DOI: https://doi.org/10.5281/zenodo.16944387

Influencia de los aspectos culturales en el desarrollo de estrategias de ciberseguridad

Influence of cultural aspects in the development of cybersecurity strategies

Dylan Alejandro Velásquez-Leonardo,[1] Juan Carlos Pérez-Arriaga,[2] Martha Elizabet Domínguez-Bárcenas[3] y Héctor Xavier Limón-Riaño[4]

Resumen: La ciberseguridad se considera como el conjunto de prácticas para prevenir amenazas o vulnerabilidades en sistemas digitales que puedan derivar en el robo, alteración o destrucción de información confidencial. Se considera que parte de los problemas de ciberseguridad, de forma intencionada o no, son generados por los usuarios de las TIC, a causa de aspectos culturales y comportamientos sociales. Este estudio se enfoca en la identificación y análisis de los aspectos culturales y el comportamiento de los usuarios que puede influir en la definición y seguimiento de estrategias de ciberseguridad. Utilizando una revisión de literatura multivocal (MLR), se identificaron 38 estudios de literatura blanca y gris que incluyen información sobre el tema. Entre los principales hallazgos se describen factores y errores humanos, elementos demográficos que afectan la ciberseguridad; así como estrategias y técnicas propuestas para contribuir a la disminución de este tipo de problemas de ciberseguridad.

Palabras clave: ciberseguridad, comportamiento humano, aspectos culturales.

Abstract: Cybersecurity is the set of practices to prevent threats or vulnerabilities in digital systems that may result in the theft, alteration, or destruction of confidential information. It is considered that a good part of cybersecurity problems, intentionally or unintentionally, are generated by ICT users due to cultural aspects and social behaviors. This study focuses on identifying and analyzing cultural aspects and user behaviors that may influence the definition and monitoring of cybersecurity strategies. Using a multivocal literature review (MLR), we identified 38 white and gray literature studies that include information on the topic. We identified some human factors, errors, and demographic elements that affect cybersecurity, such as cyber indifference, willingness to comply, age, and gender. We also identified strategies and techniques proposed to contribute to the reduction of this type of cybersecurity problems, where education and user awareness stand out.

1 Universidad Veracruzana, davl.rsc180@gmail.com; ORCID: 0009-0004-2968-5135
2 Universidad de Alcalá, juancarlos.pereza@edu.uah.es, Universidad Veracruzana, juaperez@uv.mx; ORCID: 0000-0003-2354-2462
3 Universidad Veracruzana, eldominguez@uv.mx; ORCID: 0009-0003-8197-5095
4 Universidad Veracruzana, hlimon@uv.mx; ORCID: 0000-0003-4654-636X

Keywords: cybersecurity, human behavior, cultural values

Introducción

En una revisión inicial sobre el tema se encontraron algunos datos y estudios que destacan la importancia de las decisiones humanas en aspectos de ciberseguridad. Muchos problemas en esta área se deben a errores o descuidos derivados de creencias, ideologías o aspectos culturales de los usuarios de las TIC. Se menciona la desventaja psicológica que presentan los usuarios al momento de enfrentarse a un ataque de ciberseguridad. También se destaca la necesidad de una planeación de estrategias de ciberseguridad que puedan resultar efectivas para los problemas detectados.

Ante un panorama de estudios dispersos sobre el tema, el objetivo de esta investigación es la identificación y análisis de los aspectos culturales que pueden influir en la definición y seguimiento de estrategias de ciberseguridad. Para la recopilación de información se realizó una revisión multivocal de literatura, apegada a las pautas de Garousi y otros (2019), con el fin de recuperar evidencia científica y práctica sobre el tema. La síntesis de la información se apegó a la metodología de Popay y otros (2006), para una síntesis narrativa. Las respuestas a las preguntas que guiaron la investigación quedan plasmadas en los hallazgos resultantes del análisis de 38 estudios primarios seleccionados.

Una vez analizados los estudios, se obtuvo información valiosa sobre el comportamiento y los aspectos culturales de los usuarios que influyen en el manejo de situaciones de ciberseguridad, su impacto en las organizaciones; así como la identificación de estrategias que contemplen dichos elementos para mejorar la ciberseguridad.

Problemática y contexto de la problemática

En el ámbito de la seguridad de la información un fallo mínimo puede implicar que los datos y la información se vean comprometidos. De acuerdo con un estudio realizado por Kaspersky en 2017 a nivel global, en ese momento, el 46% de los ataques e incidentes de seguridad se debieron a descuidos o falta de formación por parte del personal (Kaspersky, s.f.). Por su parte, Hamilton (2021) indica que el costo promedio de una filtración de datos en 2020 ascendió hasta 3.86 millones de dólares, lo que representa un problema muy grave para las organizaciones.

