: La tendencia a recordar los eventos más recientes que pueden resultar en malos juicios y un mal comportamiento de seguridad. Por ejemplo, la mayoría de los equipos de seguridad admiten ignorar un tercio de todas las alertas de seguridad, ya que la mayoría de ellas son falsos positivos (Carpenter, 2022).

Sesgo de autoridad

A menudo hay un cierto nivel de confianza que surge al escuchar a una figura de autoridad presentar información o ideas. El sesgo de autoridad ocurre si favorece la opinión de sus figuras de autoridad sobre los demás, a pesar de que hay información y opiniones que son más sólidas y relevantes para el problema que está tratando de resolver (Behimehr, 2018).

Las personas inconscientemente están más influenciadas por aquellos que están en una posición de autoridad. Las estafas de compromiso de correo electrónico comercial (BEC, por sus siglas en inglés) son uno de los delitos cibernéticos más dañinos desde el punto de vista financiero (casi $ 2 mil millones en 2020) y utilizan el sesgo de autoridad como un medio para defraudar a los

usuarios. Por ejemplo, los empleados del departamento de finanzas recibirán repentinamente un correo electrónico fraudulento del director ejecutivo con instrucciones para transferir grandes sumas de dinero (Carpenter, 2022).

2.1.7. Sesgos cognitivos que afectan la toma de decisiones en ciberseguridad

Según Vijayaraghavan (2022), estos son:

En un mundo perfecto, todos los humanos serían seres racionales capaces de tomar decisiones basadas en hechos y lógica. Si bien el cerebro humano es poderoso, está sujeto a limitaciones a la hora de simplificar la información. Nuestro cerebro puede volverse perezoso y tomar atajos para llegar a decisiones. Estos atajos se denominan sesgos.

Los sesgos cognitivos se definen como patrones sistemáticos de desviación de la racionalidad del juicio. En el mundo de la psicología, esto se llama descuento hiperbólico: nuestra inclinación a elegir recompensas inmediatas en lugar de recompensas que vendrán más tarde en el futuro, incluso cuando esas recompensas sean similares o superiores.

Todo ser humano es vulnerable a estos errores de juicio. Por lo tanto, comprender estos sesgos puede ayudarnos a superar cualquier error relacionado con la seguridad y diseñar una estrategia de defensa más sólida.

1. Sesgo de disponibilidad

El sesgo de disponibilidad afecta nuestras decisiones al hacer que nos concentremos en la información más reciente. Por ejemplo, si hay noticias sobre un nuevo ataque de ransomware, la mayoría de los equipos de seguridad se centrarán en proteger sus redes, aunque no se aplique a su industria.

Tales noticias pueden hacer que las organizaciones ignoren otros temas importantes que pueden causar más daño a sus redes. Aunque es necesario protegerse contra los ataques de tendencia, es igualmente importante considerar otros casos también.

2. Sesgo de confirmación

El sesgo de confirmación es la tendencia a favorecer la información que confirma nuestras creencias. Podemos ver este sesgo en acción mientras buscamos amenazas. Este sesgo puede engañar a los analistas para que busquen información específica que se alinee con sus creencias y habilidades. Muchos

analistas de seguridad experimentados se concentran en la causa de un problema antes de la investigación y solo buscan evidencia que respalde esa causa.

Por ejemplo, si un analista cree que una infracción es el resultado de un trabajo interno, puede ignorar por completo el hecho de que una determinada interacción con una parte relacionada (que involucra a proveedores y revendedores externos, autoridades gubernamentales o auditores internos) podría haber desencadenó la serie de eventos que condujeron a la violación.

Los profesionales de la seguridad también deberían estar más abiertos a las sugerencias y aceptar los diferentes puntos de vista de los demás. Esto puede ayudarlos a analizar problemas que podrían haberse perdido anteriormente.

3. Sesgo de optimismo

También conocido como la ilusión de la invulnerabilidad, el sesgo optimista nos hace creer que la posibilidad de experimentar algo positivo es mayor (o algo negativo es menor) de lo que realmente es. Un simple ataque de phishing puede permitir que los adversarios obtengan acceso a su red en poco tiempo. Si bien este sesgo puede ser bueno para nuestra vida personal, en ciberseguridad siempre es mejor tener la mentalidad opuesta al configurar servidores, aplicaciones, firewalls y más.

4. Sesgo agregado

Podemos ver el sesgo agregado en acción cuando tendemos a concluir algo sobre un individuo usando datos sobre una población más grande.

Imagine que ha habido una violación de datos en su organización. ¿Los registros de quién comenzarías a revisar primero? Definitivamente gente con mucho acceso, ¿verdad? Este sesgo puede hacer que los analistas se centren en un individuo en particular según el grupo del individuo, como administradores o usuarios privilegiados. Pero en realidad, cualquier empleado habitual podría haber hecho clic en un enlace de phishing, desencadenando una serie de eventos que finalmente condujeron a la filtración.

Le recomendamos que analice el comportamiento humano individual para detectar anomalías mediante el reconocimiento de cambios sutiles en las actividades habituales. La implementación de UEBA para detectar comportamientos maliciosos puede fortalecer sus defensas contra las amenazas internas.

5. El efecto de encuadre

El sesgo de encuadre afecta las decisiones de las personas en función de cómo se presentan las opciones, en lugar de un examen de los hechos. Los piratas informáticos pueden usar esto cuando envían correos electrónicos de phishing que se enmarcan como algo importante de un funcionario superior o como una actualización del producto.

2.1.8. Cómo capacitar para el cambio de conducta

A medida que los ataques cibernéticos crecen en volumen y sofisticación, la necesidad de abordar los prejuicios humanos de frente se vuelve aún más crítica. Trabajar de forma remota se ha convertido en la nueva norma y se ha acelerado; y los empleados aislados son más susceptibles que nunca a las estafas. Los controles técnicos, como los antivirus y la detección de intrusos, pueden filtrar algunos elementos maliciosos; sin embargo, frustrar el phishing y otras formas de ingeniería social requiere capacitar a las personas para resolver las estafas. Son la última línea de defensa. **A continuación, se presentan tres recomendaciones que pueden ayudar a las organizaciones a comenzar**:

- **Practique capacitación y compromiso consistentes y personalizados: las organizaciones solo pueden lograr un cambio de comportamiento a largo plazo a través de ejercicios de capacitación regulares. Para evitar infracciones, las organizaciones deben evaluar constantemente a los trabajadores con simulaciones de phishing del mundo real sobre amenazas nuevas y emergentes. Los empleados deben recibir entrenamiento y orientación personalizados en función de su aptitud, susceptibilidad al riesgo, roles laborales particulares y departamento.**
- **Hacer que la seguridad cibernética sea parte de la cultura central: el liderazgo debe reconocer la seguridad cibernética como un elemento fundamental de su cultura organizacional y no considerarla como una iniciativa discreta de mitigación de riesgos. Las empresas solo pueden desarrollar una cultura de seguridad cibernética si el liderazgo fomenta un entorno en el que se fomenten y celebren actitudes y comportamientos de seguridad positivos.**

- **Utilice un enfoque basado en datos para medir las actitudes: las empresas pueden encontrar la cultura de ciberseguridad difícil de medir y cuantificar, pero no es imposible. Comience por crear una evaluación de referencia de la conciencia, los comportamientos y las percepciones de los empleados, y cree una estrategia a largo plazo para rastrear y mejorar esas métricas con el tiempo** (Carpenter, 2022)**.**

2.1.9. Consejos para evitar sesgos en la toma de decisiones

Comprender los efectos del sesgo. Cuanto más comprenda el impacto del sesgo en la toma de decisiones, más probable será que esté atento a los sesgos que pueden obstaculizar su capacidad para tomar una decisión informada basada en hechos actuales (Afzal & Thompson, 2017).

Sepa qué está influyendo en su decisión. Antes de seleccionar una decisión final, examine los factores que pueden estar influyendo en su decisión. Cuando puede articular qué determinó su decisión, puede darse cuenta más fácilmente si su decisión se debió a un sesgo (Arévalo & Valarezo, 2022).

Cuestiona tus prejuicios. Piense en las formas en que puede desafiar sus sesgos actuales para asegurarse de que no sean parte de su decisión. Hágase preguntas importantes para poder pensar críticamente y asegurarse de no ignorar información clave, perderse algunas consideraciones o prestar demasiada atención a un factor sobre otro (Berthet, 2022).

