Universidad Internacional de La Rioja

Facultad de Ciencias de la Salud

Máster Universitario en Investigación en Psicología

Ciberpsicología, un análisis de los factores cognitivos que participan en el proceso de detección de amenazas informáticas: una revisión sistemática

Trabajo fin de estudio presentado por:	María Fernanda Cazares
Línea de investigación:	Revisión sistemática
Director/a:	Marta Gil Nájera
Fecha:	14 septiembre

Resumen

El presente estudio tiene como objetivo identificar los factores cognitivos que influyen en la detección de amenazas informáticas para lo cual se realizó una revisión sistemática de literatura utilizando la metodología PRISMA, en la búsqueda se obtuvo 37 artículos científicos de revista que muestren estudios experimentales en adultos, los resultados obtenidos fueron muy heterogéneos por los que se agruparon en tres funciones cognitivas que son funciones ejecutivas, percepción y aprendizaje, se puede observar que la detección de amenazas esta influenciada por las características del estímulo e interferencias en la tarea de detección, la forma en que se procesa en base a nuestras creencias sobre el riego cibernético que nos pueden llevar al uso de un procesamiento automático o inconsciente anulado las señales de sospecha que nos permiten detectar el engaño.

Palabras clave: (Factores cognitivos, phishing, seguridad cognitiva)

Abstract

The objective of this study is to identify the cognitive factors that influence the detection of computer threats, for which a systematic review of the literature was carried out using the PRISMA methodology, in the search 37 scientific journal articles were obtained that show experimental studies in adults, the results obtained were very heterogeneous for which they were grouped into three cognitive functions that are executive functions, perception and learning, it can be observed that the detection of threats is influenced by the characteristics of the stimulus and interferences in the detection task, the way in which that is processed based on our beliefs about cyber risk that can lead us to use automatic or unconscious processing that cancels the signs of suspicion that allow us to detect deception.

Keywords: (Cognitive factors, phishing, cognitive security)

Índice de contenidos

Índice de figuras

Índice de tablas

1. Introducción

Existe una gran cantidad de explicaciones sobre los procesos cognitivos en el campo de la psicología el proceso cognitivo mediante el cual los seres humanos detectamos las anomalías en situaciones de amenaza puede ayudar a mejorar las habilidades cognitivas de las personas que trabajan en el campo de la ciberseguridad, pero además es importante recalcar que todas las personas estamos expuestas a ser víctimas de ataques informáticos, por lo que recopilar los estudios que sean realizado entorno a los factores cognitivos puede permitir que todos y todas podamos realizar un entrenamiento o capacitación en esta dirección.

La pregunta de investigación que se planteó es ¿Cómo los factores cognitivos participan en el proceso de detección de amenazas informáticas?

El objetivo principal de esta investigación es crear un modelo teórico que explique los factores cognitivos y su relación en el proceso de detección de amenazas, en base a evidencias empíricas que se han desarrollado.

Los objetivos específicos son: Revisar la literatura existen en el campo de la ciberpsicología que esté relacionada a detección de amenazas. Plantear un protocolo para revisión sistemática de factores cognitivos en la detección y crear un modelo que recoja los principales factores cognitivos para ampliar el desarrollo de habilidades en detección de amenazas.

2. Marco teórico

Algunos estudios muestran los factores cognitivos que se actúan en el proceso detección o reconocimiento de patrones de anómalos o anomalías. La teoría de la detección de señales se fundamenta en el análisis de la señal (estimulo) y ruido que causa falsas alarmas, estos dos elementos presentados de forma individual y conjunta permite calcular el efecto perceptual por medio de distribuciones de probabilidad, a partir de este efecto la se darán la detección del estímulo en próximos ejercicios. Pueden existir tres tipos de criterios: liberal, neutral y conservador, los mismos que se pueden observar en la Curva de ROC (Goldstein, 2013).

2.1. Factores cognitivos

Kiebel et al. (2009) plantean que la información sensorial se genera de manera continua y fluida por lo que es difícil determinar las series temporales de su procesamiento, planteado la

existencia de secuencias dinámicas, que comparan la información previa y clasifica, este proceso se ve influenciado por la disonancia cognitiva, las personas pueden creer lo que es correcto, pero factores externos como opiniones de terceros o tendencias pueden hacerles decidir en sentido contrario. Por ejemplo, en el estudio titulado "Leveraging Behavioral Science to Mitigate Cyber Security Risk", discute aspectos como el Status Quo Bias o el Framing Effect en la toma de decisiones, (Mitre, 2020), los pensamientos futuros espontáneos podrían basarse en recuerdos o experiencias preelaboradas (Cole y Kvavilashvili, 2019). Sin embargo, el problema en el ámbito de la ciberseguridad es que estas experiencias o recuerdos pasados podrían ser falsos (falsos recuerdos) inducidos para los atacantes utilizando noticias falsas (Brown y Reavey, 2017) Por otro lado, los atacantes han perfeccionado sus técnicas de persuasión y tratan de aprovecharse de los factores emocionales que pueden alterar el juicio en los procesos de toma de decisiones (Valaskivi, 2018).

Este estudio pretende determinar los factores cognitivos asociados al ataque de Ingeniería Social, centrándose especialmente en el Phishing, entendido como un fraude que pretende obtener datos privados de los usuarios a través de Internet, especialmente para acceder a sus cuentas o datos bancarios, por eso es importante recolectar las evidencias de estudios empíricos sobre las representaciones sensoriales y el modelo interno que sigue la mente humana para detectar estímulos que pueden ser falsos, es importante en el campo de la ciberseguridad porque permitirá mejorar la formación en habilidades cognitivas, además de las técnicas.

Percepción de riesgo es una competencia que permite hacerle frente a las amenazas informáticas por medio de la conciencia sobre riesgos potenciales, el estudio de concluyo que la percepción de riesgo no disminuye la vulnerabilidad a los ataques de ingeniería social en redes sociales

Por otro lado, no hay que dejar de lado que en el ciberespacio todas y todas las personas estamos interactuando, con información ambigua o incompleta, lo que nos vuelve vulnerables por nuestra capacidad limitada para detectar información falsa. Una revisión sistemática es el punto de partida para diseñar un modelo de factores neurocognitivos que se pueden estimular y entrenar para disminuir los límites de la capacidad de detección de anomalías.

Existen revisiones de literatura sobre factores humanos en las que se analizan todas las variables humanas que influyen en la vulnerabilidad a las amenazas informáticas, también

existen revisiones sistemáticas sobre computación cognitiva. No hay una revisión de literatura que recoja todas las evidencias sobre el estudio de factores cognitivos que participan la detección de amenazas informáticas.

2.2. Amenazas informáticas

Algunos ataques informáticos se centran más en las vulnerabilidades de los seres humanos. Un estudio de Chang y Chong en el 2010 identificó que los fraudes por correo electrónico se basan en la influencia de factores psicológicos a través del uso por parte de los atacantes de la suplantación de personas u organizaciones, la influencia de un sentido de autoridad o urgencia, y la provisión de un cierto nivel de legitimidad. A este tipo de ataques se le denomina de ingeniería social pueden manejar el uso de un lenguaje que muestre autoridad para las personas y presentar una apariencia formal que parezca provenir de un CEO o CIO; mientras que otros buscan generar una sensación de oportunidad limitada, como ofertas de viajes (Butavicius, Parsons, Pattinson, y McCormac, 2016). Durante la pandemia, los atacantes se adaptaron a este contexto y los ataques empezaron a utilizar como contenido temas relacionados con la COVID-19 como el número de infectados, posibles tratamientos, vacunas, ofertas de equipos médicos.

Según el Foro Económico Mundial en su Informe sobre Riesgos Globales (MITRE, 2023), los ataques a la ciberseguridad han sido considerados entre las diez amenazas con mayor impacto en el mundo.