Los fallos de seguridad pueden ser derivados de errores o descuidos técnicos, pero muchos de ellos pueden ser generados por los usuarios. Algunos errores podrían ser generados con la intención de dañar, pero en otras ocasiones las decisiones en materia de seguridad pueden ser derivadas de creencias, ideologías o aspectos culturales.

Estudios como el de Onumo y otros (2017) indican que la cultura tiene influencia en el uso y desarrollo de sistemas de información; sin embargo, se detecta la ausencia de estudios que busquen comprender la influencia de la cultura nacional en temas de ciberseguridad. Hadlington (2017) aborda la relación que existe entre algunos factores como los comportamientos de ciberseguridad riesgosos, las actitudes hacia la ciberseguridad en un entorno empresarial, la adicción a internet y la impulsividad emocional de las personas. Wiederhold (2014) presenta evidencia de investigaciones que mencionan que la psicología puede tener un papel muy importante para mitigar el riesgo de la seguridad en el ciberespacio.

Estudios como los anteriores se encuentran dispersos en la literatura, por lo que se identificó la necesidad de recolectar y analizar aquellos estudios que sugieren que la cultura y el comportamiento de los usuarios son parte fundamental para la ciberseguridad, con la intención de exponer el panorama de oportunidades para la generación y/o fortalecimiento de una cultura de ciberseguridad.

Fundamentación teórica

La ciberseguridad se puede definir como el conjunto de herramientas, reglas y métodos que permiten mantener un entorno tecnológico seguro y proteger los activos y usuarios que dependen de dicha tecnología (Unión Internacional de Telecomunicaciones, 2008).

Burnap (2021) distingue cuatro conceptos fundamentales para una evaluación de riesgos de ciberseguridad: la vulnerabilidad, entendida como una desprotección que ante un ataque podría conducir a un resultado no deseado; la amenaza, que puede ser un individuo, evento o acción que tiene la capacidad de explotar una vulnerabilidad; la probabilidad de que un ataque aproveche una vulnerabilidad y produzca un resultado indeseable; y el impacto o efecto negativo de una amenaza que explota una vulnerabilidad. En ciberseguridad existen varios elementos que pueden influir, como: políticas y procedimientos, infraestructura tecnológica, software y aplicaciones. Sin embargo, al ser un campo en constante evolución, los factores que intervienen pueden variar a medida que se crean nuevas tecnologías y surgen nuevas amenazas, tal es el caso de los aspectos culturales.

Los aspectos culturales se refieren al conjunto de elementos y características que constituyen la identidad de una sociedad, grupo o comunidad; como pueden ser la historia, la religión, el idioma, el arte, la vestimenta, la economía, la ética, la educación, entre otros. En este sentido, la cultura organizativa, se entiende como el conjunto de creencias, valores, normas y reglas que definen el comportamiento de una organización y sus integrantes (Santander Open Academy, 2022). La cultura de seguridad es un término que abarca diferentes actitudes y valores de las personas, en aspectos relativos a la seguridad (ESGinova Group, 2020).

El comportamiento humano es el resultado de la interacción entre el ambiente y la historia de aprendizaje del individuo (Skinner, 1953), se refiere a todas las acciones y conductas que un individuo realiza en respuesta a los estímulos internos y externos que enfrenta y está influenciado por factores como la historia, el aprendizaje, el ambiente y la cultura. El error humano está directamente ligado con el comportamiento humano. Los errores ocurren como resultado de fallas latentes y fallas activas, como las condiciones del lugar de trabajo y las violaciones por parte de los humanos, respectivamente (Reason, 2008, como se cita en Sasse y Rashid, 2021). Reason identifica cuatro tipos de factores que influyen en que las personas cometan errores: factores individuales (como fatiga e inexperiencia), factores humanos (características físicas, psicológicas y sociales que afectan la interacción humana), factores de la tarea (múltiples tareas, aburrimiento, presión del tiempo, etcétera) y factores del entorno (interrupciones en tareas, equipos e información deficientes). Otro aspecto que puede afectar el comportamiento de las personas es la influencia cultural; es decir, las creencias, valores, normas y costumbres compartidos por una comunidad o sociedad, que influyen en las actitudes y comportamientos de sus miembros (Hofstede, 2002).