Usa múltiples fuentes. Al desarrollar su decisión, considere pedir a otros comentarios, recopilar datos e investigar el tema sobre el que está decidiendo para tener más información a su disposición. Esté abierto a escuchar diversas opiniones y puntos de vista para que pueda recopilar perspectivas que pueden diferir de las suyas (Cwik & Margraf, 2017).

Reflexiona sobre tus decisiones anteriores. Pregúntese si se apresuró a tomar una decisión antes o si alguna vez se sintió presionado para decidir algo importante dentro de un período de tiempo determinado. Si reconoce que ha tenido algunos sesgos en decisiones anteriores, es posible que reconozca cuando esté a punto de hacer lo mismo (Ehrlinger et al., 2016).

Russo y Shoemaker revelan los diez errores más comunes en la toma de decisiones, muchos de los cuales están relacionados con el sesgo cognitivo:

- Comenzar a recopilar información y llegar a conclusiones demasiado pronto.
- Crear un marco mental para su decisión.
- No poder definir el problema en más de una forma.
- Exceso de confianza en su juicio: no reunir información fáctica clave.
- Confiar inapropiadamente en “reglas empíricas”.
- No seguir un procedimiento sistemático al tomar la decisión final.
- No poder gestionar el proceso de toma de decisiones del grupo.
- No interpretar correctamente la evidencia de resultados pasados.
- No mantener registros sistemáticos para realizar un seguimiento de los resultados de sus decisiones.
- No crear un enfoque organizado para comprender su propia toma de decisiones (Gordon, 2022).

2.2. Disponibilidad heurística

La heurística de disponibilidad describe nuestra tendencia a utilizar la información que nos viene a la mente rápida y fácilmente al tomar decisiones sobre el futuro. Este es un sesgo cognitivo en el que toma una decisión en función de un ejemplo, información o experiencia reciente que está fácilmente disponible para usted, aunque puede que no sea el mejor ejemplo para informar su decisión (Ehrlinger et al., 2016).

En otras palabras, se supone que la información que se recuerda más fácilmente (es decir, más disponible) refleja eventos más frecuentes y/o más probables. Mientras que la información que es más difícil de recordar (es decir, menos disponible) se supone que refleja eventos menos frecuentes y/o menos probables (Kahan et al., 2017).

La heurística de disponibilidad también se ha identificado como una importante causa subyacente de los juicios egocéntricos. Es fácil concluir, por ejemplo, que usted completa la mayoría de las tareas domésticas mientras que su cónyuge realiza de manera confiable menos de la mitad de estas tareas. De hecho, es común que ambos miembros de un matrimonio exageren la responsabilidad de las tareas del hogar. Este sesgo se deriva, en parte, de una tendencia a simplemente saber más y recordar mejor las tareas que ha realizado que las tareas realizadas por otra persona. En otras palabras, las contribuciones propias al hogar están más “disponibles” que las contribuciones de los demás, lo que lleva a las

personas a asumir a menudo que las contribuciones propias son más frecuentes que las de los demás (Arellano & Solar, 2023).

2.3. Ingeniería social

Al investigar el comportamiento humano hacia las amenazas en línea, es importante centrarse en la interacción entre los atributos del individuo, su contexto actual y la táctica de persuasión del mensaje (Williams et al., Individual differences in susceptibility to online influence: a theoretical review, 2017). Según una taxonomía propuesta por Krombholz et al. (2015), las tres entidades principales que encapsulan los ataques de ingeniería social son operador, tipo y canal. El operador del ataque puede ser un software humano o malicioso.

El tipo de operador también puede determinar el tipo de ataque de ingeniería social elegido. Una taxonomía ha clasificado el tipo de ataque como de base técnica, que incluye phishing, estafa y malware, o de base humana, como suplantación de identidad, robo de identidad e ingeniería social inversa. Un ejemplo de un ataque de base técnica en las redes sociales es el ataque de secuencias de comandos entre sitios que recientemente se hizo popular entre los delincuentes en los SNS. Por el contrario, persuadir a la víctima para que contacte al atacante conectándose con los amigos de la víctima a través de una técnica de ingeniería social inversa es un ejemplo de un ataque basado en humanos en las redes sociales (Rathore et al., 2017).

El contexto juega un papel fundamental en los ataques de ingeniería social porque determina la complejidad del ataque, especialmente para el operador. Se ha argumentado que, en los sitios de redes sociales, hay tres fuentes principales en el perfil del usuario que los ciberdelincuentes utilizan para llegar a sus víctimas, el contenido, las conexiones de amistad y la configuración de privacidad. La configuración de privacidad y seguridad de una red son medidas importantes para proteger al usuario. Incluso con la funcionalidad limitada de las preferencias actuales de privacidad y seguridad de la red social, si los usuarios ajustan la configuración de privacidad de la red y evitan que personas que no son amigos accedan a su cuenta, el atacante no podrá usar la cuenta para recopilar la información necesaria para realizar ataques indirectos (Bertino & Ferrari, 2018).

2.3.1. Correos phishing

Desde que se describió por primera vez en 1987, el phishing se ha convertido en muchas tácticas altamente especializadas. Y a medida que avanzan las tecnologías digitales, este ataque continúa encontrando nuevas formas de explotar las vulnerabilidades (Albladi & Weir, 2018).

El phishing es el acto de enviar de forma electrónica y engañosa un correo para ponerse en contacto con una persona, con el fin de hacer que el individuo pueda realizar electrónicamente un hecho que sea beneficioso para el engañador y perjudicial para los engañados. Los incidentes de phishing suelen ocurrir por correo electrónico. Por ejemplo, un empleado puede recibir un correo electrónico de una dirección similar a la del jefe del departamento de TI, solicitar al destinatario que proporcione credenciales de red o ejecutar código malicioso. Si lo hace, pone en riesgo tanto el destinatario como a la su organización (Ehrlinger et al., 2016).

El phishing de correo electrónico es un tipo de ataque cibernético de ingeniería social en el que correos electrónicos aparentemente legítimos intentan atraer al receptor para que realice una acción con consecuencias negativas (por ejemplo, abrir un archivo adjunto malicioso que instala malware en el dispositivo de las víctimas). Si bien la concepción popular del phishing es un mensaje del infame "príncipe nigeriano", los correos electrónicos de phishing modernos pueden ser difíciles de distinguir de los correos electrónicos seguros, con estudios a gran escala que sugieren tasas de clics de hasta el 20% para los correos electrónicos de phishing más efectivos (Williams et al., 2018). En parte debido a esta alta tasa de clics, se estima que el phishing cuesta decenas de miles de millones de dólares cada año y ahora también se reconoce como un importante problema de salud pública asociado con resultados negativos para la salud que incluyen depresión y suicidio (Hakim et al., 2021).

El phishing es un tipo de ataque de ingeniería social que a menudo se usa para robar datos de usuarios, incluidas las credenciales de inicio de sesión y los números de tarjetas de crédito. Ocurre cuando un atacante, haciéndose pasar por una entidad confiable, engaña a la víctima para que abra un correo electrónico, un mensaje instantáneo o un mensaje de texto. Luego, se engaña al destinatario para que haga clic en un enlace malicioso, lo que puede provocar la instalación de

malware, la congelación del sistema como parte de un ataque de ransomware o la revelación de información confidencial (Arévalo & Valarezo, 2022).

El phishing, un ataque de ingeniería social desplegado por correo electrónico para engañar a las personas, es una de las mayores amenazas a la ciberseguridad. Ha habido un aumento del 782% en los delitos cibernéticos desde 2007, y el phishing representa más de un tercio de estos ataques. Estas estadísticas son particularmente preocupantes cuando se considera que solo el Pentágono recibe 10 millones de ciberataques cada día, y la mayoría de los principales bancos, instituciones financieras y organizaciones de medios informan cerca de 50.000 intrusiones cibernéticas cada día. Se han implicado ataques de phishing en delitos que van desde el robo de identidad y propiedad intelectual hasta el fraude financiero, el ciberespionaje y el hacktivismo, con pérdidas estimadas en más de 1.000 millones de dólares. Existe, pues, una urgente necesidad de abordar el problema del phishing desde una ley de aplicación, política pública y perspectiva de seguridad cibernética (Vishwanath et al., 2017).