Podemos observar que los atacantes buscan adaptar su ataque a la realidad de las personas para intentar persuadirlas de que realicen una acción. Jones et al., (2015) mencionan tres aspectos relacionados con las influencias psicológicas en el proceso de toma de decisiones por correo electrónico. En primer lugar, la capacidad de persuasión del mensaje de correo electrónico. En segundo lugar, el proceso cognitivo para juzgar la legitimidad del correo electrónico. Por último, la influencia teórica basada en las diferencias individuales. La influencia de las personas está vinculada a creencias culturales, ideológicas, éticas, valores y sesgos sociales, y a factores de información disponible que determinan los filtros mentales que se utilizan para procesar la información (Chai, 2020).

3. Marco Metodológico

Se aplicaron las once etapas de la metodología PRISMA para revisión sistemática, en apéndices se encuentra el protocolo desarrollado que fue utilizado en esta revisión sistemática de literatura y la valoración de la calidad de los artículos por medio de la matriz de sesgos (sesgo de selección, sesgo de resultados, sesgo de realización, sesgo de desgaste, sesgo de notificación y sesgo de detección).

Para la aplicación de los criterios de inclusión y exclusión se utilizó la plataforma Ryyan y para la extracción de datos una matriz de Excel con las variables identificadas en los artículos.

3.1. Estrategia de búsqueda

Se realizó la búsqueda en junio 2022, en inglés y español, con los siguientes términos (para profundizar en el proceso seguido consultar Anexo B)

La búsqueda se realizó entre abril y mayo del 2023 en las bases de datos académicas que se describen a continuación con las siguientes claves de búsqueda(Tabla 7)

Tabla 1. Claves de búsqueda

Base de datos	Ecuación de búsqueda	/Documentos encontrados	Artículos seleccionados	Revisión título (excluidos)	Quitar duplicado	Restricciones
Scopus	cognitive AND factors AND in AND cyber AND attack AND detection	13	4	9		Artículos de revista
Springer	'cognitive AND factors AND in AND cyber AND attack AND detection'	622	7	615		Artículos de revista
Web of science	cognitive AND factors AND in AND cyber AND	3	2	1		Artículos de revista

	attack AND detection				
IEEE	cognitive AND human AND factors OR cyberattacks	1421	17	1404	Tema de publicación: cognición Artículos de revista
Science Direct	Cognitive factors in human detection of cyberattacks	307	8	299	
TOTAL		2366	38	2328	

3.2. Criterios de inclusión

Se incluirán estudios con un diseño cuantitativo de tipo experimental, cuasiexperimental que muestre evidencias empíricas sobre factores cognitivos aplicados al contexto de la ciberseguridad.

Los estudios tendrán como variables los factores cognitivos básicos y superiores que participan en el proceso de detección de amenazas informáticas.

La población de los estudios que se incluyen serán adultos de 18 a 65 años.

El rango de fechas no tiene una restricción de años, puesto que el objetivo es recolectar la mayor cantidad de las evidencias empíricas.

Se incluirá estudios de todos los países del mundo.

Los estudios deben estar publicados en inglés y haber pasado por una revisión de pares.

3.3. Criterios de exclusión

Se excluyen los artículos que tengan como participantes niños, niñas, adolescentes y adultos mayores.

Se excluyen artículos que no tengan claridad y coherencia en sus resultados y que no hayan sido sometidos a una revisión por pares.

Artículos que tengan un diseño no experimental o mixto.

Contextos de estudio que no correspondan a ciberseguridad o ataques informáticos.

Protocolo

INTRODUCCIÓN

Conocer el proceso cognitivo mediante el cual los seres humanos detectamos las anomalías en situaciones de amenaza puede ayudar a mejorar las habilidades cognitivas de las personas que trabajan en el campo de la ciberseguridad, pero además es importante recalcar que todas las personas estamos expuestas a ser víctimas de ataques informáticos. La revisión sistemática puede ayudar a cualquier persona adulta que puede ser víctima de ataques informáticos, incluidos los profesionales de ciberseguridad con el objetivo de mejorar los procesos de entrenamiento cognitivo, para reducir la vulnerabilidad o aumentar los obstáculos a los atacantes.

Pregunta de investigación

¿cómo los factores cognitivos participan en el proceso de detección de amenazas?

Participantes

Adultos de 18 a 65 años, de género femenino y masculino que tengan salud mental y buen desempeño de los factores cognitivos del proceso de detección

Experimentos y cuasiexperimentos que describa los factores cognitivos básicos y superiores que participan y se relacionan en la detección de amenazas

Metodología

Criterios de inclusión

Se incluirán estudios con un diseño cuantitativo de tipo experimental, cuasiexperimental que muestre evidencias empíricas.

Los estudios tendrán como variables los factores cognitivos básicos y superiores que participan en el proceso de detección de amenazas informáticas.

La población de los estudios que se incluyen serán adultos de 18 a 65 años.

El rango de fechas no tiene una restricción de años, puesto que el objetivo es recolectar todas las evidencias empíricas.

Se incluirá estudios de todos los países del mundo.

Los estudios deben estar publicados en inglés y haber pasado por una revisión de pares.

Criterios de exclusión

Se excluyen los artículos que tengan como participantes niños, niñas, adolescentes y adultos mayores.

Se excluyen artículos que no tengan claridad y coherencia en sus resultados y que no hayan sido sometidos a una revisión por pares.

Los artículos que tengan un diseño no experimental.

La investigación no se ha realizado en el campo de ciberseguridad

Estrategia de búsqueda

La búsqueda se realizará en abril del 2023 de artículos de investigación de las bases de datos académicas: Web of Science, Scopus, IEEE y Springer.

