Recibido 05 Jun 2026 *ReCIBE, Año 15 No. 3, Sep 2026*

Aceptado 28 Ago 2026

Comportamientos humanos de riesgo en la ciberseguridad: Un análisis de contraseñas débiles, falta de actualización y clics en enlaces no verificados.

Risky Human Behaviors in Cybersecurity: An Analysis of Weak Passwords, Failure to Update, and Clicking on Unverified Links.

Alberto Jair Cruz Landa [1]
albecruz@uv.mx
Juan Manuel Gutiérrez Méndez[1]
juangutierrez02@uv.mx
Juan Carlos Jiménez Márquez [1]
jjimenez@uv.mx
Martha Elizabet Domínguez Bárcenas[1]
eldominguez@uv.mx
Alicia Yazmín Rojas Luna[1]
alirojas@uv.mx

1 Universidad Veracruzana, México

Resumen: Los comportamientos humanos relacionados con el uso de contraseñas débiles, la falta de actualizaciones de software y la interacción con hipervínculos no verificados, conllevan riesgos en el ámbito de la ciberseguridad. Cabe destacar que independientemente de los avances en el ámbito tecnológico el factor humano es responsable en un alto número de incidencias de seguridad, debido a errores, omisiones o decisiones humanas. La literatura en ciberseguridad aún presenta una desconexión entre la identificación de los comportamientos humanos de riesgo, las consecuencias que estos generan y los factores que los originan. Esta falta de articulación limita la comprensión integral del problema y provoca que muchas soluciones propuestas resulten excesivamente técnicas o poco accesibles para el usuario final, dificultando la mitigación efectiva de estas conductas dentro de los sistemas de información. El presente estudio tiene como objetivo analizar las consecuencias asociadas y factores que influyen en los comportamientos humanos de riesgo en ciberseguridad, a través de una revisión sistemática de literatura, con el fin de recuperar estrategias de prevención.
Palabras clave: Ciberseguridad, comportamiento humano, contraseñas débiles, actualización de software, enlaces no verificados, vulnerabilidad.

Abstract: Human behaviors related to the use of weak passwords, the lack of software updates, and interaction with unverified hyperlinks pose significant risks in the field of cybersecurity. Despite technological advances, the human factor remains responsible for a high number of security incidents due to human errors, omissions, or decisions. Cybersecurity literature still shows a lack of connection between the identification of risky human behaviors, the consequences they generate, and the factors that cause them. This lack of articulation limits a comprehensive understanding of the problem and leads many proposed solutions to be technical or less accessible to end users, making it difficult to effectively mitigate these behaviors within information systems. This study aims to analyze the associated consequences and factors of risky human behaviors in cybersecurity through a systematic literature review, in order to identify prevention strategies.
Keywords: Cybersecurity, human behavior, weak passwords, software updates, unverified links, vulnerability

1.- Introducción

En la era digital actual, la ciberseguridad ha alcanzado una importancia crítica debido a la creciente dependencia de la tecnología y la expansión de las redes digitales. Sin embargo, más allá de las soluciones técnicas, el factor humano, entendido como el conjunto de decisiones, acciones y errores cometidos por los usuarios al interactuar con sistemas digitales, sigue siendo considerado el eslabón más débil de la cadena de defensa (Triplett, 2022). En este sentido, se estima que el 95% de los incidentes de ciberseguridad se deben a errores humanos, con proyecciones que sitúan las pérdidas por cibercrimen global en 10.5 billones de dólares anuales para 2025 (Desolda et al., 2021).

En este contexto, el comportamiento humano de riesgo puede comprenderse como una manifestación específica del factor humano, ya que se refiere a aquellas decisiones y acciones que incrementan la probabilidad de comprometer la seguridad de la información. Estas conductas incluyen, por ejemplo, el uso de contraseñas poco robustas, el acceso a enlaces no verificados o el descuido en la actualización de software, prácticas que pueden afectar la confidencialidad, integridad y disponibilidad de la información (Yeo et al., 2022).

Uno de los comportamientos de mayor riesgo identificados en los sistemas de información es el uso de contraseñas débiles o reutilizadas. Como evidencia de ello, se encontró que el 62.2% del personal evaluado empleaba contraseñas débiles en un entorno hospitalario (Ali et al., 2022). Esta situación se ve agravada por factores de usabilidad y conveniencia, ya que los usuarios suelen priorizar la facilidad de uso frente a la seguridad, lo que influye directamente en la calidad de las

contraseñas creadas (Wash et al., 2021). Dicho comportamiento facilita el robo de credenciales y la explotación de vulnerabilidades a gran escala (Kumar, 2023).

Otro comportamiento relevante es la falta de aplicación oportuna de actualizaciones de software y sistemas. La postergación o el ignorar los parches de seguridad refleja la influencia de variables como la percepción de riesgo, la carga de trabajo o la ausencia de protocolos claros (Yeo et al., 2022). Esta conducta deja los sistemas vulnerables ante amenazas ya conocidas, incrementando significativamente el riesgo operativo (Ali et al., 2022), dado que existe la explotación de estas vulnerabilidades casi de manera inmediata (Iannone et al., 2024).

Estos comportamientos de riesgo no solo generan consecuencias como la pérdida de información, el robo de identidad o daños económicos, sino que también reflejan factores subyacentes que los originan, tales como la falta de formación en ciberseguridad, una cultura organizacional débil en materia de protección digital o la percepción errónea de que la seguridad es responsabilidad exclusiva del área técnica (Triplett, 2022).

Finalmente, estas debilidades humanas son aprovechadas mediante mecanismos de explotación como la ingeniería social, una técnica de ataque altamente eficaz que explota aspectos como la confianza, la urgencia emocional o la falta de conciencia sobre amenazas. Se ha reportado que la mayoría de los incidentes de seguridad implican errores humanos vinculados al hacer clic en enlaces maliciosos o al manejo inadecuado de credenciales (French, 2025). Asimismo, diversos estudios han demostrado que los usuarios presentan serias dificultades para identificar ataques de suplantación de identidad, lo que evidencia una vulnerabilidad significativa en los esquemas tradicionales de capacitación (Baki et al., 2017).

A pesar de los avances tecnológicos en mecanismos de defensa, la seguridad de la información continua viéndose comprometida por la persistencia de comportamientos humanos de riesgo que los usuarios mantienen al interactuar con sistemas digitales. La literatura académica y los reportes de la industria coinciden en que una proporción significativa de los incidentes de seguridad tiene su origen en este tipo de conductas. De acuerdo con estudios recientes, el 95 % de los incidentes de ciberseguridad están asociados a comportamientos humanos como errores, phishing, contraseñas débiles o malas prácticas (Jones, 2024; Coker, 2025).

Si bien estos comportamientos han sido ampliamente documentados, gran parte de la discusión se limita a su identificación, sin profundizar de manera sistemática en las consecuencias concretas que generan en la seguridad de la información. Entre dichas consecuencias se encuentran las brechas de datos, las pérdidas financieras, las interrupciones en los servicios y los daños a la reputación organizacional, evidenciando que el problema trasciende el ámbito técnico y afecta dimensiones operativas, económicas y sociales (Juma'h y Alnsour, 2020; Moustafa et al., 2021).