Algunos factores humanos pueden afectar la gobernanza de la seguridad, por ejemplo, al no creer que los activos están en riesgo o no entender que el comportamiento de las personas puede poner en riesgo el sistema (Sasse y Flechais, 2005).

Metodología aplicada

Se elaboró una revisión de literatura multivocal (MLR, por sus siglas en inglés), de acuerdo con la metodología de Garousi y otros (2019). Una MLR se caracteriza por considerar estudios que incluyan la perspectiva de investigadores y de profesionales en el área, por medio de la inclusión de literatura blanca o formal (proveniente de revistas y conferencias científicas); así como de literatura gris (producida en distintos niveles de gobierno, instituciones académicas, comerciales e industriales). Este enfoque se considera adecuado para buscar respuesta a las preguntas de investigación planteadas en la tabla 1.

Tabla 1. Preguntas de investigación

No.	Pregunta	Descripción
PI1	¿Cuál es el comportamiento humano reportado en la literatura asociado al tema de ciberseguridad?	PI1 pretende identificar el comportamiento de los usuarios al encontrarse en situaciones que involucren la toma de decisiones sobre ciberseguridad.
PI2	¿Qué aspectos culturales tienen relación con la adopción de buenas prácticas de ciberseguridad?	PI2 intenta determinar si existen aspectos culturales que afecten las buenas prácticas de ciberseguridad en los usuarios.

PI3	¿Cómo afectan los aspectos culturales en la definición y seguimiento de estrategias de ciberseguridad?	PI3 tiene como intención ayudar a comprender la influencia de los aspectos culturales en el seguimiento a las estrategias de ciberseguridad.
PI4	¿Qué estrategias son posibles de implementar para mejorar la ciberseguridad, tomando en cuenta los aspectos culturales relacionados con su adopción?	PI4 explora las estrategias que puedan diseñarse o adaptarse junto con los aspectos culturales identificados, para un entorno seguro en el uso de las tecnologías.

Estrategia de búsqueda

Como fuentes de información se consideraron bases de datos que proporcionan acceso a artículos y revistas científicas en el área de ciencias de la computación: ACM Digital Library, IEEE Explore y Science Direct. Para la literatura gris se utilizó el motor de búsqueda de Google. A partir de una exploración inicial del tema y de las preguntas de investigación, se llegó a la siguiente cadena de búsqueda: Cybersecurity AND ("culture" OR "human" OR "psycology" OR "human-behaviour" OR human-factor). La tabla 2 muestra los criterios para la selección de los estudios primarios.

Tabla 2. Criterios de inclusión y exclusión

Criterios de inclusión	Criterios de exclusión
CI1. El estudio está en idioma inglés. **CI2**. El estudio fue publicado entre 2017 y 2022 (noviembre). **CI3**. El título da indicios de responder al menos una pregunta de investigación. **CI4**. Para literatura blanca, el *abstract* da indicios de que el estudio puede aportar la investigación. **CI5**. Para literatura gris, si la fuente no tiene un *abstract*, se hace una lectura rápida para verificar si puede responder al menos a una de las preguntas de investigación. **CI6**. Si el estudio responde al menos a una de las preguntas de investigación, se toma en cuenta para su revisión.	**CE1**. Se descartan los estudios a los que no se tenga acceso completo. **CE2**. Se excluyen estudios repetidos y/o encontrados en otros motores de búsqueda. **CE3**. No se contemplan presentaciones o infografías por falta de detalle en la información que brindan. **CE4**. Se excluyen revisiones sistemáticas o multi vocales de literatura. **CE5**. Se excluyen libros al ser en su mayoría contenido limitado o con acceso de pago.

Como criterios de paro o de detención de la búsqueda, se utilizaron dos: agotamiento de la evidencia; es decir, detenerse cuando la evidencia es escasa y esfuerzo limitado, lo que implica considerar los primeros 100 resultados del motor de búsqueda en el caso literatura gris.

Criterios de evaluación de calidad

De acuerdo con las pautas de evaluación de calidad propuestas por Garousi y otros (2019), se contemplaron ocho factores de calidad agrupados en cinco criterios para la valoración de literatura gris (GL), tal como se muestra en la tabla 3. A cada pregunta se le asignó un valor numérico (Si = 1, Parcialmente = 0.5, No = 0) que permite evaluar si el estudio cumple o no, con los criterios correspondientes (al menos 70% del total).