Cognitive Vulnerability

Palabras claves en Scopus

13 result

cognitive AND factors AND in AND cyber AND attack AND detection

Palabras claves en Springer

622 Result(s) for 'cognitive AND factors AND in AND cyber AND attack AND detection'

within Article

La información se gestionará a través de Mendeley y la plataforma RYYAN

Valoración de la calidad de los artículos

Sesgo de selección

Sesgo de resultados

Sesgo de realización

Sesgo de desgaste

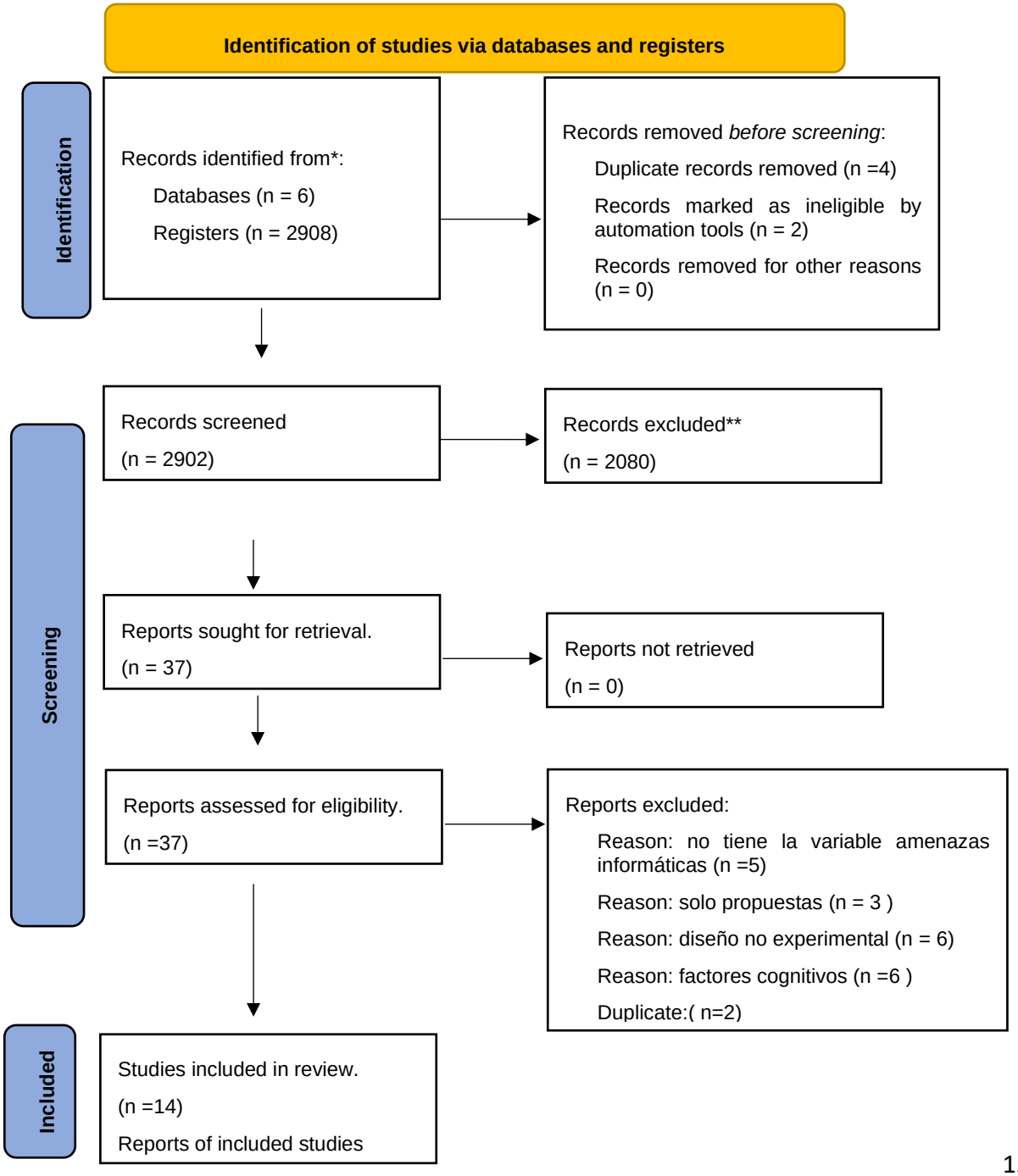
Sesgo de notificación

Sesgo de detección

3.4. Procedimiento y extracción de datos

Se aplicaron las estrategias de búsqueda señaladas y los artículos identificados se almacenaron en el gestor bibliográfico Mendeley, se incluyó 2902, En la revisión de títulos y resúmenes se excluyeron 2080 porque no encajaban en el objetivo de la revisión, Quedaron 37 artículos de los que se realizó la lectura completa. De los cuales, se excluyeron 23 por no cumplir con los criterios de inclusión, quedaron 14 artículos que son parte del estudio. En una matriz de Excel se extrajo el contenido de cada uno y se realizó el estudio de calidad.

Figura 1. *Flujograma del proceso de selección e inclusión de estudios.*



4. Resultados

En el programa Jamovi se procesaron datos descriptivos sobre las características de la muestra de los estudios seleccionados.

Tabla 2. Descriptivos

	Tipo de muestra	Tamaño de la muestra	Media de edad
N	14	14	6
Media		704	28.4
Median		238	27.6
Desviación estándar		1773	8.45
Minimum		25	20.0
Maximum		6839	40.0

Fuente: elaboración propia

Tabla 3: Frecuencias tipo de muestra

Tipo de muestra	Counts	% of Total	Cumulative %
Probabilística	9	64.3 %	64.3 %
No probabilística	2	14.3 %	78.6 %
Desconocido	3	21.4 %	100.0 %

Fuente: elaboración propia

Tabla 4. Frecuencias de factor cognitivo

Factor cognitivo	Counts	% of Total	Cumulative %
Toma de decisiones	3	21.4 %	21.4 %

Procesamiento de la información	5	35.7 %	57.1 %
Percepción	6	42.9 %	100.0 %

Fuente: elaboración propia

5.1 Características de los artículos

Los artículos seleccionados tienen un promedio de tamaño muestral 704 con una edad media de 38 años, todos son diseños experimentales con 64.43% de muestras aleatorizadas (Tabla 2), lo que nos permite tener un grado de confianza en los resultados de los artículos, en la evaluación de riesgo de sesgo tenemos un % de bajo riesgo.

En la revisión sistemática los artículos seleccionados son heterogéneos en cuanto al factor cognitivo que se investiga por lo que se los agrupo en toma de decisiones, procesamiento heurístico y percepción. Se obtuvo 21.4% de artículos sobre toma de decisiones, 35.7% sobre procesamiento de la información y 42.9% sobre percepción (Tabla 3).

5.2 Resultados de medición de la detección de amenazas en cada factor cognitivo

En el factor cognitivo de toma de decisiones vemos que la medición de la detección de amenazas se realiza con juegos de sistema de detección de intrusos, señal de resonancia magnética funcional y simulación de correos electrónicos; los diseños experimentales, se enfocan a las estrategias de Penetration Testing y Web Shell Exploit que, usadas por atacantes y defensores, las tareas de detección de sitios web falsos o reales, simulación de correos electrónicos phishing en ambientes reales.

El factor cognitivo de procesamiento de la información Harrison et al., (2016) en el experimento busca replicar las condiciones más realistas usando mensajes de correo electrónico basados en el miedo o la recompensa y la presencia o ausencia de señales de filtración para evaluar el tipo de procesamiento, , Luo et al., (2013) usa mensajes de correo electrónico que fomente el procesamiento heurístico y supriman el procesamiento sistemático, Butavicius et al., (2022) plantea el uso de dos factores experimentales presencia o ausencia de las pistas de personalización y mecánicas engañosas, así como límites de tiempo,

escenarios de red con diferentes riesgos y oportunidades en el proceso de defensa, así como el uso de herramientas como el Cofense PhishMe para simular los correos phishing

En el factor cognitivo de percepción se aplicaron escalas para evaluar hábitos de usuarios en las redes sociales, mediante un rastreador visual se evalúan el número de fijaciones oculares en las advertencias de seguridad, En base a escenarios se respondieron preguntas, tarea de clasificación y encuesta en línea para determinar si un correo es real o phishing.

5.3 Resultados de los factores cognitivos

La toma de decisiones se ve influenciada por la expectativa sobre el funcionamiento de los sistemas de detección de intrusos tanto en defensores como en atacantes, tareas de seguridad informática activan áreas de toma de decisiones, atención y resolución de problemas, se observa que una mayor atención a la información reconocida y obviar información nueva como el cuerpo del mensaje, es una condición que se debe considerar en el estudio de la detección de amenazas informáticas los efectos del mensaje miedo o recompensa, así como las señales de filtración no influyeron significativamente en la detección.

En el proceso de detección influyen el proceso de análisis detallado de la información y la conexión con el conocimiento previo.

Harrison et al., (2016) en el estudio del procesamiento de la información encontró una correlación positiva entre la elaboración de un mensaje de texto y la atención.