Asimismo, estos comportamientos de riesgo son activamente explotados por los atacantes, quienes emplean estrategias diseñadas para aprovechar errores recurrentes de los usuarios y evadir las defensas tradicionales. La ingeniería social, en particular, se ha consolidado como un mecanismo eficaz al capitalizar la confianza, la urgencia y la falta de verificación por parte de los usuarios (Montañez et al., 2020; Khadka et al., 2024; Sathe et al., 2025).

2.- Método de investigación

Para realizar este estudio, se tomó como base la metodología de Revisión Sistemática de Literatura (RSL), ya que es un método riguroso para analizar la literatura de investigación científica. Su objetivo principal no es solo integrar la evidencia existente sobre una pregunta de investigación, sino que también busca apoyar el desarrollo de pautas basadas en evidencia para los profesionales (Kitchenham et al., 2015).

En el esquema gráfico de la Ilustración 1 se representa claramente el método de trabajo, de forma secuencial en cada una de las fases y actividades que conformaron la Revisión Sistemática de Literatura.

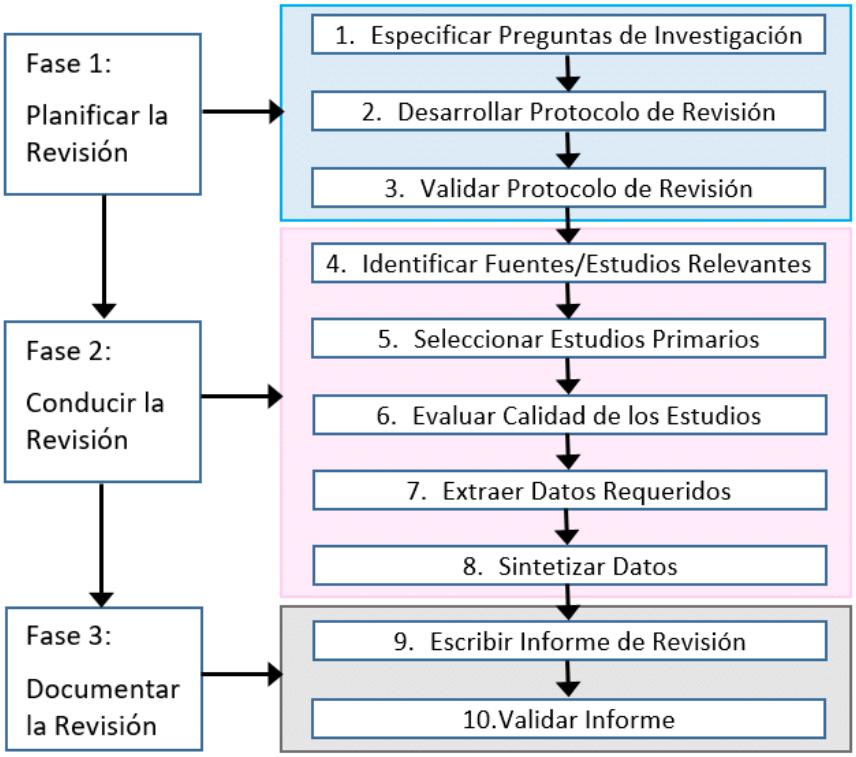

Ilustración 1 - Proceso de la estrategia de búsqueda (Kitchenham et al., 2015).

2.1.- Preguntas de investigación

Las preguntas son una herramienta clave para guiar la investigación, pero hay que respaldarlas mediante un contexto que explique su relevancia. En otras palabras, es importante justificar porque esas preguntas son significativas y como aportan en el desarrollo de la investigación, en la Tabla 1 se detallan cada una de las mismas.

Pregunta de investigación	Motivación
1.- ¿Cuáles son las consecuencias de los comportamientos humanos de riesgo, específicamente el uso de contraseñas débiles, la falta de actualización de software y la interacción con hipervínculos no verificados?	Esta pregunta resulta pertinente porque permite identificar las consecuencias que generan comportamientos humanos de riesgo ampliamente documentados en la literatura de ciberseguridad, como el uso de contraseñas débiles, la falta de actualización de software y la interacción con hipervínculos no verificados. Analizar dichas consecuencias facilita dimensionar su impacto en la seguridad de la información y refuerza la importancia de la prevención desde el usuario final.
2.- ¿Cuáles son los factores que influyen en los comportamientos humanos en entornos digitales, específicamente en el uso de contraseñas débiles, la falta de actualización de software y la interacción con hipervínculos no verificados?	La formulación de esta pregunta permite explorar las causas subyacentes que motivan los comportamientos de riesgo en los usuarios. Identificar estos factores es esencial para explicar por qué persisten dichos comportamientos.
3.- ¿Cuáles son las formas de prevención, más allá de las soluciones tecnológicas, para abordar y mitigar comportamientos humanos de riesgo, específicamente el uso de contraseñas débiles, la falta de actualización de software y la interacción con hipervínculos no verificados en ciberseguridad?	La pertinencia de esta pregunta radica en buscar alternativas centradas en el factor humano, a diferencia de las medidas puramente técnicas, estas estrategias pueden generar un cambio sostenible en la conducta de los usuarios, reduciendo los riesgos derivados de comportamientos inseguros.

Tabla 1. Preguntas de investigación

2.2 Selección de fuentes

Las bases de datos seleccionadas por su relevancia en el ámbito de la informática y la ciberseguridad fueron; ACM Digital Library, IEEE Xplore y SpringerLink y fueron consultadas por última vez el 01 de diciembre del 2025.

2.3.- Términos de búsqueda

En la Tabla 2, Se presentan los principales conceptos identificados que sirvieron como base para la construcción de la cadena de búsqueda utilizadas en las bases de datos seleccionadas.

Términos	Conceptos relacionados	Términos en inglés
Contraseñas débiles	Contraseñas Autenticación Vulnerabilidades Ataques por fuerza bruta	Weak passwords Password strength Password vulnerabilities Password reuse Brute forcé attacks
Actualización de software	Parches de seguridad Exploits Vulnerabilidades Gestión de actualizaciones Amenazas cibernéticas	Software updates Security patches Unpatched software Vulnerable software Software vulnerabilities Exploit prevention
Clic en enlaces no verificados	Ingeniería social, phishing Enlaces maliciosos Ataques de phishing Correo electrónico no deseado Amenazas cibernéticas	Phishing attacks Clicking malicious links Unverified links Social engineering Email scams Phishing vulnerability
Comportamiento humano	Conducta del usuario Concienciación Factores humanos	Human behavior User behavior Awareness Human factors

Tabla 2. Conceptos relacionados

2.4.- Criterios de selección

Se propusieron cinco criterios de inclusión (CI) y tres criterios de exlusión CE, para seleccionar los estudios primarios de los estudios recuperados de las fuentes seleccionadas, ver tabla 3 y tabla 4.