Tabla 3. Criterios de evaluación de calidad

Criterio	Factor de calidad
Autoridad del autor/editor	¿El autor/editor tiene experiencia en el tema?
	¿El autor/editor, está relacionado al campo en cuestión?
Metodología	¿La fuente tiene un objetivo claramente establecido?
	¿El trabajo cubre una pregunta específica?
	¿La fuente tiene una metodología establecida?
Objetividad	¿Las conclusiones están respaldadas por el contenido de la publicación?
Novedad	¿Enriquece o agrega algo único a la investigación?
Tipo de salida	• 1er nivel GL (medida = 1): alto control de salida/alta credibilidad: libros, revistas, tesis, informes gubernamentales, libros blancos. • 2do nivel GL de segundo nivel (medida = 0,5): Control de salida moderado/Credibilidad moderada: informes anuales, artículos de noticias, presentaciones, videos, sitios de preguntas y respuestas, artículos wiki, etc. • 3er nivel GL (medida = 0): Control de salida bajo/ Baja credibilidad: blogs, correos electrónicos, tuits.

Selección de estudios

Se obtuvo un total de 38 estudios: 18% en IEEE Xplore, 16% en ACM Digital Library, otro 16% en Science Direct y el 50% restante corresponde a estudios de literatura gris encontrados a través del motor de búsqueda Google.

Extracción, análisis y síntesis de datos

Se diseñó una plantilla de extracción de datos en la que se registraron las respuestas a las preguntas de investigación, así como los datos generales de cada estudio. Una vez analizados los 38 estudios, se observaron algunas tendencias en su distribución: se obtuvieron más respuestas para la PI1, siendo la PI3 para la que menos información se obtuvo; la mayoría de los estudios de literatura blanca corresponden a los años 2020 y 2021; los estudios de literatura gris también comenzaron a incrementar a partir del año 2020. Después del análisis de los estudios, se realizó una síntesis narrativa de acuerdon con las pautas de Popay y otros (2006).

Resultados

Una vez clasificada la información, se llegó a los siguientes resultados:

Comportamiento humano asociado al tema de ciberseguridad

El comportamiento se ve influido por diversos factores de orden genético, social, cultural, psicológico, económico y afectivo (Villanueva, 2022), por lo tanto, es importante comprender el comportamiento de los usuarios para evitar fallas o errores en la ciberseguridad. La tabla 4 destaca los resultados al respecto, divididos en cuatro aspectos del comportamiento humano.

Tabla 4. Aspectos del comportamiento humano asociado al tema de ciberseguridad

Aspecto	Autor	Resultados
Desinterés por parte del usuario	Onumo et al., 2021	El conocimiento de la ciberseguridad y las creencias cognitivas de los empleados influyen en su intención de cumplir con los mecanismos de control de la ciberseguridad organizacional. Por ejemplo, podrían incumplir los procesos de ciberseguridad por dar prioridad a la finalización del trabajo.
	Wang et al., 2021	La indiferencia hacia el trabajo dificulta el cumplimiento de las reglas de seguridad.
	Reegård et al., 2019; SecurityBrief Australia, 2022	La apatía de algunos usuarios hacia las amenazas de ciberseguridad puede derivar de que la consideran como un problema que corresponde atender al área de tecnologías de la información. El concepto de "indiferencia cibernética" se refiere a la incapacidad que siente un individuo de poder influir significativamente sobre los resultados de ciberseguridad.
	Kovacevic et al., 2020	A pesar de disponer de múltiples recursos en la internet sobre conocimientos básicos de seguridad, no se ha despertado el interés de los estudiantes universitarios por aprender al respecto.
Elementos demográficos relacionados al comportamiento de los usuarios	Creese et al. 2021	Las naciones comparten actitudes, valores y prácticas similares en torno a la seguridad cibernética, sin embargo, hay diferencias marcadas por nivel de desarrollo de los países.
	Szczepaniuk et al., 2022	Existe una relación entre la educación, la edad y el conocimiento de las amenazas en el ciberespacio. Siendo este último considerablemente mayor en personas con título académico.
	CYDEF, 2021	La experiencia de personas mayores de 51 años puede ayudarlos a detectar cuando algo "no se siente" del todo bien al recibir un correo electrónico de phishing, evitando su apertura.
Comportamientos y acciones	Abroshan et al., 2021; Greitzer et al., 2021; Ovelgönne et al., 2017	Los comportamientos y actitudes de los usuarios en internet influyen en la probabilidad de ser víctimas de ataques de phishing. El estudio de Greitzer et al. (2021) demostró que los participantes que aceptaron haber sido víctimas de phishing tenían más probabilidades de seguir un enlace que tenía el mismo objetivo. Ovelgönne et al. (2017) indican que la probabilidad e intensidad con la que una computadora es atacada por malware está relacionada con el comportamiento del usuario.