Tabla 5. Factor cognitivo: *Toma de decisiones*

Autor	Tipo de muestra	Tamaño de la muestra	Media de edad	Medida de detección de amenazas informáticas	Experimento	Análisis estadísticos	Riesgo de sesgo	Análisis cualitativo
Aggarwal et al., (2022)	Probabilística	136	34 años	juego de IDS Sistema de Detección de Intrusos	En el primer experimento, los participantes actuaron como atacantes y tuvieron que explotar vulnerabilidades en un sistema informático protegido por una de dos estrategias de defensa: PT (Penetration Testing) o WSE (Web Shell Exploit). En el segundo experimento, los participantes actuaron como defensores y tuvieron que proteger un sistema informático contra ataques realizados por atacantes humanos o automatizados. Los defensores utilizaron una de dos estrategias de enmascaramiento: PT o WSE		Riesgo bajo	La toma de decisiones del atacante y defensor se ve influenciadas por los fallos y falsas alarmas que cada uno realiza. Los atacantes y los defensores confiaron en la información de alerta del sistema de detección de intrusos. Almacenar una expectativa sobre la precisión de los IDSs en sus memorias influye en las acciones de atacantes y defensores.
Autor	**Tipo de muestra**	**Tamaño de la muestra**	**Media de edad**	**Medida de detección de amenazas informáticas**	**Experimento**	**Análisis estadísticos**	**Riesgo de sesgo**	**Análisis cualitativo**
Neupane et al., (2016)	No probabilística	25	21.5 años	señal de resonancia magnética funcional (fMRI)	Se presentaron a los participantes diferentes	Pruebas t y análisis de varianza (ANOVA)	Riesgo bajo	El estudio encontró que los participantes mostraron una actividad cerebral significativa en regiones clave asociadas con la

			tareas de seguridad informática (12 tareas falsas fáciles, 13 tareas falsas difíciles y 14 tareas reales). Cada tarea se presentó en forma de una captura de pantalla de un sitio web durante 6 segundos, seguida de una pausa de 6 segundos. Los participantes debían indicar si el sitio web era real o falso utilizando un joystick. Además, se incluyó una condición de línea base de fijación en la que los participantes se relajaban y miraban una cruz en la pantalla durante 10 segundos. Se registraron las respuestas y los	para comparar las diferencias en la actividad cerebral entre las diferentes condiciones de las tareas de seguridad informática.	toma de decisiones, la atención y la resolución de problemas durante la realización de tareas de seguridad informática. Además, se descubrió que ciertos rasgos individuales, como la impulsividad, tienen un efecto negativo significativo en la activación cerebral en estas tareas.

					tiempos de respuesta de los participantes.			
Autor	**Tipo de muestra**	**Tamaño de la muestra**	**Media de edad**	**Medida de detección de amenazas informáticas**	**Experimento**	**Análisis estadísticos**	**Riesgo de sesgo**	**Análisis cualitativo**
Greitzer, et al. 2021	Probabilística	6938	27-41 años	Correos electrónicos simulados de phishing	Durante un período de 3 semanas, Las semanas de estudio comenzaron los martes y terminaron los lunes. Las campañas de correo electrónico, dando a cada correo electrónico al menos una semana completa para abrirlo y hacer clic en él por cada usuario. Registramos el sistema operativo y el tiempo de los clics para poder vincular el haga clic en el comportamient	medias, desviaciones estándar, razones de probabilidades y niveles de significancia	Riesgo bajo	Los participantes tendieron a centrarse en la información reconocida (encabezados y pies de página con logotipos y firmas) y descuidar la información nueva (cuerpo del texto) antes de tomar una decisión de confianza. Las experiencias previas de haber experimentado un ataque de phishing aumentan la probabilidad de detectar

	o de los datos de TI e identifique indicadores técnicos que sugieran la susceptibilidad al phishing	correos electrónicos de phishing.

Fuente: Elaboración propia.

Tabla 6. Factor cognitivo: *Procesamiento de la información.*

Autor	Tipo de muestra	Tamaño de la muestra	Media de edad	Medida de detección de amenazas informáticas	Experimento	Análisis estadísticos	Riesgo de sesgo	Análisis cualitativo
Harrison et al., (2016)	Probabilística	194	20 años	Cuestionario sobre Procesamiento de la información: elaboración y atención. Cuestionario sobre conocimiento de correo electrónico y phishing	El objetivo del experimento era examinar cómo el procesamiento cognitivo, junto con los factores a nivel de mensaje y a nivel individual, influyen en la victimización de phishing. El estudio buscaba replicar de manera más realista las condiciones en las que los usuarios se encuentran en la vida cotidiana al recibir correos electrónicos de	Regresión y correlaciones	Riesgo Bajo	Elaboración y atención: Se encontró una correlación significativa entre la elaboración de texto y la atención de los participantes hacia los elementos del

		phishing, sujetos de 2x2 con dos tipos de mensajes de correo electrónico (basados en el miedo o en la recompensa) y dos tipos de señales de filtración (presentes o no presentes). Los correos electrónicos de los participantes se asignaron aleatoriamente a una de estas cuatro condiciones de correo electrónico.	mensaje. Aquellos participantes que mostraron mayor elaboración del mensaje también prestaron más atención a los elementos del mensaje. Efecto de los mensajes y señales de filtración: No se encontró evidencia de que los tipos de mensajes de correo electrónico (basados en el miedo o en la recompensa) o las señales de

				filtración (presentes o no presentes) tuvieran un efecto significativo en la elaboración del mensaje. Influencia del conocimiento subjetivo y objetivo: Se encontró que el conocimiento subjetivo y objetivo sobre el phishing tenía un impacto significativo en la elaboración del mensaje. Los participantes con un mayor

								conocimiento subjetivo y objetivo mostraron una mayor elaboración del mensaje.
Autor	**Tipo de muestra**	**Tamaño de la muestra**	**Media de edad**	**Medida de detección de amenazas informáticas**	**Experimento**	**Análisis estadísticos**	**Riesgo de sesgo**	**Análisis cualitativo**
Luo et al., (2013)	No probabilístico	105		ejercicio pretendía medir la susceptibilidad del cuerpo docente y del personal y la eficacia del phishing selectivo. La suplantación de	La primera fase implicó la creación de un mensaje que lograra dos objetivos: Incorporar múltiples técnicas para	Regresión logística	Bajo riesgo	El método analítico de datos es insuficiente para captar el efecto niveles de necesidad de cognición, conjeturamos que los

	identidad (spear phishing)	fomentar el procesamiento heurístico incorrecto o sesgado y suprimir el procesamiento sistemático. Sobrevivir al menos al procesamiento sistemático mínimo si no se lograba el primer objetivo. La segunda fase consistió en incluir un hipervínculo dentro del correo electrónico para que la víctima completara una encuesta sobre	mensajes de phishing que tienen menos necesidad de cognición podrían justificar aún más el éxito de este ataque de phishing. La elaboración del correo se refiere a la frecuencia de los participantes en el procesamiento cognitivo profundo del contenido del correo electrónico, particularmente el proceso de considerar

					eventos actuales en la institución. El objetivo era obtener las credenciales de inicio de sesión y contraseña del personal y el cuerpo docente, tal como lo haría un ciberdelincuente.			cuidadosamente los méritos de la información del correo electrónico y conectar estas señales con el conocimiento previo, las experiencias y las creencias.
Autor	**Tipo de muestra**	**Tamaño de la muestra**	**Media de edad**	**Medida de detección de amenazas informáticas**	**Experimento**	**Análisis estadísticos**	**Riesgo de sesgo**	**Análisis cualitativo**
Butavicius et al., (2022)	Probabilística	472	40 años	Tasa de aciertos (proporción de correos electrónicos de phishing clasificados correctamente) y la	Tarea de clasificación de correos electrónicos, en la que los participantes	El estudio también utilizó análisis de regresión lineal múltiple para examinar cómo estas variables predecían la capacidad de los participantes para distinguir	Bajo riesgo	Se encontró que la precisión general de los participantes en la tarea de clasificación de correos electrónicos fue solo del 56%, con una