Clave	Descripción
CI-1	Se incluyeron solo artículos publicados en inglés
CI-2	Se considero únicamente artículos con fecha de publicación a partir de 2015 hasta el 2025. Esto para tomar información actualizada y relevante, dada la rápida evolución del panorama tecnológico y las amenazas cibernéticas en los últimos años.
CI-3	El título debía dar indicio a responder al menos una pregunta de investigación.
CI-4	Durante la lectura del resumen o abstract debía dar indicio a que responderá al menos una pregunta de investigación
CI-5	En la lectura completa del estudio se encuentra respuesta a al menos una pregunta de investigación

Tabla 3. Criterios de inclusión

Clave	Descripción
CE-1	Se descartaron documentos que sean duplicados para garantizar la inclusión de información única y evitar redundancias en la revisión
CE-2	Se excluyeron aquellos estudios cuyo texto completo no esté disponible para su consulta.
CE-3	Se excluyeron estudios que no aborden directamente alguno de los tres comportamientos humanos: uso de contraseñas débiles, falta de actualización de software o interacción con hipervínculos no verificados.

Tabla 4. Criterios de exclusión

2.5. Construcción de la cadena de búsqueda

Para la construcción de la cadena de búsqueda se aplicó el enfoque propuesto por Zhang et al. (2011), conocido como Quasi-Gold Standard (QGS). Este método tiene como propósito evaluar y optimizar la efectividad de las cadenas de búsqueda utilizadas en revisiones sistemáticas de literatura (RSL).

El proceso inició con la selección manual de un grupo de estudios clave sobre el tema de investigación (estudios relevantes). A partir de estos, se extrajeron los términos más frecuentes y significativos para construir combinaciones de búsqueda mediante operadores booleanos (AND,

OR, NOT). Posteriormente, la cadena generada se validó utilizando las métricas de desempeño propuestas por Zhang et al. (2011):

La métrica de "precisión" indica la proporción de documentos recuperados que son relevantes para la consulta, véase la ecuación (1); mientras que la métrica de "recuperación" (recalles) se refiere a la proporción de documentos relevantes que se recuperan con éxito, véase la ecuación (2).

$$Precisión = \frac{(Documentos\ Relevantes\ recuperados)}{(Total\ de\ documentos\ recuperados)} \quad (1)$$

$$retornos = \frac{(Documentos\ relevante\ recuperados)}{(Total\ de\ documentos\ relevantes)} \quad (2)$$

La selección inicial del QGS se realizó mediante una búsqueda manual, considerando como criterios preliminares la relevancia temática, la alineación con los comportamientos humanos de riesgo definidos en el estudio (uso de contraseñas débiles, falta de actualización de software e interacción con hipervínculos no verificados) y el cumplimiento de los criterios de inclusión y exclusión establecidos anteriormente.

Como resultado de este proceso, se seleccionaron diez estudios, los cuales fueron considerados suficientes para representar el núcleo temático del estudio y servir como referencia para la validación de la cadena de búsqueda.

2.6 Evaluación de la cadena

Durante el proceso de validación se diseñaron y evaluaron cinco cadenas de búsqueda, las cuales fueron analizadas de acuerdo con las métricas de retorno y precisión conforme al método de Zhang et al. (2011). El QGS se construyó utilizando exclusivamente el motor de búsqueda IEEE Xplore, por razones metodológicas, al concentrar una alta proporción de literatura revisada por pares en el ámbito de la informática y la ciberseguridad. En Tabla 5 se muestran los resultados.

#	Cadena	Estudios encontrados	Estudios relevantes	Retorno	Precisión
1	("password vulnerabilities" OR "password reuse" OR "weak passwords") AND ("software vulnerabilities" OR "unpatched software" OR "lack of updates") AND ("clicking unverified links" OR "phishing attacks" OR "malicious emails") AND ("human behavior" OR "user awareness" OR "human factors")	3,020	3	(3/10) * 100 = 30%	(3/3,020) * 100 = 0.1%
2	("weak passwords" OR "password vulnerabilities") AND ("software updates" OR "unpatched software") AND ("clicking unverified links" OR "phishing") AND "cybersecurity" AND	2,771	4	(4/10) * 100= 40%	(4/2,771) * 100 = 0.1%

	("human behavior" OR "user awareness" OR "human factors")				
3	("weak passwords" OR "password strength" OR "password vulnerabilities" OR "password reuse" OR "brute force attacks") AND ("software updates" OR "security patches" OR "unpatched software" OR "vulnerable software" OR "software vulnerabilities" OR "exploit prevention") AND ("phishing attacks" OR "clicking malicious links" OR "unverified links" OR "email scams" OR "social engineering" OR "phishing vulnerability") AND ("human behavior" OR "user behavior" OR "awareness" OR "human factors")	516	4	(4/10) * 100= 40%	(4/516) * 100 = 0.8%
4	("behavioral cybersecurity" OR "human factors in cybersecurity") AND ("weak passwords" OR "software updates" OR "unverified hyperlinks" OR "phishing" OR "social engineering")	3,369	6	(6/10) * 100= 60%	(6/3,369) * 100 = 0.2%
5	("password security" OR "password strength" OR "password reuse" OR "weak passwords" OR "password vulnerabilities") AND ("software security" OR "software updates" OR "security patches" OR "unpatched vulnerabilities" OR "outdated software") AND ("phishing" OR "social engineering" OR "clicking unverified links" OR "malicious emails" OR "email threats") AND ("cybersecurity" OR "information security" OR "cyber threats" OR "system vulnerabilities") AND ("human behavior in cybersecurity" OR "user awareness" OR "human factors in information security")	528	8	(8/10) * 100= 80%	(8/528) * 100= 1.5%

Tabla 5. Evaluación de precisión y retorno de artículos

Al analizar los resultados obtenidos en la tabla anterior, se observa que la quinta cadena de búsqueda presentó un mayor retorno de estudios (80%) en comparación con las demás. Aunque su precisión (1.5%) fue baja, este resultado es esperable dentro del enfoque metodológico de Zhang et al. (2011), el cual prioriza una estrategia de alta sensibilidad, es decir, maximizar el retorno de estudios relevantes sobre la precisión inicial. En este sentido, se decidió priorizar el retorno (80%), ya que esta estrategia permitió recuperar un conjunto más amplio de documentos potencialmente relevantes, incrementando así la cobertura del estudio.

Una vez aplicados los criterios de inclusión y exclusión, se identificaron 20 estudios primarios, los cuales permitieron dar respuesta a cada una de las preguntas de investigación planteadas. La Tabla 6 muestra el número de estudios primarios identificados en cada una de las fuentes, junto con la reducción progresiva obtenida tras aplicar los criterios de selección.