Un ataque típico de phishing tiende a ser bastante simple y utiliza un breve correo electrónico que actúa como cebo con un hipervínculo incrustado o un archivo adjunto. El objetivo de tales ataques de enlaces y ataques de archivos adjuntos es para dirigir a las personas a sitios falsos o lanzar software espía en la computadora host. En estudios simulados, se ha demostrado que una sola campaña de correo electrónico de phishing victimiza al 50% de los destinatarios del correo electrónico; cuando se repite dos veces, la misma campaña tiende a generar el 80% de sus víctimas previstas. Según los estudiosos que estudian el phishing, estas altas tasas de victimización ocurren porque las personas no reconocen las pistas en los correos electrónicos que revelan el engaño. Esto ha llevado al desarrollo de intervenciones educativas dirigido a mejorar la capacidad de las personas para procesar cognitivamente y detectar señales engañosas dentro de los correos electrónicos de phishing (Albladi & Weir, 2018).

Sin embargo, investigaciones emergentes sugieren que el procesamiento de la información puede no ser el único determinante de la susceptibilidad al phishing. En una serie de estudios llamada Carronade Experimentos realizados en West Point, los cadetes del ejército fueron entrenados en varias formas para detectar eficazmente los correos electrónicos de phishing antes de someterlos a ataques de phishing reales. La investigación encontró que la educación y la capacitación solo

eran efectivas a corto plazo, con cualquier efecto que desaparezca en unas pocas horas después de que los cadetes volvieron a sus patrones habituales de uso del correo electrónico. En consecuencia, la mayoría de ellos eran phishing con éxito dentro de las cuatro horas posteriores a la administración de la intervención educativa. Esto sugiere que los patrones habituales de uso de los medios, un factor que aún no se ha considerado en la investigación del engaño, puede ser otro factor que contribuya al alto éxito de los ataques de phishing (Arévalo & Valarezo, 2022).

Un ataque puede tener resultados devastadores. Para las personas, esto incluye compras no autorizadas, el robo de fondos o el robo de identidad. Además, el phishing se usa a menudo para afianzarse en las redes corporativas o gubernamentales como parte de un ataque mayor, como un evento de amenaza persistente avanzada. En este último escenario, los empleados se ven comprometidos para eludir los perímetros de seguridad, distribuir malware dentro de un entorno cerrado u obtener acceso privilegiado a datos protegidos (Younis & Musbah, 2020).

Una organización que sucumbe a un ataque de este tipo suele sufrir graves pérdidas financieras además de una disminución de la cuota de mercado, la reputación y la confianza del consumidor. Según el alcance, un intento de phishing puede convertirse en un incidente de seguridad del que la empresa tendrá dificultades para recuperarse (Ross, 2017).

El phishing por correo electrónico es un juego de números. Un atacante que envía miles de mensajes fraudulentos puede obtener información importante y sumas de dinero, incluso si solo un pequeño porcentaje de los destinatarios cae en la estafa. Como se vio anteriormente, existen algunas técnicas que los atacantes utilizan para aumentar sus tasas de éxito (Albladi & Weir, 2018). Por un lado, harán todo lo posible para diseñar mensajes de phishing para imitar correos electrónicos reales de una organización falsificada. El uso de las mismas frases, tipos de letra, logotipos y firmas hace que los mensajes parezcan legítimos.

2.3.2. Tipos de phishing

Phishing de correo electrónico estándar: posiblemente la forma más conocida de phishing, este ataque es un intento de robar información confidencial a través de un correo electrónico que parece ser de una organización legítima. No es un ataque dirigido y puede llevarse a cabo en masa (Vishwanath et al., 2017).

Phishing de malware: utilizando las mismas técnicas que el phishing de correo, este ataque alienta a los objetivos a hacer clic en un enlace o descargar un archivo adjunto para que el malware se pueda instalar en el dispositivo. Actualmente es la forma más generalizada de ataque de phishing (Albladi & Weir, 2018).

Spear Phishing: donde la mayoría de los ataques de phishing arrojan una amplia red, este es un ataque bien investigado y altamente dirigido, generalmente enfocado en ejecutivos de negocios, personas públicas y otros objetivos lucrativos (Arévalo & Valarezo, 2022).

Smishing: el phishing habilitado para SMS ofrece enlaces cortos maliciosos a los usuarios de teléfonos inteligentes, a menudo disfrazados de avisos de cuentas, notificaciones de premios y mensajes políticos (Rathore et al., 2017).

Suplantación de identidad en motores de búsqueda: en este tipo de ataque, los ciberdelincuentes crean sitios web fraudulentos diseñados para recopilar información personal y pagos directos. Estos sitios pueden aparecer en resultados de búsqueda orgánicos o como anuncios pagados para términos de búsqueda populares (Albladi & Weir, 2018).

Vishing: el vishing, o phishing de voz, involucra a una persona que llama maliciosamente y pretende ser de soporte técnico, una agencia gubernamental u otra organización y trata de extraer información personal, como información bancaria o de tarjeta de crédito (Arévalo & Valarezo, 2022).

Pharming: también conocido como envenenamiento de DNS, el pharming es una forma técnicamente sofisticada de phishing que involucra el sistema de nombres de dominio (DNS) de Internet. El pharming redirige el tráfico web legítimo a una página falsificada sin el conocimiento del usuario, a menudo para robar información valiosa (Behimehr, 2018).

Clone Phishing: en este tipo de ataque, un actor sombrío compromete la cuenta de correo electrónico de una persona, realiza cambios en un correo electrónico existente intercambiando un enlace legítimo, un archivo adjunto u otro elemento con uno malicioso, y lo envía a los contactos de la persona para propagar la infección (Cwik & Margraf, 2017).

Ataque Man-in-the-Middle: un ataque man-in-the-middle consiste en un espía que supervisa la correspondencia entre dos partes desprevenidas. Estos ataques a menudo se llevan a cabo mediante la creación de redes WiFi públicas

falsas en cafeterías, centros comerciales y otros lugares públicos. Una vez que se une, el hombre en el medio puede phishing para obtener información o introducir malware en los dispositivos (Albladi & Weir, 2018).

BEC (compromiso de correo electrónico comercial): el compromiso de correo electrónico comercial implica un correo electrónico falso que parece ser de alguien en o asociado con la empresa del objetivo que solicita una acción urgente, ya sea transferir dinero o comprar tarjetas de regalo. Se estima que esta táctica causó casi la mitad de todas las pérdidas comerciales relacionadas con el ciberdelito en 2019 (Arévalo & Valarezo, 2022).

Malvertising: este tipo de phishing utiliza software de anuncios digitales para publicar anuncios de apariencia normal con código malicioso implantado en su interior (Albladi & Weir, 2018).

CAPÍTULO III

3. MARCO METODOLÓGICO

3.1. Diseño de investigación

El presente trabajo de investigación es de enfoque cuantitativo, de alcance descriptivo-correlacional, de corte transversal. Es de enfoque cuantitativo porque se van a utilizar datos para probar la hipótesis planteada previamente con base en la medición numérica y el análisis estadístico. Es de alcance descriptivo-correlacional porque busca especificar propiedades y características importantes del tema planteado, así como establecer la asociación entre las variables basados en la población de estudio (Hernández et al., 2017, p. 10).

3.2. Tipo de investigación

Investigación descriptiva

La investigación descriptiva tiene como objetivo describir de manera precisa y sistemática una población, situación o fenómeno. Puede responder preguntas de qué, dónde, cuándo y cómo, pero no preguntas de por qué (Gallardo, 2018).

Un diseño de investigación descriptivo puede usar una amplia variedad de métodos de investigación para investigar una o más variables. A diferencia de la investigación experimental, el investigador no controla ni manipula ninguna de las variables, sino que solo las observa y mide (Palacios, 2014).

Investigación correlacional

La investigación correlacional es un tipo de método de investigación no experimental en el que un investigador mide dos variables y comprende y evalúa la relación estadística entre ellas sin la influencia de ninguna variable extraña (Baena, 2017).

3.3. Población y muestra

La población estuvo conformada por profesionales de ciberseguridad de la ciudad de Quito.

La muestra lo conformaron 44 profesionales de ciberseguridad de la ciudad de Quito que cumplieron con los criterios de inclusión.

El muestreo empleado fue no probabilístico, se aplicó el instrumento en base a la disponibilidad de **participación de estudiantes** y profesionales de ciberseguridad.

Criterios de inclusión

- Profesionales de ciberseguridad de la ciudad de Quito.
- Profesionales que desearon participar en la investigación.
- Profesionales con más de un año de experiencia.
- **Estudiantes de ingeniería en ciencias de la computación**.