		tasa de falsas alarmas (proporción de correos electrónicos legítimos clasificados incorrectamente como sospechosos). El sesgo de respuesta (B'') se calculó a partir de la tasa de falsas alarmas y la tasa de omisiones (proporción de correos electrónicos de phishing clasificados incorrectamente como legítimos	debían identificar si cada correo era legítimo o un intento de phishing. Se manipularon dos factores experimentales: la presencia o ausencia de pistas de personalización y mecánicas engañosas en los correos electrónicos, y la presencia o ausencia de límites de tiempo para responder a cada correo electrónico. Los participantes fueron	entre correos electrónicos de phishing y correos electrónicos genuinos (A') y su sesgo hacia declarar un correo electrónico de phishing (B''). Además, el estudio utilizó pruebas t y ANOVA para comparar los efectos de diferentes condiciones experimentales en el rendimiento de detección de phishing de los participantes.	tasa de aciertos promedio del 42% y una tasa promedio de falsas alarmas del 31%. Esto significa que los participantes identificaron correctamente solo el 42% de los correos electrónicos de phishing, mientras que identificaron erróneamente el 31% de los correos electrónicos legítimos como phishing. Además, 25 de los participantes (5.3%) no identificaron correctamente un solo correo electrónico de phishing en todo el experimento, y solo 11 (2.6%) identificaron los 12 correos electrónicos de phishing. El estudio también encontró que la

					asignados aleatoriamente a uno de los ocho grupos experimentales y se les presentó una secuencia única y aleatoria de 36 correos electrónicos, incluyendo un correo electrónico de verificación para controlar la atención.			aplicación de un plazo (presión de tiempo) condujo a una reducción en la capacidad de discriminación de 0.597 a 0.5164, lo que equivale a una disminución del 5.1% en la precisión de las personas para juzgar los correos electrónicos. En general, el estudio destaca la necesidad de una mejor capacitación y estrategias para inhibir el uso de heurísticas y activar un modo de pensamiento más analítico al procesar correos electrónicos.
Autor	**Tipo de muestra**	**Tamaño de la muestra**	**Media de edad**	**Medida de detección de amenazas informáticas**	**Experimento**	**Análisis estadísticos**	**Riesgo de sesgo**	**Análisis cualitativo**

Woods et al., (2022)	Probabilístico	91	____	una interfaz de usuario que permitía a los participantes asignar recursos a diferentes componentes de la red mediante un menú desplegable. Esta interfaz se utilizó en los cinco escenarios de red presentados a los participantes. Los investigadores recopilaron datos sobre las decisiones de asignación de recursos tomadas por los participantes en cada escenario y utilizaron estos datos para analizar el impacto de la ponderación de probabilidad no lineal y otros sesgos en las	Es un experimento de laboratorio incentivado que utiliza una tarea de defensa de red para evaluar cómo la ponderación no lineal de la probabilidad afecta las decisiones de asignación de recursos de defensa de red. El experimento utilizó cinco escenarios de red diferentes, cada uno de los cuales presentaba diferentes riesgos y oportunidades	Regresiones censuradas de tipo Tobit para analizar el impacto de la ponderación de probabilidad no lineal y otros sesgos en las estrategias de defensa.	Bajo riesgo	Los resultados sugieren que las decisiones de defensa de red están influenciadas por una serie de sesgos cognitivos y que la comprensión de estos sesgos puede ser importante para mejorar la efectividad de la defensa de red.

				estrategias de defensa.	de defensa. Los sujetos jugaron cada uno de los cinco escenarios de red 10 veces consecutivas para permitir cierto aprendizaje y retroalimentación.			
Autor	**Tipo de muestra**	**Tamaño de la muestra**	**Media de edad**	**Medida de detección de amenazas informáticas**	**Experimento**	**Análisis estadísticos**	**Riesgo de sesgo**	**Análisis cualitativo**
Buckley et al., (2023)	Probabilística	590		Se registraron dos respuestas a los correos electrónicos de phishing para capturar comportamientos cibernéticos	Los participantes fueron asignados al azar para recibir uno de los cuatro correos electrónicos de phishing: Actividad sospechosa, Paquete no entregado, Recompensa o PDF	Media, desviación estándar y regresión logística binaria multivariante	Riesgo bajo	Confianza en la intuición sobre un correo electrónico de phishing aumenta la resistencia a un ciberataque lo que nos dice que las formas automáticas de procesamiento pueden influir positivamente en el grado de sospecha.

		riesgosos y seguros. El comportamiento cibernético riesgoso se operacionalizó como una respuesta de "Hacer clic". Los participantes se consideraron que habían mostrado un comportamiento cibernético riesgoso si abrían el correo electrónico de phishing y hacían clic en uno de los tres enlaces dentro del correo electrónico. Una respuesta de "Hacer clic" se	recibido. Los correos electrónicos de phishing se diseñaron y enviaron a las direcciones de correo electrónico de las empresas de los participantes mediante Cofense PhishMe™ que es una herramienta de capacitación en seguridad cibernética que produce simulaciones de phishing basadas en las últimas amenazas conocidas para eludir las puertas de enlace de correo electrónico seguras (SEG) ("Cofense", Cofense 2019, 2020b). Todos los participantes desconocían el propósito del estudio y no sabían que el correo electrónico era un	

	capturaba automáticamente mediante la herramienta de ciberseguridad Cofense PhishMe™. El comportamiento cibernético seguro se operacionalizó como una respuesta de "Reportar". Los participantes se consideraron que habían mostrado un comportamiento cibernético seguro si reenviaban el correo electrónico a la bandeja de entrada	correo electrónico de phishing simulado hasta que dieron una respuesta.	

41		dedicada de la institución financiera para correos electrónicos sospechosos de phishing. Una respuesta de "Reportar" era capturada por el equipo de seguridad de la institución financiera.

Tabla 7. Factor cognitivo: *Percepción.*

Autor	Tipo de muestra	Tamaño de la muestra	Media de edad	Medida de detección de amenazas informáticas	Experimento	Análisis estadísticos	Riesgo de sesgo	Análisis cualitativo
Albladi & Weir, (2020)	Desconocido	316	_____	Las escalas utilizadas para medir los hábitos de usuario en las redes sociales se han adoptado de (Fogel y Nehmad 2009).	El experimento realizado en esta investigación consistió en presentar a los participantes seis imágenes de publicaciones de Facebook. Estas publicaciones se clasificaron en escenarios de alto riesgo y escenarios de bajo riesgo. Los escenarios de alto riesgo incluyeron phishing, clickjacking con un archivo ejecutable, programa maligno y estafa de phishing, que se encuentran entre los ataques cibernéticos más destacados en las redes sociales. Se pidió a los	algoritmo PLS para proporcionar estimaciones estándar del modelo, como el coeficiente de ruta, el coeficiente de determinación (valores R2), el tamaño del efecto y estadísticas de colinealidad. Se utilizó un enfoque de bootstrap para probar la significancia	Riesgo bajo	No tiene influencia directa en la vulnerabilidad, pero el presente estudio encontró riesgo percibido al aumentar significativamente el nivel de competencia de las personas para hacer frente a los ataques de ingeniería social. Se ve influenciada por diversos factores, como la experiencia, la cultura, las afiliaciones políticas y otros constructos sociales.

				participantes que revisaran estas imágenes y juzgaran el nivel de riesgo asociado con cada publicación. El objetivo era medir la susceptibilidad de los participantes a los ataques de ingeniería social. El experimento tuvo como objetivo identificar los factores que influyen en el juicio de los usuarios sobre los ataques basados en ingeniería social y determinar los puntos más débiles en el comportamiento de detección de los usuarios.	de las relaciones en el modelo estructural. Finalmente, se utilizó un procedimiento de enmascaramiento para evaluar la relevancia predictiva (Q2) del modelo estructural. Además, se llevaron a cabo análisis de regresión, pruebas t y pruebas ANOVA para explorar la relación entre las características demográficas de los usuarios y su susceptibilidad a los ataques de ingeniería social.		
Autor	**Tipo de muestra**	**Tamaño de la muestra**	**Medi a de edad**	**Medida de detección de amenazas informáticas**	**Experimento**	**Análisis estadísticos**	**Riesgo de sesgo**	**Análisis cualitativo**