Aspecto	Autor	Resultados
El factor y el error humano	Linkov et al., 2019	El uso frecuente de computadora en el trabajo, para fines no laborales, indica una menor conciencia de la seguridad en la internet. Las personas ansiosas tienen menos éxito al detectar un ciberataque. Los hombres tienen más experiencia en ciberseguridad que las mujeres.
	Hughes-Lartey et al., 2021	La cultura de la seguridad se considera como un factor humano asociado con la voluntad del usuario para seguir los procedimientos de seguridad establecidos.
	Trilateral Research, 2022	Las diferentes áreas de una organización tienen conflicto de prioridades respecto a la seguridad cibernética; ciertas presiones impiden el desarrollo de una ciberseguridad efectiva en la organización. Ver a los empleados como vectores de amenazas afecta los niveles de confianza dentro de la organización.
	Ahola, 2022	Tres factores que intervienen en el error humano son: la oportunidad de que exista el error, factores ambientales y falta de conciencia sobre el efecto de las acciones realizadas.
	Johnston y Warkentin, 2010; Herath y Rao, 2009; Posey et al., 2015, como se cita en Li y He, 2022	La influencia social y la información organizacional pueden ayudar a que los usuarios adopten programas de seguridad. Si la organización cuenta con políticas bien establecidas, es más probable que los usuarios reciban capacitación, información o consejos al respecto.
	Siruela, 2021; VOX Network Solutions, 2019	El factor humano debe ser considerado como un elemento básico dentro de la ciberseguridad, ya que tanto la estructura de seguridad, como las acciones técnicas y formativas están diseñadas por personas. Se recomienda el autodiagnóstico de malos hábitos y comportamientos negligentes por parte de los empleados, así como su identificación y señalamiento por parte de los gerentes.

Aspectos culturales relacionados con las prácticas de ciberseguridad

Se identificaron algunos aspectos culturales y su relación con elementos demográficos y con el comportamiento humano, que impactan en la ciberseguridad, los cuales se describen en la tabla 5. Cabe destacar que una de las consecuencias de los incidentes de ciberseguridad en los que se involucran aspectos culturales, son los altos costos que la mayoría de las pequeñas y medianas empresas no pueden permitirse (CYDEF, 2021).

Estrategias para mejorar la ciberseguridad tomando en cuenta aspectos culturales

Las estrategias identificadas se muestran en la tabla 6.

Tabla 5. Aspectos culturales que influyen en las prácticas de ciberseguridad

Relación	Autor	Resultados
Elementos demográficos	Hughes-Lartey et al., 2021	La cultura nacional puede tener un efecto directo sobre el nivel de protección de la información y el comportamiento. Por ejemplo, las culturas organizacionales occidentales son más individualistas, mientras que las asiáticas son más colectivas.
	Li y He, 2022; Kocksch et al., 2018	Las mujeres reconocen mejor las acciones no éticas y es más probable que reporten malas acciones relacionadas con TI. El cuidado de la seguridad de TI es predominantemente masculino, sin embargo, son frecuentes las demandas de más atención es aspectos de seguridad, por ello se considera que la ciberseguridad podría mejorar con mujeres expertas en el área en posiciones de liderazgo.
	Van Bavel et al., 2019, como se cita en Li y He, 2022	Los adultos mayores son más vulnerables a ciertos ataques de phishing, mientras que los jóvenes nacidos después de 1996 se consideran menos sensibles a los ciberataques, dado que tienen más experiencia al respecto.
Comportamiento humano	SecurityBrief Australia, 2022	La seguridad cibernética se percibe como muy costosa, demasiado compleja y un esfuerzo inútil, debido al poder de las amenazas cibernéticas.
	Kaspersky, s/f	La existencia de reglas estrictas y poco claras puede fomentar temores entre el personal, derivando en la falta de comunicación de los incidentes de ciberseguridad a la alta dirección y a recursos humanos, para evitar ser sancionados.
	Wang et al., 2021	La inexperiencia de los nuevos empleados, puede hacerlos caer en ataques de ingeniería social, en el afán de causar una buena primera impresión.