Criterios de exclusión

- Profesionales de ciberseguridad que no sean de la ciudad de Quito.
- Profesionales que no desearon participar en la investigación.
- Profesionales con menos de un año de experiencia.
- Estudiantes de otras carreras.

3.4. Técnicas e instrumentos de investigación

Se empleó el cuestionario de sesgos cognitivos y reflexibilidad cognitiva (Corral, 2019)**.** En la búsqueda de información no se encontró un instrumento que evalué los sesgos cognitivos relacionados a situaciones que enfrentan los profesionales de ciberseguridad, se crearon 18 ejemplos de escenarios en los que los profesionales de este campo deben tomar sus decisiones técnicas, y a través de sus respuestas se puede determinar la existencia de sesgos.

Para evaluar el test de los sesgos cognitivos se tomaron los valores de 0 como ausencia de sesgos cognitivos y 1 como presencia de sesgos cognitivos, posteriormente se sumaron todos los valores alcanzados en las 18 preguntas que contenía el test y se evaluaron los sesgos cognitivos en presencia de sesgos cognitivos y ausencia de sesgos cognitivos.

En el caso del test de reflexibilidad cognitiva se tomaron los razonamientos de las preguntas y se evaluaron **en razonamiento heurístico y razonamiento lógico**.

Plataforma de ejercicios para el caso del test de phishing se calificaron las **respuestas en aciertos y desaciertos, además se tomaron la cantidad de errores cometidos en el test.**

3.5. Análisis estadístico

Los datos obtenidos en esta investigación se procesaron con el empleo del utilitario estadístico SPSS versión 26 programa que se usa para los estudios sociales, por medio del cual fueron analizados los resultados obtenidos en el test de sesgos cognitivos, test de reflexibilidad cognitiva y el test de phishing. Al utilizar estos test de acuerdo a la escala de Likert, se consiguieron valores ordinales, lo que facilitó usar el coeficiente de correlación de Spearman, prueba no paramétrica utilizada para saber si existe asociación entre variables discretas.

3.6. Procedimiento

El test de sesgo cognitivo estuvo integrado por 18 preguntas que facilitó interpretar la forma en que los participantes procesaban pensamientos, emitir juicios y tomar decisiones.

El test de reflexibilidad cognitiva lo conformaron tres preguntas que permitieron determinar de acuerdo a las respuestas dadas por los participantes si tuvieron un razonamiento heurístico o lógico.

El test de phishing permitió determinar los aciertos en cada una de las interrogantes proporcionadas a los participantes.

3.7. Hipótesis

Las características del perfil cognitivo de los usuarios de internet influyen en la tarea de detección de correos phishing.

3.8. Operacionalización de las variables

Variables	Dimensiones	Indicadores	Instrumentos
Sesgos cognitivos “Conjunto de errores mentales predecibles que surgen de nuestra capacidad limitada para procesar la información de manera objetiva”	Ausencia de sesgos cognitivo	0	Cuestionario de sesgos cognitivos.
	Presencia de sesgos cognitivos	1	
Correos tipo phishing	Aciertos	A	Test de phishing

“Acto de enviar de forma electrónica y engañosa un correo para ponerse en contacto con una persona, con el fin de hacer que el individuo pueda realizar electrónicamente un hecho que sea beneficioso para el engañador y perjudicial para los engañados”	Errores	E	
Reflexibilidad cognitiva “Habilidad de la función ejecutiva empleada en la vida diaria que ayuda a usar la información de diversas maneras.	Razonamiento heurístico	RH	Test de reflexibilidad cognitiva.
	Razonamiento lógico	RL	

CAPÍTULO IV

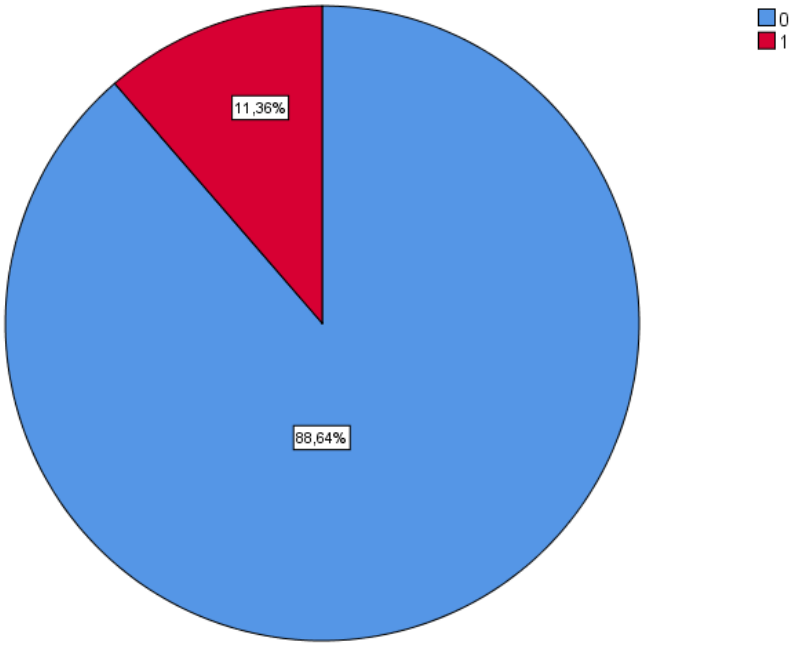
4. RESULTADOS

4.1. Sesgos cognitivos en Ciberseguridad

Tabla 2 Sesgos cognitivos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	0	39	88,6	88,6	88,6
	1	5	11,4	11,4	100,0
	Total	44	100,0	100,0	

Figura No. 1 Sesgos cognitivos

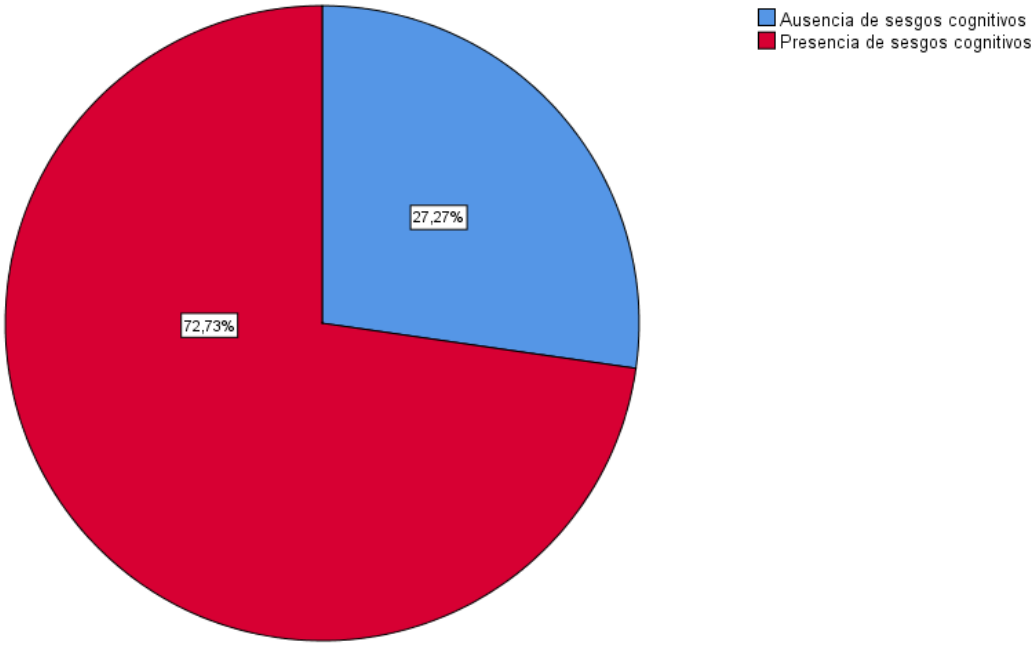


Los resultados de la investigación realizada de acuerdo al test de sesgos cognitivos se encontraron que el 88,6% presentaron ausencia de sesgos cognitivos y el 11,4% tenían presencia de sesgos cognitivos.