Fuente de información	Total de estudios encontrados	Fase 1: CI-1 y CI-2	Fase 2: CI-3, CE-1, CE-2	Fase 3: CE-3, CI-4	Fase 4: CI-5	Total de estudios seleccionados
IEEE Xplore	528	476	398	54	11	11
ACM Digital Library	642	583	472	38	6	6
Springer Link	720	654	519	41	3	3
Total general	1,890	1,713	1,389	133	20	20

Tabla 6. Aplicación de criterios de inclusión y exclusión

2.7 Snowballing

El snowballing es una técnica utilizada en revisiones sistemáticas de la literatura que consiste en identificar estudios relevantes a partir de las referencias bibliográficas de artículos previamente seleccionados (backward snowballing) y, de manera complementaria, mediante la identificación de trabajos que citan a dichos artículos (forward snowballing). Este enfoque permite ampliar y refinar el conjunto de estudios primarios, fortaleciendo la cobertura del proceso de búsqueda. La aplicación del snowballing resulta especialmente útil en áreas donde los términos de búsqueda pueden variar o no capturar la totalidad de la literatura pertinente (Wohlin, 2014).

Con el objetivo de ampliar el conjunto de estudios y garantizar una cobertura más completa de la literatura relevante, se aplicó la técnica de Snowballing, tanto hacia atrás como hacia adelante. Dando como resultado un total de 17 artículos recuperados medio de dicho proceso.

3.- Resultados

Para realizar el proceso de síntesis se optó por aplicar una síntesis narrativa, conforme a los lineamientos metodológicos propuestos por Popay et al. (2006), con el fin de integrar los resultados obtenidos de los estudios primarios seleccionados. Esta decisión metodológica se justifica porque los documentos analizados presentan diversidad en enfoques, métodos y unidades de análisis, por lo que no resulta adecuado el uso de técnicas cuantitativas o metaanálisis. A continuación, se presentan los resultados de la investigación.

3.1 P1 ¿Cuáles son las consecuencias de los comportamientos humanos de riesgo, específicamente el uso de contraseñas débiles, la falta de actualización de software y la interacción con hipervínculos no verificados?

Los estudios revisados sugieren un patrón consistente: las vulnerabilidades explotables no surgen únicamente de fallos técnicos, sino de la interacción reiterada entre los sistemas y prácticas humanas cotidianas. Bajo esta perspectiva, la evidencia analizada indica que la ciberseguridad puede entenderse como un fenómeno socio-técnico, donde el componente humano desempeña un papel determinante en la generación del riesgo.

Respecto al uso de contraseñas débiles o reutilizadas, los hallazgos sugieren que este comportamiento deriva directamente el debilitamiento de los mecanismos de autenticación,

facilitando ataques automatizados como la fuerza bruta o la reutilización de credenciales. Más allá de la fragilidad técnica de las contraseñas, los estudios revisados indican que estas prácticas están asociadas a percepciones distorsionadas del riesgo y a modelos mentales que subestiman las capacidades reales de los atacantes (Ur et al., 2016). Por lo tanto, la vulnerabilidad no se explica únicamente por la falta de conocimiento, sino por la normalización de hábitos inseguros que llevan al usuario a confiar en soluciones aparentemente suficientes, pero fácilmente explotables.

Asimismo, la evidencia sugiere que la debilidad de las contraseñas es resultado de presiones cognitivas y contextuales. La gestión simultánea de múltiples cuentas y la necesidad de facilitar el recuerdo conducen a la adopción de estrategias simplificadas, como la repetición de claves o la creación de patrones predecibles (Zimmermann et al., 2020). Desde esta perspectiva, la consecuencia principal no es solo la exposición de una cuenta individual, sino la ampliación del impacto potencial cuando dichas credenciales son reutilizadas en distintos servicios, lo que incrementa de manera significativa la superficie de ataque.

En relación con la falta de actualización del software, los hallazgos permiten interpretar este comportamiento como un factor que transforma vulnerabilidades conocidas en consecuencias reales de explotación. La literatura revisada sugiere que el retraso en la aplicación de parches genera una acumulación progresiva de riesgo, ya que los atacantes suelen desarrollar y emplear exploits en lapsos más cortos que los ciclos de actualización organizacionales (Bilge et al., 2017). En este contexto, la consecuencia principal no es la existencia de la vulnerabilidad en sí, sino la permanencia de esta en el tiempo, lo que incrementa la probabilidad de incidentes de seguridad.

Los estudios sugieren que la postergación de actualizaciones no suele originarse en la negligencia deliberada, sino en tensiones operativas y organizacionales, como el temor a afectar la estabilidad de los sistemas o interrumpir servicios críticos (Pashchenko et al., 2020). Esta dinámica tiene como consecuencia que los sistemas más críticos, y por tanto más valiosos, permanezcan expuestos durante periodos prolongados, lo que incrementa su atractivo para actores maliciosos y amplifica el impacto potencial de un ataque exitoso.

Por su parte, la interacción con hipervínculos no verificados aparece como uno de los comportamientos con consecuencias más inmediatas para la seguridad. Los estudios revisados sugieren que este comportamiento facilita el acceso inicial a los sistemas mediante técnicas de phishing, independientemente del nivel de conocimientos técnicos del usuario (Jampen et al., 2020). La consecuencia principal no radica únicamente en hacer clic en sí, sino en la explotación de factores psicológicos como la urgencia, la confianza o la familiaridad, que reducen la capacidad del usuario para evaluar el riesgo de manera crítica.

La evidencia también indica que incluso usuarios con formación previa pueden verse afectados por este tipo de ataques, lo que refuerza la idea de que el phishing no debe interpretarse como un fallo individual aislado, sino como un mecanismo diseñado para explotar sesgos humanos recurrentes (Ivanov et al., 2021). En consecuencia, la interacción con enlaces maliciosos no solo compromete credenciales o información sensible, sino que puede actuar como punto de entrada inicial para ataques más complejos.

En conjunto, los estudios revisados sugieren que las consecuencias de estos comportamientos humanos de riesgo no se manifiestan de forma aislada, sino que se refuerzan mutuamente. La combinación de contraseñas débiles, sistemas no actualizados y la interacción con hipervínculos no verificados configura escenarios de riesgo compuesto, donde una acción facilita o amplifica el impacto de las demás. Desde esta perspectiva, las vulnerabilidades explotables pueden interpretarse como el resultado de una cadena de decisiones humanas interconectadas, en la que el comportamiento del usuario se convierte en un punto crítico de convergencia para la autenticación, el acceso y la integridad de los sistemas de información.

3.2.- P2 ¿Cuáles son los factores que influyen en los comportamientos humanos en entornos digitales, específicamente en el uso de contraseñas débiles, la falta de actualización de software y la interacción con hipervínculos no verificados?

La evidencia sugiere que dichos comportamientos no pueden atribuirse a la ignorancia o a la falta de interés por la seguridad, sino a una interacción compleja entre factores cognitivos, emocionales, sociales, organizacionales y conductuales. Por lo tanto, las prácticas inseguras observadas deben entenderse como respuestas humanas recurrentes ante contextos de sobrecarga, presión situacional y limitaciones estructurales.