Tabla 6. Estrategias para mejorar la ciberseguridad considerando aspectos culturales

Estrategia	Autor	Resultados
Capacitación y concientización	Greitzer et al., 2021; Frenken, 2020	Se sugiere brindar capacitación a los usuarios sobre hábitos saludables de seguridad, así como concientizar a los usuarios de las posibles consecuencias negativas de no cumplir con dichos hábitos. La formación en ciberseguridad debe ser periódica a lo largo del año.
	Siruela, 2021	Una iniciativa que apoya a la concientización en ciberseguridad es la recompensa y el reconocimiento a aquellos empleados que participen en la detección de vulnerabilidades o fallos de seguridad, tanto a nivel técnico como de gestión.
Implementación de frameworks o metodologías	AlQadheeb et al., 2022	Se proponen un marco de seguridad que considera las intenciones humanas, las actitudes, las normas y los comportamientos en la toma de decisiones en ciberseguridad, centrándose en cuatro elementos: protección de dispositivos, generación de contraseñas, concienciación proactiva y actualización.
	Hughes-Lartey et al.,2021	Se proponen un marco de seguridad de la información para el Internet de las Cosas (IoT) enfocado en factores humanos, que considera contramedidas para: hacking, pérdida y robo, acceso o divulgación no autorizados y eliminación inadecuada.
	Hajny et al., 2021	Se comparte una metodología que permite diseñar programas de estudio de educación superior en ciberseguridad, basada en el diseño del Marco de Habilidades de Ciberseguridad de los Programas Estratégicos para la Investigación y Tecnología Avanzadas en Europa (SPARTA CSF), en el trabajo de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), la Organización Europea de Seguridad Cibernética (ECSO) y otros proyectos piloto de Cyber Competence Network (CCN).
Fomento de una cultura de seguridad	Florida Tech Online, 2023	Se recomienda evaluar el estado actual de la seguridad organizacional, establecer la meta para la seguridad y la tecnología, involucrar a ejecutivos y a empleados, definir roles y expectativas.
	VOX Network Solutions, 2019; McAlmont, 2022	Se recomienda limitar accesos y vigilar de cerca el trabajo de los empleados. Hacer que la ciberseguridad forme parte de las evaluaciones de desempeño y los sistemas de recompensa, responsabilizar a los empleados que no cumplan con los protocolos de ciberseguridad.
	OnSolve, 2020; VOX Network Solutions, 2019	Se recomienda elaborar un plan que incorpore las mejores prácticas de ciberseguridad.

Discusión

Una vez analizados los hallazgos se encontró que, para la pregunta PI1 sobre el comportamiento humano reportado en la literatura, asociado al tema de ciberseguridad, destacan el factor y el error humano, señalando aspectos como el comportamiento y actitudes del usuario que lo puede volver víctima de ataques (Ovelgönne et al., 2017; Linkov et al., 2019; Hughes-Lartey et al., 2021), la falta de conciencia sobre las implicaciones de no cumplir con los procedimientos de seguridad (Linkov et al., 2019), así como aspectos organizacionales, como el conflicto de prioridades (Trilateral Research, 2022) y la falta de políticas bien establecidas (Li y He, 2022). El desinterés de los usuarios por cumplir con los procedimientos de seguridad puede derivar del grado de conocimiento y creencias cognitivas de los empleados (Onumo et al., 2021), de una falta de claridad de las responsabilidades de cada parte de la organización o de la sensación de incapacidad para contribuir a mejorar la ciberseguridad (Reegård et al., 2019; SecurityBrief Australia, 2022). Algunos elementos demográficos relacionados con el comportamiento de los usuarios en ciberseguridad son el nivel de desarrollo de los países, la educación, la edad y la experiencia (Creese et al. 2021; Szczepaniuk et al., 2022; CYDEF, 2021).

Respecto a la pregunta PI2 sobre los elementos culturales que tienen relación con la adopción de buenas prácticas de ciberseguridad, se encontraron aspectos culturales relacionados con elementos demográficos como la cultura nacional (Hughes-Lartey et al., 2021), el género (Li y He, 2022; Kocksch et al., 2018) y la edad (Van Bavel et al., 2019, como se cita en Li y He, 2022); así como aspectos culturales relacionados con el comportamiento humano, como la percepción de alta complejidad en la ciberseguridad (SecurityBrief Australia, 2022), la generación de temores al respecto (Kaspersky, s.f.) y la inexperiencia (Wang et al., 2021).