Tabla 3 Sesgo cognitivo total

Presencia de sesgos					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ausencia de sesgos cognitivos	12	27,3	27,3	27,3
	Presencia de sesgos cognitivos	32	72,7	72,7	100,0
	Total	44	100,0	100,0	

Figura No. 2 Sesgos cognitivos totales



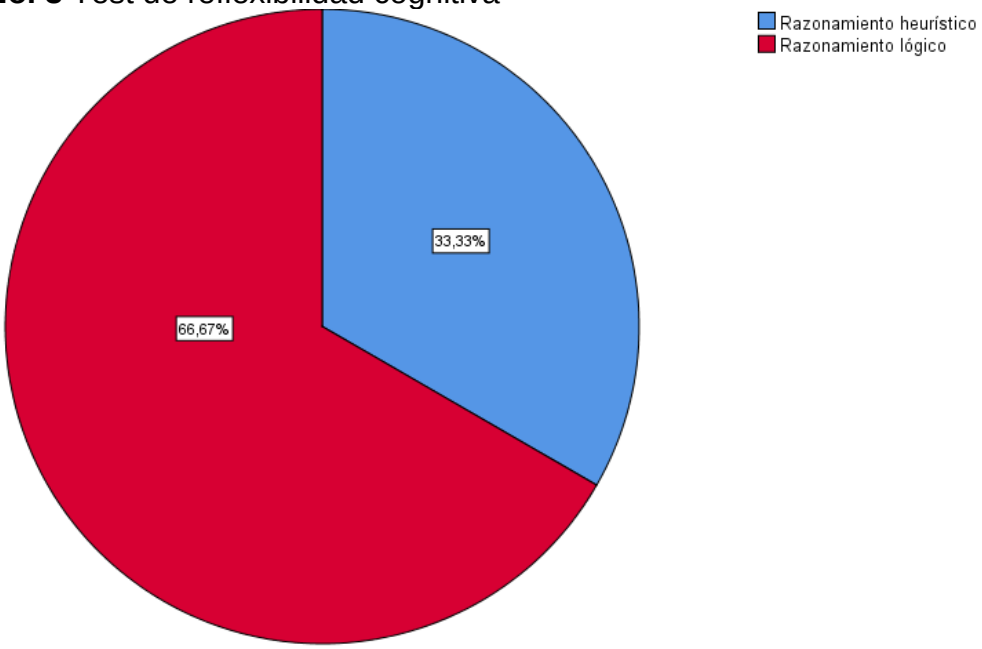
Los resultados de la investigación realizada de acuerdo a las respuestas obtenidas en el test de sesgos cognitivos se encontraron que el 72,7% tuvieron presencia de sesgos cognitivos y el 27,3% con ausencia de sesgo cognitivo.

4.2. Test de Reflexividad Cognitiva

Tabla 4 Test de reflexibilidad cognitiva

Razonamiento					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Razonamiento heurístico	14	33,3	33,3	33,3
	Razonamiento lógico	28	66,7	66,7	100,0
	Total	42	100,0	100,0	

Figura No. 3 Test de reflexibilidad cognitiva



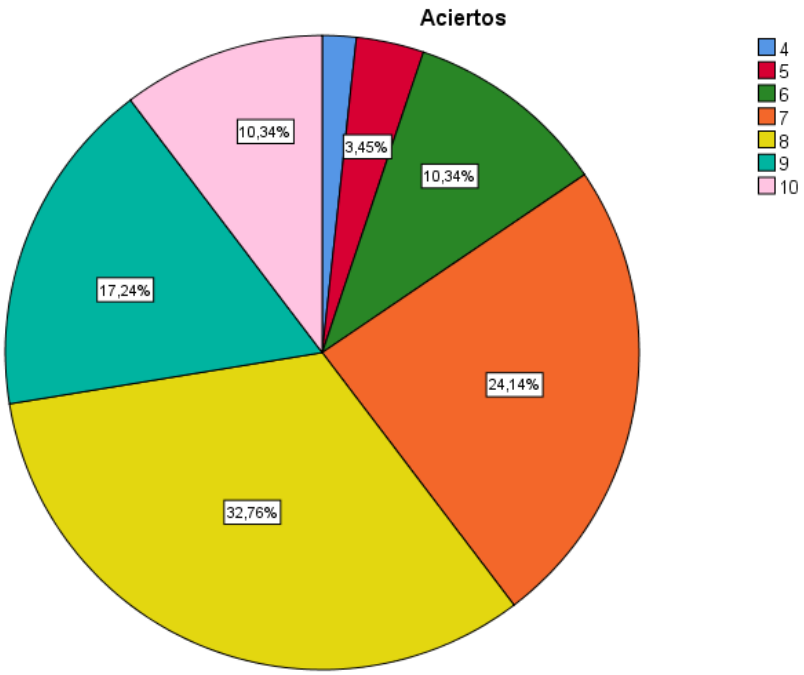
Los resultados de la investigación realizada de acuerdo a las respuestas obtenidas en el test de reflexibilidad cognitiva se encontraron que el 66,7% tuvieron razonamiento heurístico y el 33,3% razonamiento lógico.

4.3. Test de Phishing

Tabla 5 Aciertos del test de phishing

Aciertos					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	4	1	1,7	1,7	1,7
	5	2	3,4	3,4	5,2
	6	6	10,3	10,3	15,5
	7	14	24,1	24,1	39,7
	8	19	32,8	32,8	72,4
	9	10	17,2	17,2	89,7
	10	6	10,3	10,3	100,0
	Total	58	100,0	100,0	

Figura No. 4 Aciertos del test de phishing

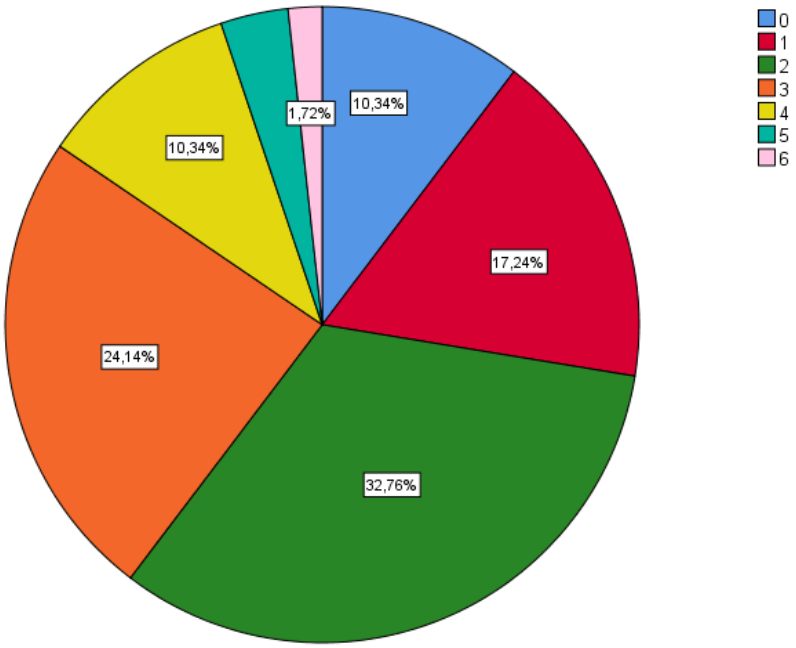


Los resultados de la investigación realizada de acuerdo a las respuestas obtenidas en el test de phishing se encontraron que el 32,8% tuvieron 8 aciertos, el 24,1% 7, el 17,2% 9 aciertos, el 10,3% tuvieron 10 y 6 aciertos respectivamente, el 3,4% 5 acierto y el 1,7% 4 acierto.

Tabla 6 Errores del test de phishing

Errores					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	0	6	10,3	10,3	10,3
	1	10	17,2	17,2	27,6
	2	19	32,8	32,8	60,3
	3	14	24,1	24,1	84,5
	4	6	10,3	10,3	94,8
	5	2	3,4	3,4	98,3
	6	1	1,7	1,7	100,0
	Total	58	100,0	100,0	

Figura No. 5 Errores del test de phishing



Los resultados de la investigación realizada de acuerdo a los errores obtenidos en el test de phishing se encontraron que el 32,8% tuvieron 2 errores, el 24,1% 3, el 17,2% 1 error, el 10,3% tuvieron 0 y 4 errores respectivamente, el 3,4% 5 errores y el 1,7% 6 errores.

4.4. Comprobación de la hipótesis

Hipótesis

Las características del perfil cognitivo de los usuarios de internet influyen en la tarea de detección de correos phishing.