Desde la dimensión cognitiva, los estudios revisados indican que uno de los principales factores es la presencia de modelos mentales incorrectos sobre el funcionamiento real de las amenazas. La literatura sugiere que muchos usuarios sobreestiman la efectividad de cambios superficiales y subestiman las capacidades técnicas de los atacantes (Ur et al., 2016). Estas percepciones distorsionadas generan una brecha entre el conocimiento percibido y el conocimiento necesario para actuar de forma segura. Investigaciones posteriores muestran que este fenómeno no se limita a usuarios sin formación técnica, ya que incluso perfiles especializados priorizan riesgos percibidos como la posible interrupción de un sistema sobre riesgos objetivos previamente identificados (Pashchenko et al., 2020). Esto sugiere que el problema no radica en la ausencia de información, sino en cómo esta es interpretada y valorada durante la toma de decisiones.

Los factores emocionales emergen como un segundo eje explicativo clave. La evidencia analizada sugiere que emociones como la prisa, la frustración, el miedo o la curiosidad influyen directamente en la adopción de comportamientos humanos de riesgo, desplazando el razonamiento deliberado (Jayatilaka et al., 2021). Cuando las medidas de seguridad se perciben como obstáculos o castigos, los usuarios tienden a evitarlas, aun reconociendo su importancia (Von Preuschen et al., 2024). En este contexto, la emoción actúa como un catalizador de decisiones impulsivas, facilitando acciones automáticas que reducen la evaluación crítica del riesgo.

Desde una perspectiva social y cultural, los estudios sugieren que los comportamientos humanos de riesgo se ven moldeados por normas grupales y dinámicas de pertenencia. La literatura indica que las decisiones relacionadas con la seguridad rara vez se toman de forma aislada; por el contrario, los individuos tienden a imitar prácticas normalizadas dentro de su entorno laboral o social (Kovačević y Putnik, 2020). En organizaciones donde estas prácticas son toleradas o minimizadas, los comportamientos inseguros se reproducen y consolidan, incluso cuando existen políticas formales de seguridad. Esta presión social explica por qué las prácticas de riesgo pueden propagarse de manera sistemática dentro de equipos completos.

El entorno organizacional constituye otro factor determinante. Los estudios revisados muestran que, en muchos contextos, la seguridad compite directamente con prioridades operativas como la disponibilidad, la productividad o la estabilidad de los sistemas (Wang et al., 2017). Esta tensión genera escenarios donde las decisiones conservadoras, orientadas a evitar interrupciones inmediatas, favorecen la permanencia de riesgos a largo plazo (Mugarza et al., 2021). Además, políticas de seguridad mal diseñadas o excesivamente rígidas tienden a generar fatiga y resistencia, reduciendo su efectividad y fomentando comportamientos de evasión (Petelka et al., 2019).

Finalmente, los factores conductuales y psicológicos permiten explicar cómo estos comportamientos se mantienen en el tiempo. La evidencia sugiere que muchas acciones inseguras se realizan de forma automática, reforzadas por experiencias previas sin consecuencias negativas

(Jayatilaka et al., 2021). Sesgos como el optimismo irreal, la familiaridad o la confianza mal colocada son sistemáticamente explotados por técnicas de ingeniería social (Ivanov et al., 2021). No obstante, algunos estudios indican que estos patrones pueden modificarse mediante intervenciones diseñadas para el comportamiento real del usuario, como nudges y retroalimentación adaptativa, en lugar de enfoques punitivos o normativos (Zimmermann et al., 2023).

En conjunto, la literatura revisada sugiere que los comportamientos humanos de riesgo en ciberseguridad no son conductas irracionales ni fallas individuales aisladas, sino respuestas previsibles a una combinación de factores cognitivos, emocionales, sociales y organizacionales. Comprender estos factores permite interpretar por qué prácticas inseguras persisten incluso en contextos con conocimiento técnico disponible. Desde esta perspectiva, la mitigación de dichos comportamientos requiere enfoques que integren diseño, comunicación y apoyo organizacional, reconociendo al usuario como un agente humano real y no como un actor idealizado.

3.3.- P3 ¿Cuáles son las formas de prevención, más allá de las soluciones tecnológicas, para abordar y mitigar comportamientos humanos de riesgo en ciberseguridad?

Si bien las herramientas técnicas son necesarias, resultan insuficientes cuando no consideran los factores emocionales, cognitivos, sociales y organizacionales que influyen en la conducta del usuario. Por consiguiente, la prevención efectiva requiere intervenir sobre el contexto humano en el que se toman las decisiones, más que limitarse al fortalecimiento de los mecanismos técnicos.

La evidencia analizada indica que una de las principales limitaciones de las estrategias tradicionales de seguridad radica en su enfoque racionalista. Los usuarios no siempre responden de forma lógica ante las exigencias del sistema; por el contrario, sus decisiones suelen estar mediadas por emociones como frustración, presión o ansiedad. Estudios recientes muestran que las políticas percibidas como coercitivas o punitivas tienden a generar resistencia y evasión, incluso cuando los usuarios reconocen su importancia (Von Preuschen et al., 2024). Desde esta perspectiva, la prevención se fortalece cuando se promueve una cultura de seguridad psicológica que reduzca la carga emocional, fomente la autonomía y permita aprender de los errores sin temor a sanciones. Cuando el entorno es percibido como justo y de apoyo, la disposición a adoptar comportamientos seguros aumenta.

Esta dimensión emocional se articula con la forma en que se concibe la educación en ciberseguridad. Los estudios analizados destacan que los enfoques tradicionales, centrados en normas abstractas y listas de advertencias, presentan una efectividad limitada. En contraste, los programas que incorporan aprendizaje experiencial, retroalimentación inmediata y escenarios realistas permiten una comprensión más profunda del riesgo (Jayatilaka et al., 2021). La participación activa del usuario, a través de ejercicios prácticos y discusiones guiadas, facilita que este identifique sus propios patrones de conducta y comprenda las consecuencias de sus decisiones (Kuraku et al., 2023). Asimismo, las advertencias contextuales integradas en la experiencia cotidiana del usuario han demostrado ser más efectivas que la capacitación aislada, lo que resalta la importancia del diseño pedagógico situado (Petelka et al., 2019).

Otra línea de prevención identificada en los estudios revisados es el uso de nudges o intervenciones conductuales suaves. Los hallazgos subrayan que estos mecanismos, al guiar la conducta sin imponer restricciones rígidas, resultan más eficaces que las políticas obligatorias. Investigaciones recientes muestran que la retroalimentación visual, los mensajes motivacionales y la explicación transparente de las decisiones seguras favorecen la adopción de buenas prácticas (Zimmermann et al., 2023). Estos enfoques aprovechan principios psicológicos como la

motivación positiva y la autoeficacia, reduciendo el rechazo emocional y fortaleciendo hábitos seguros de manera progresiva (Gulenko, 2015).

La comunicación organizacional también desempeña un papel relevante en la prevención. Los estudios indican que la distancia entre los equipos técnicos y los usuarios finales suele generar incomprensión y desconfianza. Cuando los mensajes de seguridad utilizan lenguaje excesivamente técnico o un tono autoritario, la colaboración disminuye. Diversos autores sostienen que una comunicación empática, clara y accesible facilita la comprensión y promueve una mayor adherencia a las medidas de seguridad (Von Preuschen et al., 2024). En este contexto, la figura del embajador de seguridad emerge como una estrategia efectiva para traducir el conocimiento técnico a un lenguaje cotidiano, favoreciendo el aprendizaje entre pares.