Brinton Anderson et al., (2016)	Desconocido	62	21.66 años	Un rastreador ocular que registraba las fijaciones a una velocidad de 60 Hz, capturando millones de registros de movimientos oculares de los participantes mientras veían las advertencias. El número de fijaciones se analizó utilizando el modelado de curvas de crecimiento latentes, una técnica estadística longitudinal utilizada para estimar las trayectorias de	Métodos de NeuroIS para observar directamente el cerebro y obtener información sobre fenómenos de sistemas de información que de otra manera no se podrían obtener. Además, se menciona que se utilizó el seguimient	Modelado de curvas de crecimiento latentes, una técnica estadística longitudinal utilizada para estimar las trayectorias de crecimiento a lo largo del tiempo. El análisis estima una intersección (intercept) y una pendiente (slope) para los valores observados a lo largo del tiempo. En el contexto del estudio, los valores observados se refieren al número de fijaciones en la advertencia y el texto en cada visualización sucesiva de una advertencia.	Poco claro	Se puede inducir la interferencia de tareas mediante la memorización de un código alfanumérico de siete dígitos y la respuesta a un mensaje de seguridad mientras se mantiene el código en la memoria

				crecimiento a lo largo del tiempo.	o ocular (eye tracking) para medir la habituación mientras los participantes veían las advertencias de seguridad en una configuración típica de computadora de escritorio			de trabajo.

Autor	**Tipo de muestra**	**Tamaño de la muestra**	**Media de edad**	**Medida de detección de amenazas informáticas**	**Experimento**	**Análisis estadísticos**	**Riesgo de sesgo**	**Análisis cualitativo**

Vishwanath et al., (2018)	Probabilístico	125 y 200	_____	En la mayoría de los elementos, los sujetos indicaron su acuerdo utilizando una escala de respuesta que variaba de 1 (totalmente en desacuerdo) a 5 (totalmente de acuerdo).	Experimento 1: El correo electrónico con un hipervínculo fue enviado a los sujetos. Al hacer clic en el hipervínculo, los sujetos eran redirigidos a una encuesta web. Los sujetos se consideraban "pescados" si hacían clic en el hipervínculo. El ataque fue implementado utilizando software de marketing por correo	El modelo SCAM se probó utilizando un análisis de trayectoria en AMOS. Para cada modelo, se estimó la bondad de ajuste utilizando una combinación de cuatro índices de ajuste: χ2, chi-cuadrado relativo (χ2/df; Bentler, 1990; Bentler & Bonett, 1980), índice de ajuste comparativo (CFI), índice de bondad de ajuste (GFI) y error cuadrático medio de aproximación	Poco claro	Las creencias del riesgo cibernético, hace que las personas no se dan cuenta de las señales que podrían haber llevado a sospecha y revelar el engaño. Esto da como resultado que los individuos actúen automáticam ente.

	electrónico que, junto con la encuesta web, permitió al equipo de investigación rastrear a las personas que abrieron el correo electrónico y/o hicieron clic en el enlace de la encuesta. Una semana después de la implementación del ataque inicial, se envió un recordatorio por correo electrónico a todos los sujetos que

	aún no habían abierto sus correos electrónicos. Una semana después, se envió un correo electrónico a los estudiantes que aún no habían respondido a los dos intentos de phishing, solicitando su participación en una encuesta web. En esta encuesta, se les preguntó a los sujetos si recordaban

	haber visto un correo electrónico de phishing; luego se les presentaron algunos ejemplares, uno de los cuales incluía el correo electrónico de phishing que se les envió, y se les pidió que identificaran el correo electrónico de phishing que recibieron. Solo los sujetos que recordaron haber visto un correo

	electrónico de phishing y lo identificaron correctamente se mantuvieron en el estudio. Experimento 2: Todos los sujetos en el ataque de archivo adjunto recibieron un correo electrónico con un archivo Adobe PDF adjunto. Este formato de documento se utilizó porque es comúnmente utilizado en correos	

	electrónicos, así como por los phishers. Los sujetos se consideraban "pescados" si abrían el archivo adjunto. Al igual que con el ataque de enlace, los sujetos fueron rastreados utilizando software de marketing por correo electrónico, y aquellos que aún no habían respondido una semana después del ataque inicial recibieron

		otro recordatorio. Los sujetos que no respondieron después de los dos intentos de phishing fueron contactados por el equipo de investigación y, después de verificar la recepción del correo electrónico de phishing, se les solicitó que completaran la encuesta web de seguimiento.

Autor	Tipo de muestra	Tamaño de la muestra	Media de edad	Medida de detección de amenazas informáticas	Experimento	Análisis estadísticos	Riesgo de sesgo	Análisis cualitativo
Canfield et al., (2016)	Probabilístico	62	32 años	Preguntas para cada correo electrónico: (a) "¿Es este un correo electrónico de phishing?" (sí/no; detección), (b) "¿Qué harías si recibieras este correo electrónico?" (con opciones de múltiple elección de Sheng et al., 2010; comportamiento), (c) "¿Cuán seguro te sientes con tu respuesta?" (50%–100%; confianza), y (d) "Si este fuera un correo electrónico de phishing y cayeras en él, ¿qué tan malas serían las consecuencias?" (1 = nada	Siguiendo el diseño basado en escenarios los participantes revisaron los correos electrónicos de una persona ficticia. Para reducir la carga del participante y el estudio costos, los correos electrónicos de phishing aparecen en una base alta (50 %), en relación con entornos del mundo real (<1 %). Asignamos aleatoriamente a los	modelado de curvas de crecimiento latentes, una técnica estadística longitudinal utilizada para estimar las trayectorias de	Poco claro	La mayoría de los participantes trataron las falsas alarmas como más costos que las fallas, lo que favorece la confianza en su capacidad y percepción de consecuencias. La confianza estuvo fuertemente

		mal, 5 = muy mal; consecuencias percibidas)	participantes a las condiciones. creado cruzando tres variables de tarea: (a) tarea orden (Experimento 1 únicamente), (b) tipo de tarea (Experimento 2 únicamente) y (c) notificación de tasa base. (Experimento 1 únicamente), (b) tipo de tarea (Experimento 2 únicamente) y (c) notificación de tasa base. Los participantes recibieron información sobre phishing y luego evaluó 40 correos electrónicos. El información fue la tira cómica PhishGuru de Kumaraguru et al.	crecimien to a lo largo del tiempo. El análisis estima una intersecci ón (intercept) y una pendiente (slope) para los valores observad os a lo largo del tiempo. En el contexto del estudio, los valores observad	relacionada con la tarea de detección.

		(2010). Señaló que los atacantes puede falsificar remitentes y advirtió: "No confíes en los enlaces en un correo electrónico." Para la tarea de evaluación de correo electrónico, los participantes examinaron 19 correos electrónicos legítimos, 19 correos electrónicos de phishing y dos controles de atención correos electrónicos Para cada correo electrónico, los participantes realizaron las tareas de detección y comportamiento, luego evaluadas su confianza en sus juicios y las consecuencias	os se refieren al número de fijaciones en la advertencia y el texto en cada visualización sucesiva de una advertencia.