Para la pregunta PI3 sobre la forma en que los aspectos culturales afectan en la definición y seguimiento de estrategias de ciberseguridad, se obtuvieron pocos hallazgos directamente ligados con las respuestas a la pregunta anterior. El impacto puede ser negativo o positivo dependiendo de las características del contexto particular, relacionadas con cultura nacional, género, edad, experiencia y comportamiento humano. Una implicación claramente señalada por CYDEF (2021) es la falta de capacidad de las pequeñas y medianas empresas para cubrir los costos derivados de incidentes de ciberseguridad en los que se involucran aspectos culturales.

Finalmente, para la pregunta PI4 sobre estrategias a implementar para mejorar la ciberseguridad, tomando en cuenta aspectos culturales, destaca la necesidad de capacitación y concientización periódica (Greitzer et al., 2021; Frenken, 2020) y se mencionan propuestas de *frameworks* y metodologías que pueden apoyar en este proceso, considerando factores humanos (AlQadheeb et al., 2022; Hughes-Lartey et al.,2021; Hajny et al., 2021).

Conclusiones

Dada la necesidad de integrar un estudio sobre la influencia de los aspectos culturales en el desarrollo de estrategias de ciberseguridad, a partir de los 38 estudios detectados por la MLR, se encontraron hallazgos sobre cuatro aspectos principales: el comportamiento de los usuarios ante la ciberseguridad, los aspectos culturales que influyen en la ciberseguridad, los efectos de los aspectos culturales y del comportamiento humano en la ciberseguridad, así como las estrategias que consideran estos aspectos para mejorar el manejo de la seguridad.

Los resultados del estudio pueden representar un punto de partida para aquellas organizaciones interesadas en mejorar su seguridad cibernética desde una perspectiva humana. Identificando las razones que podrían dar origen a los comportamientos de su personal en materia de ciberseguridad, así como sus implicaciones, para considerarlas en la definición de políticas y procedimientos, alineadas a un marco de referencia que se adapte a su contexto particular.

Un área de oportunidad que se detecta es la actualización del estudio para poder integrar hallazgos posteriores al periodo establecido en los criterios de selección de estudios. Como oportunidades de investigación o de aplicación del conocimiento se plantean: la relación entre los aspectos demográficos y psicológicos involucrados en las decisiones en materia de ciberseguridad, así como la capacitación y formación en ciberseguridad con la finalidad de disminuir el error humano. Por último, es fundamental que usuarios, profesionales de las TIC y tomadores de decisiones tengan presente que la ciberseguridad no solo implica habilidades técnicas, ya que, en la planeación, el diseño y la aplicación de las estrategias correspondientes siempre estará presente el factor humano.

Referencias

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. IEEE Access, 9, 44928–44949. https://doi.org/10.1109/ACCESS.2021.3066383

Ahola, M. (2022, 17 junio). The Role of Human Error in Successful Cyber Security Breaches. usecure Blog. https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

AlQadheeb, A., Bhattacharyya, S., & Perl, S. (2022). Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior. Array, 14, 100146. https://doi.org/10.1016/j.array.2022.100146

Burnap, P. (2021), Risk Management & Governance. The Cyber Security Body of Knowledge version 1.0.1. University of Bristol. [Online]. https://www.cybok.org/

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: A comparative study of nations and regions. Personal and Ubiquitous Computing, 25(5), 941–955. https://doi.org/10.1007/s00779-021-01569-6

CYDEF. (2021, mayo 19). The Human Factor: The Hidden Problem of Cybersecurity. https://cydef.ca/blog/the-human-factor-the-hidden-problem-of-cybersecurity/

ESGinova Group. (29 de enero del 2020). ¿Qué es la cultura de seguridad en las organizaciones?. Recuperado 20 de junio de 2023, de https://www.nueva-iso-45001.com/2020/01/que-es-la-cultura-de-seguridad-en-las-organizaciones/

Florida Tech Online. (1 de mayo del 2023). Creating a Cybersecurity Culture in Your Organization. Online Degrees - Florida Institute of Technology. https://www.floridatechonline.com/blog/information-technology/creating-a-cybersecurity-culture-in-your-organization/

Frenken, P. (2020). Building a Culture of Security. ISACA Journal, Volume 5. Recuperado el 7 de marzo de 2025, de https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security

Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Information and Software Technology, 106, 101–121.

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

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. Heliyon, 3(7), e00346.

Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., & De Nicola, R. (2021). Framework, Tools and Good Practices for Cybersecurity Curricula. IEEE Access, 9, 94723–94747. https://doi.org/10.1109/ACCESS.2021.3093952

Hamilton, J. (2021, 9 abril). El factor humano: el eslabón más débil de la ciberseguridad. GlobalSign. Recuperado 2 de mayo de 2023, de https://www.globalsign.com/es/blog/human-element-cybersecuritys-weakest-link

Hofstede, G. (2002). Culture's consequences: comparing values, behaviors, institutions, and organizations across nations. Academy of Management Review, 27(3), 460.