El diseño centrado en el usuario constituye otro componente clave. La evidencia recopilada apunta a que las medidas de seguridad resultan más efectivas cuando se integran de forma natural en el flujo de trabajo, considerando las limitaciones cognitivas y operativas del usuario. Interfaces intuitivas, alertas claras y márgenes de decisión controlados incrementan la aceptación de las medidas preventivas (Zimmermann et al., 2023). Este enfoque resulta particularmente relevante en entornos de alta criticidad, donde políticas rígidas pueden interferir con la operación y provocar conductas de evasión (Mugarza et al., 2021).

Finalmente, los estudios revisados coinciden en que la prevención debe concebirse como un proceso continuo y colaborativo. La conciencia en ciberseguridad se fortalece cuando existen espacios de aprendizaje colectivo, retroalimentación periódica y revisión compartida de incidentes (Makanto y Eze, 2023). La creación de comunidades internas donde los usuarios intercambian experiencias contribuye a normalizar comportamientos seguros y a reforzar la resiliencia organizacional (Hossain et al., 2023). Dado que las amenazas evolucionan constantemente, la actualización continua de estas estrategias resulta indispensable (Alkhalil et al., 2021).

En conjunto, el análisis de las investigaciones revisada sugiere que la prevención de los comportamientos humanos de riesgo en ciberseguridad requiere un enfoque integral que trascienda las soluciones tecnológicas. La combinación de apoyo emocional, educación adaptativa, nudges conductuales, comunicación empática, diseño centrado en el usuario y aprendizaje colaborativo permite transformar hábitos y reducir vulnerabilidades de forma sostenible. Desde esta perspectiva, la tecnología no actúa como un reemplazo del factor humano, sino como un aliado dentro de un entorno diseñado para apoyar decisiones seguras.

4.- Amenazas a la validez

Como en toda Revisión Sistemática de Literatura, existen ciertas amenazas metodológicas que deben ser reconocidas para contextualizar adecuadamente los hallazgos y evitar interpretaciones absolutas de los resultados.

Una de las principales amenazas corresponde a la barrera del idioma, dado que los estudios analizados se encuentran publicados en inglés y fueron traducidos para su análisis. Este proceso puede introducir riesgos de interpretación, especialmente al interpretar conceptos que vinculan la ciberseguridad con la psicología. Para reducir esta amenaza, la traducción se realizó de manera cuidadosa, priorizando el significado contextual de los conceptos sobre la traducción literal, y contrastando términos clave con definiciones técnicas estandarizadas. Asimismo, se mantuvo consistencia terminológica a lo largo del análisis para evitar ambigüedades conceptuales. Aun así, se reconoce que pueden persistir matices semánticos que no se reflejen completamente en la síntesis narrativa.

Otra amenaza está relacionada con la selección de los estudios primarios, la cual depende de las bases de datos consultadas y de los criterios de inclusión y exclusión definidos. Para mitigar esta limitación, se empleó una cadena de búsqueda estructurada y se consultaron múltiples fuentes académicas reconocidas, con el objetivo de ampliar la cobertura temática y reducir la omisión de trabajos relevantes. No obstante, es posible que algunos estudios pertinentes no hayan sido identificados o no estuvieran disponibles en las fuentes seleccionadas.

5.- Trabajo futuro

A partir de lo expuesto, los trabajos futuros pueden enfocarse en el diseño, evaluación y validación de estrategias orientadas a intervenir estos comportamientos desde una perspectiva centrada en el ser humano. Estas líneas de investigación se agrupan en tres ejes principales: en el rediseño de mecanismos de seguridad y la usabilidad segura, en la intervención cognitivo-emocional en la toma de decisiones de los usuarios y en las estrategias organizacionales y la evaluación longitudinal de dichas intervenciones.

Una de las oportunidades se relaciona con el diseño de mecanismos de seguridad más intuitivos y alineados con las capacidades cognitivas reales de los usuarios. Diversos estudios sugieren que la complejidad y rigidez de muchas medidas de seguridad favorecen la adopción de prácticas inseguras, lo que abre la posibilidad de investigar alternativas a los esquemas tradicionales basados exclusivamente en contraseñas, como mecanismos de autenticación multifactor, biometría o enfoques sin contraseña. Asimismo, futuras investigaciones podrían explorar el uso de nudges o intervenciones conductuales suaves como complemento o alternativa a políticas coercitivas, evaluando su efectividad no solo de manera inmediata, sino también en el tiempo, con el fin de identificar posibles efectos de habituación o fatiga de seguridad.

De igual forma podría explorarse el uso de inteligencia artificial para personalizar mensajes de concienciación en ciberseguridad, así como el diseño de alertas y contenidos empáticos que consideren el estado emocional del usuario. Asimismo, se abre la posibilidad de investigar fenómenos como la fatiga de seguridad, evaluando cómo la sobreexposición a advertencias o capacitaciones impacta negativamente en la atención y el cumplimiento de las recomendaciones de seguridad.

Adicionalmente, se destaca la dimensión organizacional y social de la ciberseguridad. La literatura revisada indica que los comportamientos de riesgo están influenciados por normas grupales, dinámicas laborales y culturas organizacionales. Investigaciones futuras podrían enfocarse en el análisis de la tensión entre usabilidad y seguridad en entornos institucionales, así como en el diagnóstico de la cultura de seguridad mediante instrumentos de medición específicos. Adicionalmente, podrían desarrollarse y evaluarse intervenciones organizacionales, como programas de embajadores de seguridad, capacitaciones colaborativas o estrategias de aprendizaje continuo, a través de estudios de caso o análisis longitudinales.

6.- Conclusiones

La síntesis de evidencia realizada a través de esta revisión sistemática permite identificar tendencias consistentes que sitúan a los comportamientos humanos de riesgo como uno de los factores de mayor incidencia en la seguridad de los sistemas de información. El uso de contraseñas débiles, la falta de actualización de software y la interacción con hipervínculos no verificados actúan como catalizadores de vulnerabilidades cuya explotación se ve favorecida cuando convergen factores cognitivos y emocionales. Los resultados analizados indican que estas

conductas no son eventos aislados, sino patrones estructurales que emergen de la interacción cotidiana del usuario con el entorno digital.

En relación con el uso de contraseñas, los estudios revisados muestran que esta práctica constituye una de las causas predominantes de accesos no autorizados. La evidencia señala que una parte considerable de los usuarios mantiene hábitos inseguros debido a una subestimación del riesgo o a la priorización de la conveniencia. Este comportamiento deriva en un debilitamiento de la autenticación que, como se ha observado, requiere soluciones que integren el rediseño técnico con el apoyo cognitivo, facilitando el recuerdo sin comprometer la robustez del sistema.