						percibidas si el correo electrónico era phishing. El orden de los correos electrónicos fue aleatorio para cada participante. El orden de detección y las tareas de comportamiento se aleatorizaron entre los participantes.		
Autor	**Tipo de muestra**	**Tamaño de la muestra**	**Media de edad**	**Medida de detección de amenazas informáticas**	**Experimento**	**Análisis estadísticos**	**Riesgo de sesgo**	**Análisis cualitativo**
Nicholson et al., (2017)	Probabilística	281	33.6 años	Tarea: se clasificó cada correo electrónico como genuino o phishing. Esta fue una decisión binaria, pero también se registró el tiempo que se tomó para tomar la decisión (en segundos) en cada	Experimento en línea a través de Amazon Mechanical Turk, donde se pidió a los participantes que vieran 18 correos electrónicos (6 de phishing y 12 reales) y decidieran si cada correo electrónico	Estadística descriptiva y pruebas t independientes	Riesgo bajo	El nudge de saliencia del remitente, presentado solo y en combinación con un nudge de saliencia del receptor, mejoró la detección de correos electrónicos de phishing en comparación con la condición de control. En otras palabras, el simple acto de resaltar campos que ya están presentes en un correo electrónico, como el nombre del remitente, la

			correo electrónico, comenzando cuando se cargó la página y concluyendo cuando se presionó el botón de radio para la decisión. Finalmente, se les pidió a los participantes que calificaran cuán seguros se sentían con su propia clasificación del correo electrónico como genuino o phishing, utilizando un menú desplegable con opciones que iban desde 0% hasta 100% de confianza en incrementos del 10%.	representaba un mensaje legítimo o un mensaje de phishing. Los correos electrónicos fueron diseñados por los investigadores, pero se basaron en mensajes reales recibidos en los últimos 3 meses.			dirección de correo electrónico y la hora de envío, fue un medio efectivo para mejorar la seguridad del usuario

Autor	**Tipo de muestra**	**Tamaño de la muestra**	**Media de edad**	**Medida de detección de amenazas informáticas**	**Experimento**	**Análisis estadísticos**	**Riesgo de sesgo**	**Análisis cualitativo**

Yerdon et al., (2022)	Probabilístico	105		dos simulaciones para probar la eficacia de la detección de amenazas internas activadas por la IA utilizando el seguimiento ocular.	Este experimento utilizó un diseño mixto de 2 × 2 con el rol del participante (control y TI) como la variable dentro de sujetos y la simulación (financiera y de espionaje) como la variable independiente entre sujetos. Para la manipulación del rol del participante, una tarea secundaria dentro de la simulación se enmarcó durante el entrenamiento como legítima (control) o ilícita (TI). La asignación de roles fue equilibrada en ambas simulaciones.	ANOVAs de modelo mixto	Poco claro	Las métricas de seguimiento ocular pueden ser útiles para detectar comportamientos de amenaza interna en entornos simulados

Autor	**Tipo de muestra**	**Tamaño de la muestra**	**Media de edad**	**Medida de detección de amenazas informáticas**	**Experimento**	**Análisis estadísticos**	**Riesgo de sesgo**	**Análisis cualitativo**

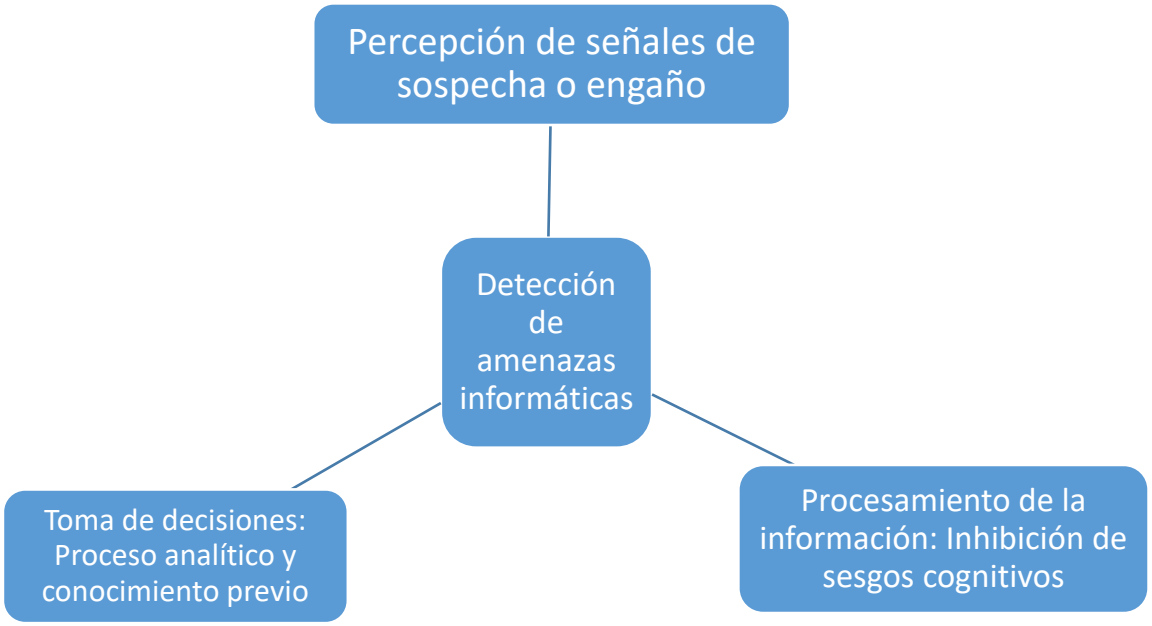
Wang et al., (2012)	Desconocido	321	Encuesta en línea que presentó a los participantes una imagen del correo electrónico de phishing original. La imagen del correo electrónico de phishing real presentada a los sujetos sirvió como estímulo para su juicio.	El experimento realizado en el estudio involucró el uso de un correo electrónico real de spear phishing como estímulo para recopilar datos de una muestra de su población objetivo con una encuesta. El ataque de phishing se dirigió a usuarios de correo electrónico en una gran universidad en el noreste de los EE. UU. para obtener identificaciones de cuentas y contraseñas. El experimento realizado en el estudio involucró el uso de un correo electrónico real de spear phishing como estímulo para recopilar datos de una muestra de su población objetivo con una encuesta. El ataque	Modelo estructural: cargas factoriales	Bajo riesgo	La atención a los desencadenantes viscerales es modelado como un formativo de segundo orden con un constructo latente con dos de primer orden y constructos reflexivos de la siguiente manera: “Atención al título y “Atención a la urgencia” son de primer orden que se modelan con la atención al phishing e indicadores de engaño que son constructos latentes de segundo orden, la combinación de ambos dan lugar a los constructos reflexivos “atención al error gramatical” y Atención a la dirección del remitente

		de phishing se dirigió a usuarios de correo electrónico en una gran universidad en el noreste de los EE. UU. para obtener identificaciones de cuentas y contraseñas.	

Fuente: Elaboración propia.

Figura 2. Modelo cognitivo para detección de amenazas

Las evidencias encontradas en la revisión sistemática nos permiten integrar tres factores cognitivos toma de decisiones, percepción y procesamiento de la información.



5. Discusión y Conclusiones

Los artículos seleccionados tienen un diseño experimental y una asignación probabilística en sus muestras, pero la población de la mayoría de los estudios es adultos jóvenes, lo que hace que las conclusiones no se puedan generalizar a todo el ciclo evolutivo de adultez.

En los estudios sobre toma de decisiones se describe entorno a la decisión de confianza que realiza el usuario: la confianza en los sistemas de detección, cuando la acumulación de evidencias, es tardía puede aumentar la tolerancia y disminuir la capacidad de detectar el engaño, por lo tanto confiará más, la información reconocida como el titulo y el encabezado puede hacer que no se detecte la información nueva, las creencias de riesgo tienen un rol importante en la identificación de señales que llevan a la sospecha y que revela el engaño, por otro lado el procesamiento cognitivo profundo hace que la información presentada se evalúe de manera más detallada, frente a esto la discusión se centra en si los estilos de procesamiento inconscientes o automáticos que se pueden ver influenciados por los estímulos priming son el problema en la detección de amenazas informáticas, pero la

evidencia apunta a que el objetivo no es pasar al estilo analítico sino buscar estrategias que puedan inhibir el uso de heurísticas.