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon, 7(3), e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

Kaspersky (s/f). The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Kocksch, L., Korn, M., Poller, A., & Wagenknecht, S. (2018). Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 1–20. https://doi.org/10.1145/3274361

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors Related to Cyber Security Behavior. IEEE Access, 8, 125140–125148. https://doi.org/10.1109/ACCESS.2020.3007867

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. Computers in Human Behavior Reports, 5, 100165. https://doi.org/10.1016/j.chbr.2021.100165

Linkov, V., Zámečník, P., Havlíčková, D., & Pai, C.-W. (2019). Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research. Frontiers in Psychology, 10. https://www.frontiersin.org/articles/10.3389/fpsyg.2019.00995

McAlmont (13 de mayo del 2022). Cybersecurity Learning: Building a Culture of Cyber Awareness. Spiceworks Inc. https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/cybersecurity-learning-building-a-culture-of-cyber-awareness/

OnSolve. (2020). Create a Culture that Promotes Cybersecurity Awareness Communication. https://www.onsolve.com/blog/creating-culture-cyber-security-awareness/

Onumo, A., Cullen, A., & Ullah-Awan, I. (2017). An Empirical Study of Cultural Dimensions and Cybersecurity Development. 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), 70–76. https://doi.org/10.1109/FiCloud.2017.41

Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures. ACM Transactions on Management Information Systems, 12(2), 1–29. https://doi.org/10.1145/3424282

Ovelgönne, M., Dumitraş, T., Prakash, B. A., Subrahmanian, V. S., & Wang, B. (2017). Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks: A Data-Driven Approach. ACM Transactions on Intelligent

Systems and Technology, 8(4), 1–25. https://doi.org/10.1145/2890509
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. ResearchGate. https://doi.org/10.13140/2.1.1018.4643.
Reegård, K., Blackett, C., & Katta, V. (2019). The Concept of Cybersecurity Culture. Proceedings of the 29th European Safety and Reliability Conference (ESREL), 4036–4043. https://doi.org/10.3850/978-981-11-2724-3_0761-cd
Santander Open Academy (2022). Cultura organizativa: qué es y por qué es tan importante para las empresas. Recuperado el 23 de junio de 2023, de https://www.becas-santander.com/es/blog/cultura-organizativa.html
Sasse M. A. & Rashid A. (2021). Human Factors. The Cyber Security Body of Knowledge version 1.0.1. University of Bristol. [Online]. https://www.cybok.org/
Sasse, M. A., & Flechais, I. (2005). Why Do We Need It? How Do We Get It? en Cranor & Garfinkel (Ed.), Security and Usability (pp. 12-30). O'Reilly
SecurityBrief Australia. (s/f). It's the culture: The impact of cyber indifference on cybersecurity. Recuperado el 31 de agosto de 2022, de https://securitybrief.com.au/story/it-s-the-culture-the-impact-of-cyber-indifference-on-cybersecurity
Siruela, C. del C. A. (2021, septiembre 20). The human factor: A key element of cyber security. Think Big. https://business.blogthinkbig.com/human-factor-key-element-cybersecurity/
Skinner, B. F. (1953). Science and human behavior. The MacMillan Company.
Szczepaniuk, E. K., & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. Telecommunications Policy, 46(3), 102282. https://doi.org/10.1016/j.telpol.2021.102282
Trilateral Research (8 de febrero del 2022). Analysing the human-factor-based aspects of cybersecurity. https://trilateralresearch.com/cybersecurity/analysing-the-human-factor-based-aspects-of-cybersecurity
Unión Internacional de Telecomunicaciones. (2008, abril). Recomendación UIT-T X.1205. https://www.itu.int/rec/T-REC-X.1205-200804-I/es
Villanueva M. (2022). Definición de Comportamiento. Recuperado 16 de mayo de 2022, de https://significado.com/comportamiento/
VOX Network Solutions. (9 de diciembre del 2019). Cyber Security Awareness and the Human Factor. https://www.voxns.com/cyber-security-awareness-human-factor/
Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. IEEE Access, 8, 8509485115. https://doi.org/10.1109/ACCESS.2020.2992807
Wiederhold, B. K. (2014). The Role of Psychology in Enhancing Cybersecurity. Cyberpsychology, Behavior, and Social Networking, 17(3), 131–132.