Tabla 7 Correlación de Rho de Spearman de los sesgos cognitivos, reflexibilidad cognitiva y el Phishing

Correlaciones

			Reflexibilidad cognitiva	PHISHING	Sesgos cognitivos
Rho de Spearman	Reflexibilidad cognitiva	Coeficiente de correlación	1,000	,733	,812
		Sig. (bilateral)	.	,835	,681
		N	42	42	42
	PHISHING	Coeficiente de correlación	,733	1,000	,776**
		Sig. (bilateral)	,835	.	,800
		N	42	42	42
	Sesgos cognitivos	Coeficiente de correlación	,812	,776**	1,000
		Sig. (bilateral)	,681	,800	.
		N	42	42	42

**. La correlación es significativa en el nivel 0,01 (bilateral).

En el análisis de correlación de Rho de Spearman de los sesgos cognitivos, reflexibilidad cognitiva y el Phishing, se encontró que existe un alto grado de correlación entre los sesgos cognitivos, la reflexibilidad cognitiva y el phishing. Con lo que se demuestra que existe asociación entre estas variables estudiadas.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- Los resultados de la investigación muestran que la mayoría de los participantes han obtenido altos índices de presencia de sesgos cognitivos, lo que influye en la toma de decisiones que tienen que tomar en los problemas que se presentan en la vida diaria. El análisis de correlación muestra que existe una alta correlación entre los sesgos cognitivos, la reflexibilidad cognitiva y el correo phishing.
- De acuerdo al test de sesgos cognitivos se encontró que un alto porcentaje de los participantes en el estudio tenían presencia de sesgos cognitivos. Lo que les impiden a estos individuos poder valorar apropiadamente la situación actual y elegir la mejor opción. Demostrando que algunas decisiones tomadas por parte de estas personas son ilógicas y, en algunos casos, automáticamente emplean un mecanismo llamado error cognitivo.
- En el test de reflexibilidad cognitiva un porcentaje elevado tuvieron razonamiento heurístico. Lo que describe la tendencia del participante a utilizar la información que le llega a la mente rápida y fácilmente al tomar decisiones sobre el futuro.
- Con relación a las respuestas obtenidas en el test de phishing se encontraron que un porcentaje bajo tuvieron aciertos y un porcentaje alto errores. Al estudiar el comportamiento del ser humano hacia las amenazas en línea, es de suma importancia centrarse en la interacción entre los atributos del individuo, su contexto actual y la táctica de persuasión del mensaje.
- Las decisiones humanas están restringidas por mecanismos (por ejemplo, la memoria, la propagación de la activación, y el patrón emparejamiento) que reflejan las estadísticas y la dinámica del ambiente. Al manipular ese entorno, nuevos patrones pueden surgir que cambien el comportamiento del usuario.

5.2. Recomendaciones

- Se recomienda realizar otros estudios sobre los sesgos cognitivos, la toma de decisiones y el phishing.
- Es necesario realizar capacitaciones periódicas a los profesionales de ciberseguridad para que estén alertas a cualquier ataque cibernético.
- El diseño de un modelo cognitivo de detección de correos electrónicos de phishing por parte del usuario final puede ser útil para comprensión de la susceptibilidad humana a los ataques de phishing.
- Los conocimientos sugieren que la detección de correos electrónicos de phishing está influenciada por el historial previo de correos electrónicos del usuario final, su reciente experiencias y sus sesgos cognitivos innatos y aprendidos.

Bibliografía

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: the effects of human behaviors and demographics on each step of a phishing process . *IEEE Access, 10*(11). https://doi.org/https://doi.org/10.1109/ACCESS.2021.3066383

Afzal, W., & Thompson, K. (2017). Contributions of cognitive science to information science: an analytical synopsis. *Emporia State Res Stud , 47*(1), 18-23.

Alavi, R., Islam, S., Mouratidis, H., & Lee, S. (2015). "Managing Social Engineering Attacks – Considering Human Factors and Security Investment," Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance. *HAISA*, 161-171.

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

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security, 68*, 160-196. https://doi.org/doi:10.1016/j.cose.2017.04.006

Alper, O., Cagatay, C., Emrah, D., & Behcet, S. (2023). A hybrid DNN–LSTM model for detecting phishing URLs. *Neural Computing and Applications , 35*, 4957–4973 . https://doi.org/https://link.springer.com/article/10.1007/s00521-021-06401-z

APWG. (2014). Global Phishing Survey: Trends and Domain Name Use in 2H2014. *Working Group*, 245. http://www.antiphishing.org/download/document/245/APWG_Global_Phishing_Report_2H_2014.pdf

Arellano, J., & Solar, R. (2023). Disponibilidad Heurística. *Revista de Investigación en Tecnologías de la Información, 10*(20), 80-84. https://doi.org/DOI: https://doi.org/10.36825/RITI.10.20.007

Arévalo, D. A., & Valarezo, D. I. (2022). *Plataforma Web para entrenamiento de ataques de Phishing mediante seguridad y psicología.* ESPEC. http://repositorio.espe.edu.ec/jspui/bitstream/21000/32745/1/T-ESPE-052520.pdf

Baddeley, A., & Hitch, G. (2016). *Working memory. In: Bower GA (ed.) The psychology of learning and motivation: advances in research and theory.* New York: Academic Press.

Baena, G. (2017). *Metodología de la Investigación.* Grupo Editorial Patria. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf

Behimehr, S. (2018). *The role of cognitive biases in scientific information behavior of postgraduate students in Kharazmi University.* Tehran, Iran: University of Kharazmi.

Beldhuis, I. E., Marapin, R., & Jiang, Y. (2021). Cognitive biases, environmental, patient and personal factors associated with critical care decision making: A scoping review. *Journal of Critical Care, 64*, 144-153. https://doi.org/https://doi.org/10.1016/j.jcrc.2021.04.012

Berthet, V. (2022). The Impact of Cognitive Biases on Professionals' Decision-Making: A Review of Four Occupational Areas. *Front. Psychol, 2*(1), 243. https://doi.org/https://doi.org/10.3389/fpsyg.2021.802439

Bertino, E., & Ferrari, E. (2018). Big data security and privacy. In: A comprehensive guide through the Italian database research over the last 25 years. *Springer International Publishing, Berlin , 31*, 425–439.

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2015). Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails. *Australasian Conference on Information Systems*, 1-10. https://arxiv.org/ftp/arxiv/papers/1606/1606.00887.pdf

Cano, J. (2019). Seguridad cognitiva. Un paradigma emergente frente a la inseguridad de la información . *Revista Sistemas, 142*, 53-58.

Carpenter, P. (2022). *The five most popular cognitive biases that result in phishing attacks*. Phishing, Cybercrime: https://www.scmagazine.com/perspective/phishing/the-five-most-popular-cognitive-biases-that-result-in-phishing-attacks

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

Corral, L. (2019). *Validación del Cuestionario de Sesgos Cognitivos para la Psicosis (CBQp): Relación con sintomatología, insight y neurocognición.* Tarragona: Universitat Rovira Virgili. https://www.tesisenred.net/bitstream/handle/10803/670511/TESI%20L%C3%ADa%20Corral.pdf?sequence=1&isAllowed=y

Cwik, J., & Margraf, J. (2017). Information order effects in clinical psychological diagnoses. *Clin Psychol Psychother , 24*(1), 1142-1154.

Desolda, G., Ferro, L., Marrella, A., Catarci, T., & Costabile, F. (2021). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys, 54*(8), 1-35. https://doi.org/https://doi.org/10.1145/3469886

Ehrlinger, J., Readinger, W., & Kim, B. (2016). *Decision-Making and Cognitive Biases. Encyclopedia of Mental Health.* https://doi.org/10.1016/B978-0-12-397045-9.00206-8

Ehrlinger, J., Readinger, W., & Kim, O. (2016). Decision-Making and Cognitive Biases. *Elsevier*, 5-12. https://www.sciencedirect.com/science/article/pii/B9780123970459002068?via%3Dihub

Fan, Y., Xu, K., Wu, H., Zheng, Y., & Tao, B. (2020). Spatiotemporal modeling for nonlinear distributed thermal processes based on KL decomposition, MLP and LSTM network. *IEEE Access, 8*, 25111–25121.