Respecto a la falta de actualización de software, los patrones identificados la posicionan como una de las brechas críticas de seguridad. Los reportes coinciden en que el retraso en la aplicación de parches es un resultado directo del desconocimiento o la percepción de interrupción operativa. La tendencia general subraya que esta omisión transforma vulnerabilidades conocidas en vectores de ataque recurrentes, lo que resalta la urgencia de transitar hacia una cultura de mantenimiento preventivo que reduzca la superficie de ataque organizacional.

Sobre la interacción con hipervínculos no verificados, los hallazgos confirman que este comportamiento persiste como uno de los vectores más explotados. Las investigaciones exponen que la eficacia del phishing reside en su capacidad para aprovechar automatismos y sesgos emocionales. La evidencia recopilada sugiere que la vulnerabilidad en este punto no se limita a una carencia técnica, sino que responde a factores psicopedagógicos, lo que orienta las estrategias de prevención hacia entrenamientos vivenciales y advertencias inteligentes.

En cuanto a los factores de influencia, la revisión documental demuestra que la seguridad digital es indisociable de las dimensiones cognitivas, emocionales y organizacionales. Los hallazgos subrayan que los fallos suelen estar vinculados a modelos mentales incompletos o sobrecarga informativa. Este panorama plantea que la ciberseguridad debe abordarse desde el diseño de entornos que consideren las capacidades y limitaciones reales del individuo, mitigando el impacto de la fatiga de seguridad.

Por otra parte, las estrategias de prevención dirigidas a usuarios finales emergen como enfoques transversales donde la educación adaptativa, el diseño centrado en el usuario y los nudges (intervenciones sutiles para orientar decisiones seguras) se posicionan como las tendencias más prometedoras. El análisis permite concluir que la ciberseguridad debe integrar de manera equilibrada los controles técnicos con la comprensión del factor humano. En última instancia, esta investigación valida que un enfoque holístico y empático es la vía más efectiva para transformar hábitos inseguros en resiliencia digital sostenible.

De manera específica, las estrategias de prevención más efectivas identificadas en esta revisión se caracterizan por su orientación no represiva y su adaptación al contexto humano del usuario final. La evidencia analizada permite concluir que las intervenciones basadas en educación emocional, formación experiencial, retroalimentación conductual mediante nudges y comunicación organizacional empática generan mejores resultados que los enfoques normativos tradicionales. Estas estrategias reducen la resistencia, favorecen la internalización del riesgo y promueven una participación del usuario en la seguridad de la información. Asimismo, el fortalecimiento de culturas organizacionales positivas y de esquemas de aprendizaje continuo se consolida como un elemento clave para sostener los comportamientos seguros en el tiempo. En este sentido, la prevención en ciberseguridad no debe concebirse como una acción puntual, sino como un proceso estratégico, progresivo y centrado en las personas.

Referencias

Baki, S., Verma, R., Mukherjee, A., & Gnawali, O. (2017). Scaling and effectiveness of email masquerade attacks: Exploiting natural language generation. En *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (pp. 469–482). Association for Computing Machinery. **https://doi.org/10.1145/3052973.3053037**

Bilge, L., Han, Y., & Dell'Amico, M. (2017). RiskTeller: Predicting the risk of cyber incidents. En *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1299–1311). Association for Computing Machinery. **https://doi.org/10.1145/3133956.3134022**

Coker, J. (2025). *95% of data breaches tied to human error in 2024*. Infosecurity Magazine. **https://www.infosecurity-magazine.com/news/data-breaches-human-error/**

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys, 54*(8), Article 173, 1–35. **https://doi.org/10.1145/3469886**

French, L. (2025, 11 de marzo). *95% of data breaches involve human error, report reveals*. SC World. **https://www.scworld.com/news/95-of-data-breaches-involve-human-error-report-reveals/**

Gulenko, I. (2014). Improving passwords: Influence of emotions on security behaviour. *Information Management & Computer Security, 22*(2), 167–178. **https://doi.org/10.1108/IMCS-09-2013-0068**

Hossain, M. N., Hassan, M. M., Monir, R. J., Sayeed, M. S., Wajiha, S., & Ullah, S. W. (2023). Cyber security and people: Human nature, psychology, and training affect user awareness, social engineering, and security professional education and preparedness. En *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE. **https://doi.org/10.1109/ICCCNT56998.2023.10307467**

Iannone, E., Sellitto, G., Iaccarino, E., Ferrucci, F., De Lucia, A., & Palomba, F. (2024). Early and realistic exploitability prediction of just-disclosed software vulnerabilities: How reliable can it be? *ACM Transactions on Software Engineering and Methodology, 33*(6), 1–41. **https://doi.org/10.1145/3654443**

Ivanov, N., Lou, J., Chen, T., Li, J., & Yan, Q. (2021). Targeting the weakest link: Social engineering attacks in Ethereum smart contracts. En *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security* (pp. 787–801). Association for Computing Machinery. **https://doi.org/10.1145/3433210.3453085**

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences, 10*, Article 33. https://doi.org/10.1186/s13673-020-00237-7

Jayatilaka, A., Arachchilage, N. A. G., & Babar, M. A. (2021). Falling for phishing: An empirical investigation into people's email response behaviors. En *Proceedings of the 42nd International Conference on Information Systems (ICIS 2021)*. **https://doi.org/10.48550/arXiv.2108.04766**

Jones, A. (2024). *Human error cybersecurity statistics*. I.S. Partners. **https://www.ispartnersllc.com/blog/human-error-cybersecurity-statistics/**

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting & Information Management, 28*(2), 275–301. **https://doi.org/10.1108/IJAIM-01-2019-0006**

Khadka, K., Ullah, A. B., Ma, W., Marroquin, E. M., & Alem, Y. (2023). A survey on the principles of persuasion as a social engineering strategy in phishing. En *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 1631–1638). IEEE. **https://doi.org/10.1109/TrustCom60117.2023.00222**

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering* (EBSE Technical Report EBSE-2007-01). Keele University & Durham University. **https://ebse.webspace.durham.ac.uk/ebse-bibliography/guidelines-for-performing-systematic-literature-reviews-in-software-engineering/**

Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors related to cyber security behavior. *IEEE Access, 8*, 125140–125148. **https://doi.org/10.1109/ACCESS.2020.3007867**

Kumar, I. (2023). Emerging threats in cybersecurity: A review article. *International Journal of Applied and Natural Sciences, 1*(1), 1–8. **https://bluemarkpublishers.com/index.php/IJANS/article/view/2**

Kuraku, S., Kalla, D., Smith, N., & Samaah, F. (2023). Exploring how user behavior shapes cybersecurity awareness in the face of phishing attacks. *International Journal of Computer Trends and Technology, 71*(11), 74–79. **https://doi.org/10.14445/22312803/IJCTT-V71I11P111**

Makanto, P. K., & Eze, J. S. (2023). *Mitigating human vulnerabilities in cybersecurity: Understanding human flaws and implementing effective countermeasures*. Bournemouth University. **https://www.researchgate.net/publication/376520059_Mitigating_Human_Vulnerabilities_in_Cybersecurity_Understanding_Human_Flaws_and_Implementing_Effective_Countermeasures**