En la función de percepción se puede evidenciar que las investigaciones se centran en las características del estímulo como un primer aspecto a tomarse en cuenta, es el nivel de elaboración que tiene un mensaje de correo electrónico en el caso de phishing, esto es procesado en la atención desde los constructos de primer orden como el título y encabezado, los de segundo o latentes como las señales de sospecha, estos interactúan entre sí y dan lugar a los constructos reflexivos como errores gramaticales y dirección del remitente, además las interferencias durante la tarea de detección pueden influir en el desempeño de la memoria de trabajo, pero el proceso de percepción, no solo se relaciona con los estímulos, sino también con la información interna de la mente del usuario y ahí la cultura y política pueden influir en las creencias de riegos cibernético, así como el riesgo percibido y gravedad de amenaza, que juega un rol importante en el nivel de competencia para la detección.

En el aprendizaje la evidencia fue menor y se destaca el rol del refuerzo en la dinámica del atacante y del defensor, la estrategia que cada uno utiliza influye en la respuesta del otro y la habituación y advertencias polimorfas en el tiempo de fijación.

La pregunta de investigación planteada fue como los factores cognitivos influyen en el proceso de detección de amenazas informáticas, en la revisión sistemática podemos ver evidencias, que la detección de amenazas informáticas, es un proceso complejo en el que participan factores cognitivos de primer orden como la percepción, factores de tercer orden como las funciones ejecutivas, en el que la forma de procesar la información (sistemática o heurística) dependen de factores individuales y los estímulos.

5.1. Limitaciones

La revisión sistemática realizada la experticia de la autora puede limitar la aplicación de la rigurosidad que la metodología PRISMA propone y probablemente se pueden haber quedado por fuera mucha evidencia empírica de los factores cognitivos sobre el proceso de detección de amenazas informáticas. Uno de los aspectos que genero dificultades y la heterogeneidad de resultados, lo que se buscó solucionar mediante búsqueda de elementos o características que permitan su agrupación.

5.2. Prospectiva

En la revisión sistemática de literatura se puede evidenciar evidencias sobre personalidad y aspectos emocionales que influyen en el proceso de detección, que este trabajo no fueron considerados ya que la pregunta de investigación estaba delimitada a factores cognitivos, pero poder ser una línea futura de investigación que puede completar el trabajo de e comprensión sobre los factores cognitivos que hemos realizado., con la evidencia encontrada se puede realizar intervenciones para aumentar la habilidad de detección del engaño que ahora en el ciberespacio es fundamental, así como un fortalecimiento de los modelos teóricos que se usan en el campo de ciberseguridad.

Ampliar investigaciones que incluyan todos los rangos de edad de la adultez para conocer si hay diferencias en la detección de amenazas informáticas entre adultez media, tardía y juventud.

6. REFERENCIAS BIBLIOGRÁFICAS

*Aggarwal, P., Thakoor, O., Jabbari, S., Cranford, E. A., Lebiere, C., Tambe, M., & Gonzalez, C. (2022). Designing effective masking strategies for cyberdefense through human experimentation and cognitive models. Computers & Security, 117, 102671. https://doi.org/https://doi.org/10.1016/j.cose.2022.102671

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

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

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

Brown, S. D. and Reavey, P. (2017) 'False memories and real epistemic problems', Culture & Psychology, 23(2), pp. 171–185. doi: 10.1177/1354067X17695764.

*Buckley, J., Lottridge, D., Murphy, J. G., & Corballis, P. M. (2023). Indicators of employee phishing email behaviours: Intuition, elaboration, attention, and email typology. International Journal of Human Computer Studies, 172, 102996. https://doi.org/10.1016/j.ijhcs.2023.102996

Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails.

*Butavicius, M., Taib, R., & Han, S. J. (2022). Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security*, *123*, 102937. https://doi.org/https://doi.org/10.1016/j.cose.2022.102937*Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying Phishing Susceptibility for Detection and Behavior Decisions. Human Factors, 58(8), 1158–1172. https://doi.org/10.1177/0018720816665025

Cole, S. and Kvavilashvili, L. (2019). Spontaneous and deliberate future thinking: a dual process account. Psychological Research https://doi.org/10.1007/s00426-019-01262-7

Chai, S. (2020) Does Cultural Difference Matter on Social Media? An Examination of the Ethical Culture and Information Privacy Concerns. Sustainability, 12, 8286. https://doi.org/10.3390/su12198286

Chang, J. and Chong, M. (2010). Psychological influences in e-mail fraud. Journal of Financial Crime. 17. 337-350. 10.1108/13590791011056309.

* Dutt, V., Ahn, Y.-S., & Gonzalez, C. (2012). Cyber Situation Awareness: Modeling Detection of Cyber Attacks With Instance-Based Learning Theory. *Human Factors*, *55*(3), 605–618. https://doi.org/10.1177/0018720812464045

*Fischer, P., Lea, S. E. G., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal*

*Ge, Y., Lu, L., Cui, X., Chen, Z., & Qu, W. (2021). How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Applied Ergonomics*, *97*, 103526. https://doi.org/https://doi.org/10.1016/j.apergo.2021.103526

Gómez, M. (2020), Bias and Misperception in Cyberspace at: https://isnblog.ethz.ch/cyber/bias-and-misperception-in-cyberspace, [Accessed 9 April 2023].

*Guedes, I., Martins, M., & Cardoso, C. S. (2022). Exploring the determinants of victimization and fear of online identity theft: an empirical study. Security Journal. https://doi.org/10.1057/s41284-022-00350-5

*Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*, *40*(2), 265–281. https://doi.org/10.1108/OIR-04-2015-0106

Jones HS, Towse JN & Race N. (2015) Susceptibility to email fraud: A review of psychological perspective, data-collection methods, and ethical considerations. International Journal of Cyber Behavior, Psychology, and Learning. 5(3): 13–29.

* Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. Computers & Security, 125, 103049. https://doi.org/https://doi.org/10.1016/j.cose.2022.103049

*Luo, X. (Robert), Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. Computers & Security, 38, 28–38. https://doi.org/https://doi.org/10.1016/j.cose.2012.12.003

MITRE. Leveraging Behavioral Science to Mitigate Cyber Security Risk Available at: https://www.mitre.org/sites/default/files/pdf/12_0499.pdf, [Accessed 9 April 2023].

*Neupane, A., Saxena, N., Maximo, J. O., & Kana, R. (2016). Neural Markers of Cybersecurity: An fMRI Study of Phishing and Malware Warnings. *IEEE Transactions on Information Forensics and Security*, *11*(9), 1970–1983. https://doi.org/10.1109/TIFS.2016.2566265

*Nicholson, J., Coventry, L., & Briggs, P. (2017). Can We Fight Social Engineering Attacks by Social Means? Assessing Social Salience as a Means to Improve Phish Detection. Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security, 285–298.

Pedersen, T., Johansen, C. & Jøsang, A. Behavioural Computer Science: an-agenda for combining modelling of human and system behaviours. Hum. Cent. Comput. Inf. Sci. 8, 7 (2018). https://doi.org/10.1186/s13673-018-0130-0

Valaskivi, K. (2018) Beyond Fake News: Content confusion and understanding the dynamics

of the contemporary media environment, HybridCOE Strategic Analysis.

*Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. Communication Research, 45(8), 1146–1166. https://doi.org/10.1177/0093650215627483

*Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, *55*(4), 345–362. https://doi.org/10.1109/TPC.2012.2208392

* Woods, D., Abdallah, M., Bagchi, S., Sundaram, S., & Cason, T. (2022). Network defense and behavioral biases: an experimental study. Experimental Economics, 25(1), 254–286. https://doi.org/10.1007/s10683-021-09714-x

*Yerdon, V. A., Lin, J., Wohleber, R. W., Matthews, G., Reinerman-Jones, L., & Hancock, P. A. (2022). Eye-Tracking Active Indicators of Insider Threats: Detecting Illicit Activity During Normal Workflow. *IEEE Transactions on Engineering Management*, *69*(6), 3838–3847.

https://doi.org/10.1109/TEM.2021.3059240