Fonseca, D. (2017). *Ensaios sobre vieses cognitivos no processo de tomada de decisáo gerencial.* Universidade Federal de Lavras. http://repositorio.ufla.br/bitstream/1/15434/1/TESE_Ensaios%20sobre%20vieses%20cognitivos%20no%20processo%20de%20tomada%20de%20decis%C3%A3o%20gerencial.pdf

Franco, R. (2018). *The conjunction fallacy and interference effects.* https://doi.org/https://arxiv.org/pdf/0708.3948&ved

Gallardo, E. E. (2018). *Metodología de la Investigación.* Universidad Continental. https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

Garcia, M. E., & Padilla, G. A. (2022). *La Dramatización como estrategia para el desarrollo socio-emocional. UTC.* Pujilí Ecuador: Universidad Técnica de Cotopaxi (UTC). http://repositorio.utc.edu.ec/handle/27000/9059

Goel, D., & Jain, A. (2018). Mobile phishing attacks and defence mechanisms: state of art and open research challenges . *Comput Secur , 73*, 519-544.

Gomroki, G., Behzadi, H., Fattahi, R., & Fadardi, J. S. (2021). Identifying effective cognitive biases. *Journal of Information Science, 10*(3), 1-11. https://doi.org/DOI: 10.1177/01655515211001777

Gordon, J. (2022). *Cognitive Biases and Errors in Decision Making - Explained*. https://thebusinessprofessor.com/en_US/management-leadership-organizational-behavior/common-biases-and-errors-in-decision-making

Hakim, Z. M., Ebner, N. C., Oliveira, D., & Getz, S. (2021). The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. *Behav Res Methods, 53*(3), 1342–1352. https://doi.org/doi: 10.3758/s13428-020-01495-0

Haselton, M., Nettle, D., & Andrews, P. (2017). *The evolution of cognitive bias. In: Buss DM (ed.) The handbook of evolutionary psychology.* Hoboken, NJ: John Wiley & Sons.

Hernández, R., Fernández, C., & Baptista, P. (2017). *Metodología de la Investigación Científica.* McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V. https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Jing, R. (2021). A self-attention based LSTM network for text classification. 1207:012008. *J Phys Conf Ser, 17*(7), 208.

Kahan, D., Peters, E., Dawson, E., & Slovic, P. (2017). *Motivated Numeracy and Enlightened Self-Government.*

Kahneman, D., & Tversky, A. (2017). Prospect theory: analysis of decision under risk. *Econometrica, 18*(7), 183. https://doi.org/DOI:10.1142/9789814417358_0006

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *J Inf Secur Appl , 22*, 113–122.

Kumar, S., & Goyal, N. (2016). Evidence on rationality and behavioral biases in investment decision making. *Qual Res Financ Market, 8*(4), 270–287.

Lau, A., & Coiera, E. (2017). Do people experience cognitive biases while searching for information? . *J Am Med Inform Assoc, 14*(5), 599–608.

Lilienfeld, S. (2019). Ammirati R and Landfield K. Giving debiasing away: can psychological research on correcting cognitive errors promote human welfare? *J Assoc Psychol Sci , 4*(4), 390-398.

Lubin, P., Maciá, A., & Rubio de Lerma, P. (2005). *Psicología matemática I y II.* Madrid: UNED.

Nindao, R. (2022). *Heurística de Disponibilidad.* https://es.scribd.com/document/552494002/Heuristica-de-Disponibilidad

Ortiz-Garcés, I., Cazares, M., & Andrade, R. (2019). Detection of Phishing Attacks with Machine Learning Techniques in Cognitive Security Architecture. *International Conference on Computational Science and Computational Intelligence, 10*(9), 366-370. https://doi.org/doi: 10.1109/CSCI49370.2019.00071

Palacios, S. P. (2014). *Manual de investigación cualitativa. México, D. E.* Editorial Fontamara, S. A.

Park, M. (23 de February de 2023). *Prospect Theory*. https://corporatefinanceinstitute.com/resources/capital-markets/prospect-theory/

Rathore, S., Sharma, P., & Park, J. (2017). XSSClassifier: an efficient XSS attack detection approach based on machine learning classifier on SNSs. *J Inf Process Syst , 13*(4), 1014–1028.

Ross, A. (2017). *31 Mobile Marketing Statistics to Help You Plan for 2017.* iMPACT branding & design.

Ruiz, M., Diaz, M., & Villalobos, A. (2018). *What are cognitive bias and how to avoid them? (trans. Salazar A). Mnual de technicas de intervencion cognitive conductuales.* Bilbao: Desclee de Brouwer.

Tagg, J. (2018). *Cognitive distortion.* https://doi.org/http://daphne.palomar.edu/jtagg/cds.htm#cogdis

Torre, G., Rad, P., Choo, K., & Beebe, N. (2020). Detecting internet of things attacks using distributed deep learning. *J Netw Comput Appl , 163*, 662.

Torres, C. A. (2018). *Sesgos cognitivos y su relación con el bienestar psicológico en estudiantes universitarios de la ciudad de Ambato.* Pontificia Universisad Católica del Ecuador Sede Ambato. https://repositorio.pucesa.edu.ec/bitstream/123456789/2172/1/76594.pdf

Veksler, V., Buchler, N., Hoffman, B., Cassenti, D., Sample, C., & Sugrim, S. (2018). Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users. *Frontiers in Psychology, 9*(691). https://doi.org/ doi: 10.3389/fpsyg.2018.00691

Vijayaraghavan, M. (2022). 5 cognitive biases that affect your cybersecurity decisions. *ManageEngine*. https://www.manageengine.com/log-management/cyber-security/top-five-cognitive-biases-that-affect-your-security-posture.html

Vishwanath, A., Harrison, B., & Ng, Y. (2017). Suspicion, cognition, and automaticity model of phishing susceptibility. *Commun Res*, 1-21. https://doi.org/https://doi.org/10.1177/0093650215627483

Weems, C., Costa, N., & Watts, S. (2017). Cognitive errors, anxiety sensitivity, and anxiety control beliefs: their unique and specific associations with childhood anxiety symptoms. *Behav Modif , 31*(2), 174-201.

Wilke, A., & Mata, R. (2016). Cognitive bias. In: Ramachandran VS (ed.) Encyclopedia of human behavior. *London: Academic Press, 1*(1), 531–535.

Williams, E., Beardmore, A., & Joinson, A. (2017). Individual differences in susceptibility to online influence: a theoretical review. *Comput Hum Behav, 72*(1), 412–421. https://doi.org/https://doi.org/10.1016%2Fj.chb.2017.03.002

Williams, E., Hinds, J., & Joinson, A. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies, 120*, 1-13. https://doi.org/DOI:10.1016/j.ijhcs.2018.06.004

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

ANEXOS

ANEXO 1: DOCUMENTO DE CONSENTIMIENTO INFORMADO

INFORMACIÓN

Usted ha sido invitado(a) a participar en la investigación “Estudio de los sesgos cognitivos en el proceso de toma de decisiones, en la detección de correos phishing en profesionales de ciberseguridad de la ciudad de Quito”. Su objetivo es Identificar los sesgos cognitivos predominantes que influyen en la toma de decisiones y detección de los ataques de ingeniería social al momento de identificar correos tipo phishing. Usted ha sido seleccionado(a) por ser un profesional de ciberseguridad de la ciudad de Quito.

El investigador responsable de este estudio es Daniel Badillo, de la Universidad Politécnica Salesiana.

Para decidir participar en esta investigación, es importante que considere la siguiente información.

Participación: Tu participación consistirá en llenar el cuestionario de Sesgos Cognitivos, a quiénes se le invitará a la investigación, con el fin de identificar los sujetos potenciales. La entrevista/cuestionario/grupo focal durará alrededor de 30 minutos, y abarcará varias preguntas sobre diferentes temas.

Riesgos: Esta investigación no posee ningún tipo de riesgo.

Beneficios: Usted no recibirá ninguna recompensa por participar en este estudio. No obstante, su participación permitirá generar información para beneficio social.

Voluntariedad: Su participación es absolutamente voluntaria. Usted tendrá la libertad de contestar las preguntas que desee, como también de detener su participación en cualquier momento que lo desee. Esto no implicará ningún perjuicio.

Confidencialidad: Sus datos y opiniones serán confidenciales, y mantenidas en estricta reserva. En las presentaciones y publicaciones de esta investigación, no aparecerá asociado a ninguna opinión particular.

Conocimiento de los resultados: Usted tiene derecho a conocer los resultados de esta investigación. La forma en que se le hará llegar los resultados será por correo electrónico.