Montañez, R., Golob, E., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. *Frontiers in Psychology, 11*, 1755. **https://doi.org/10.3389/fpsyg.2020.01755**

Mugarza, I., Yarza, I., Agirre, I., Lussiana, F., & Botta, S. (2021). *Safety and security concept for software updates on mixed-criticality systems*. CORDIS, European Commission. **https://cordis.europa.eu/project/id/871465/results**

Pashchenko, I., Vu, D.-L., & Massacci, F. (2020). A qualitative study of dependency management and its security implications. En *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1513–1531). Association for Computing Machinery. **https://doi.org/10.1145/3372297.3417232**

Petelka, J., Zou, Y., & Schaub, F. (2019). Put your warning where your link is: Improving and evaluating email phishing warnings. En *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery. **https://doi.org/10.1145/3290605.3300748**

Popay, J., Roberts, H., Sowden, A., Petticrew, M., Arai, L., Rodgers, M., Britten, N., Roen, K., & Duffy, S. (2006). *Guidance on the conduct of narrative synthesis in systematic reviews: A product from the ESRC Methods Programme*. **https://doi.org/10.13140/2.1.1018.4643**

Sathe, A. K., Patil, D. D., Lalge, G. V., & Nawale, S. R. (2025). Social engineering attack: Understanding human vulnerability in cybersecurity. *International Journal of Social Impact*. **https://ijsi.in/pdf-viewer/?id=2254**

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy, 2*(3), 573–586. **https://doi.org/10.3390/jcp2030029**

Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016). Do users' perceptions of password security match reality? En *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 3748–3760). Association for Computing Machinery. **https://doi.org/10.1145/2858036.2858546**

von Preuschen, A., Schuhmacher, M. C., & Zimmermann, V. (2024). Beyond fear and frustration: Towards a holistic understanding of emotions in cybersecurity. En *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (pp. 623–642). USENIX Association. **https://www.usenix.org/conference/soups2024/presentation/von-preuschen**

Wang, B., Li, X., de Aguiar, L. P., Menasché, D. S., & Shafiq, Z. (2017). Characterizing and modeling patching practices of industrial control systems. *Proceedings of the ACM on Measurement and Analysis of Computing Systems, 1*(1), 1–23. **https://doi.org/10.1145/3084455**

Wash, R., & Rader, E. (2021). Prioritizing security over usability: Strategies for how people choose passwords. *Journal of Cybersecurity, 7*(1), tyab012. **https://doi.org/10.1093/cybsec/tyab012**

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. En *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*. Association for Computing Machinery. **https://doi.org/10.1145/2601248.2601268**

Yeng, P. K., Fauzi, M. A., & Yang, B. (2022). A comprehensive assessment of human factors in cyber security compliance toward enhancing the security practice of healthcare staff in paperless hospitals. *Information, 13*(7), 335. **https://doi.org/10.3390/info13070335**

Yeo, L. H., & Banfield, J. (2022). Human factors in electronic health records cybersecurity breach: An exploratory analysis. *Perspectives in Health Information Management, 19*(Spring), 1i. **https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525/**

Zhang, H., Babar, M. A., & Tell, P. (2011). Identifying relevant studies in software engineering. *Information and Software Technology, 53*(6), 625–637. https://doi.org/10.1016/j.infsof.2010.12.010

Zimmermann, V., Marky, K., & Renaud, K. (2020). How experts detect phishing scam emails. *Proceedings of the ACM on Human-Computer Interaction, 4*(CSCW2), 1–28. **https://doi.org/10.1145/3415231**

Zimmermann, V., Marky, K., & Renaud, K. (2023). Hybrid password meters for more secure passwords: A comprehensive study of password meters including nudges and password information. *Behaviour & Information Technology, 42*(6), 700–743. **https://doi.org/10.1080/0144929X.2022.2042384**

Bibliografías

Alberto Jair Cruz Landa: es profesor de tiempo completo en la Facultad de Estadística e Informática de la Universidad Veracruzana adscrito a la licenciatura en ingeniería de Ciberseguridad e Infraestructura de Cómputo en la ciudad de Xalapa, Veracruz. Licenciado en Informática, con maestría en Redes Computacionales y Doctorado en ciencias en el área de alta dirección. Sus áreas de interés se encuentran enfocado en el área de ciberseguridad, principalmente en el rubro de aspectos humanos, organizativos y regulatorios, así como la seguridad en infraestructura ataques y defensas.

Juan Manuel Gutiérrez Méndez: es Profesor de Tiempo Completo de la Facultad de Estadística e Informática de la Universidad Veracruzana y participa en la Licenciatura en Ciberseguridad e Infraestructura de Cómputo. Su trayectoria profesional y académica se ha desarrollado en los ámbitos de tecnologías de la información, infraestructura tecnológica, desarrollo de software y ciberseguridad. Sus áreas de interés se centran en las tecnologías de la información y la ciberseguridad, particularmente en protección de datos, seguridad de infraestructura, ciberseguridad usable y aplicación de marcos de referencia con una perspectiva tecnológica, organizacional y humana.

Juan Carlos Jiménez Márquez: es Profesor de Tiempo Completo de la Facultad de Estadística e Informática de la Universidad Veracruzana. Es Licenciado en Informática, Maestro en Comunicación y Tecnologías Educativas y Doctor en Educación. Su trayectoria académica y profesional se ha desarrollado en las áreas de tecnologías de la información, redes, servicios de cómputo, infraestructura tecnológica y ciberseguridad. Sus áreas de interés se centran en ciberseguridad, seguridad de redes e infraestructura, Internet de las Cosas y aplicación de tecnologías emergentes en contextos educativos.

Martha Elizabet Domínguez Bárcenas. Es Profesora de Tiempo Completo en la Facultad de Estadística e Informática de la Universidad Veracruzana, con adscripción a la Lic. en Ingeniería de Ciberseguridad e Infraestructura de Cómputo. Es Licenciada en Informática y Maestra en Redes y Telecomunicaciones. Su trayectoria académica se ha desarrollado en las áreas de redes e infraestructura tecnológica. En el ámbito de la ciberseguridad, sus áreas de interés se orientan a la seguridad de infraestructura y a la ciberseguridad social.

Alicia Yazmín Rojas Luna: es Técnico Académico de la Facultad de Estadística e Informática de la Universidad Veracruzana. Es Licenciada en Informática, Maestra en Sistemas Interactivos Centrados en el Usuario y Maestra en Ciberseguridad. Su experiencia académica y profesional se desarrolla en las áreas de Interacción Humano-Computadora, Experiencia de Usuario y Ciberseguridad, con énfasis en diseño centrado en el usuario, evaluación de usabilidad y UX, accesibilidad y seguridad usable. Sus áreas de interés se enfocan en el estudio de la interacción entre las personas y los sistemas digitales, particularmente en privacidad, diseño de experiencias seguras, comportamiento del usuario ante riesgos de ciberseguridad y evaluación de tecnologías interactivas desde una perspectiva humana, tecnológica y de seguridad.