Datos de contacto: Si requiere mayor información, o comunicarse por cualquier motivo relacionado con esta investigación, puede contactar al investigador responsable de este estudio:

Nombre investigador responsable: Daniel Badillo.
Teléfonos:
Dirección:
Correo Electrónico:

FORMULARIO DE CONSENTIMIENTO INFORMADO

Yo, _____, acepto participar voluntariamente en el estudio “Estudio de los sesgos cognitivos en el proceso de toma de decisiones, en la detección de correos phishing en profesionales de ciberseguridad de la ciudad de Quito”.

Declaro que he leído y he comprendido las condiciones de mi participación en este estudio.

En caso de cualquier notificación relacionada a la investigación, pueden contactarme a través de:

Correo electrónico: _____
Teléfono: _____

_____ _____

Firma Participante Firma Investigador

Lugar y Fecha:

Este documento se firma en dos ejemplares, quedando una copia en poder de cada parte.

ANEXO No 2 Cuestionario para evaluar sesgos cognitivos en ciberseguridad
Responda las siguientes preguntas, teniendo en cuenta:
Sí (la probabilidad es alta). No (la probabilidad es baja)
1.Una empresa experimentó recientemente un ataque de phishing que resultó en el robo de datos confidenciales de los empleados. Unos meses después, el departamento de TI de la empresa propone una nueva solución de ciberseguridad que ayudaría a prevenir ataques similares en el futuro. Según el ataque reciente, ¿cree que la probabilidad de otro ataque de phishing exitoso es alta o baja?

2.Una organización experimentó recientemente un ataque de ransomware que resultó en el apagado completo de su red durante varios días. El equipo de ciberseguridad de la organización ha recomendado implementar una nueva solución de copia de seguridad y recuperación que podría ayudar a mitigar el impacto de futuros ataques. Según el ataque reciente, ¿Cree que la probabilidad de otro ataque exitoso de ransomware es alta o baja?

3.El departamento de TI de una empresa está evaluando la seguridad de sus sistemas y aplicaciones basados en la nube. Uno de los miembros del equipo sugiere que realicen una evaluación de vulnerabilidades y pruebas de penetración para identificar posibles debilidades. Otro miembro del equipo descarta esta sugerencia y afirma que nunca antes habían experimentado un ataque exitoso en sus sistemas en la nube. En base a la falta de ataques anteriores, ¿Cree que la probabilidad de un ataque exitoso a los sistemas en la nube de la empresa es alta o baja?

4.Una empresa está evaluando dos soluciones de ciberseguridad diferentes que pueden ayudar a proteger su red de ataques externos. La Solución A se comercializa como un paquete completo todo en uno que puede detectar y prevenir una amplia gama de amenazas. La Solución B se comercializa como la mejor solución especializada que sobresale en la detección y prevención de un tipo específico de amenaza. Según los mensajes de marketing, ¿Qué solución cree que es más eficaz?

5.Un experto en seguridad cibernética presenta un informe sobre los riesgos potenciales asociados con una nueva tecnología que la empresa planea adoptar. El experto presenta la información de dos maneras diferentes: una versión destaca los beneficios potenciales de la tecnología, mientras que la otra versión se enfoca en los riesgos potenciales. Según la forma en que se presenta la información, ¿cree que los riesgos asociados con la tecnología son altos o bajos?

6.Una empresa está evaluando dos proveedores de servicios en la nube diferentes que pueden alojar sus datos y aplicaciones. El Proveedor A enfatiza la seguridad de su plataforma, mientras que el Proveedor B enfatiza la facilidad de uso y la flexibilidad de su plataforma. Según los mensajes de marketing, ¿qué proveedor cree que es más seguro?

7.Una empresa está evaluando dos productos de software antivirus diferentes que afirman ofrecer el mismo nivel de protección. Un producto tiene una interfaz simple y fácil de usar, mientras que el otro producto tiene una interfaz técnica más

compleja. Según las interfaces, ¿Qué producto cree que será más efectivo para detectar y prevenir amenazas cibernéticas?

8.Un experto en ciberseguridad está presentando un informe sobre los riesgos potenciales asociados con un nuevo tipo de ataque cibernético que se está volviendo más común. El experto presenta la información de dos maneras diferentes: una versión usa jerga técnica y terminología compleja, mientras que la otra versión usa lenguaje simple y analogías. Según la forma en que se presenta la información, ¿Cree que los riesgos asociados con el nuevo ciberataque son altos o bajos?

9.Una empresa está evaluando dos administradores de contraseñas diferentes que afirman ofrecer el mismo nivel de seguridad. Un administrador de contraseñas tiene una interfaz familiar que es similar a otro software que usa la empresa, mientras que el otro administrador de contraseñas tiene una interfaz única y poco convencional. Según las interfaces, ¿Qué administrador de contraseñas cree que será más efectivo para proteger las contraseñas de la empresa de las ciberamenazas?

10.Un experto en seguridad sugiere que una empresa fije su presupuesto para seguridad cibernética en $100,000 para el año. Con base en esta sugerencia, ¿cree que la empresa debería aumentar, disminuir o mantener su presupuesto para ciberseguridad?

11.Un consultor de ciberseguridad le dice a una empresa que su sitio web tiene 5 vulnerabilidades conocidas que podrían ser explotadas por piratas informáticos. Según esta información, ¿Cree que la empresa debería priorizar la reparación de las 5 vulnerabilidades o solo las más críticas?

12.Un empleado recibe un correo electrónico de un colega que le pide que descargue y abra un archivo adjunto. El correo electrónico parece ser legítimo, pero el empleado no está seguro de si el archivo adjunto es seguro. El empleado nota que el correo electrónico se envió desde una dirección IP ubicada en un país conocido por los ataques cibernéticos. Según esta información, ¿Cree que es seguro descargar y abrir el archivo adjunto?

13.Un empleado recibe un correo electrónico de su gerente, que parece ser legítimo, pidiéndole que comparta sus credenciales de inicio de sesión para un sistema de la empresa. Según su conocimiento y experiencia en ciberseguridad, el empleado confía en que el correo electrónico es genuino y comparte su información de inicio de sesión. ¿Es probable que el empleado tenga un exceso de confianza en esta situación?

14.Un experto en ciberseguridad tiene la tarea de evaluar la seguridad de la red de una empresa. Después de completar la evaluación, el experto afirma que la red es completamente segura y no puede ser violada. ¿Es probable que el experto se confíe demasiado en esta situación?

15.El equipo de TI de una empresa instala un nuevo firewall que cree que brindará una protección completa contra todos los ataques cibernéticos. A pesar de las advertencias de otros expertos en seguridad, el equipo de TI confía en que su firewall es impenetrable. ¿Está usted de acuerdo?

16.El equipo de TI de una empresa tiene la política de usar software de código abierto para todos sus sistemas, a pesar de que hay varias opciones propietarias

disponibles. El equipo cree que el software de código abierto siempre es más seguro que el software propietario. ¿La decisión del equipo es adecuada?
17.El equipo de seguridad de una empresa ignora de forma rutinaria las posibles vulnerabilidades de seguridad que informan los empleados porque creen que los empleados no comprenden los riesgos de ciberseguridad tan bien como ellos. ¿Está usted de acuerdo?
18.Un empleado recibe un correo electrónico que parece ser un intento de phishing, pero decide ignorar las señales de advertencia y hace clic en el enlace porque cree que su conocimiento personal y experiencia en ciberseguridad es suficiente para evitar cualquier riesgo. ¿La decisión es adecuada?

ANEXO No 3 Test de Reflexividad Cognitiva
Conteste las siguientes preguntas

1.Un bate y una pelota cuestan 1,10 dólares en total. Sabiendo que el bate cuesta 1 dólar más que la pelota. ¿Cuánto cuesta la pelota?

Escriba su respuesta

2.Si cinco máquinas tardan cinco minutos en fabricar cinco objetos, ¿cuánto tiempo tardarían cien máquinas en fabricar cien objetos?

Escriba su respuesta

3.En un lago hay un grupo de nenúfares y cada día duplican su extensión. Sabiendo que tardan 48 días en cubrir todo el lago entero… ¿Cuánto tiempo tardarán en cubrir solo la MITAD?

Anexo No 5 TEST DE PHISHING

Nombre

Apellido

Profesión

- Estudiante
- Profesional

Género

- Masculino
- Femenino

Edad

Elija una opción

Codigo De La Clase

Elija una opción

Direccion

Correo Electrónico

Carrera

Elija una opción

Experiencia-Ciberseguridad

Elija los años