EPICENTRO
Ciencia - Tecnología - Innovación

TENDENCIAS ACTUALES Y DESAFÍOS EN EL NIVEL DE CONOCIMIENTO DE CIBERSEGURIDAD EN USUARIOS

Bohen Gisela Solís Tejedor
Universidad Tecnológica Oteima
bohen.solis@oteima.ac.pa
ORCID N° 0000-0002-2159-3584

Michael Enrique Trejos Valdés
Universidad Tecnológica Oteima
michael.trejos@oteima.ac.pa
ORCID N° 0009-0007-3061-901
DOI: 10.61209/re.v2i1.38

RESUMEN.
La ciberseguridad se ha convertido en una preocupación creciente en la sociedad actual, ya que el uso de las tecnologías de la información y la comunicación ha aumentado exponencialmente en los últimos años, por lo tanto, un número cada vez mayor de personas utiliza dichas tecnologías, exponiendo su información personal en línea, por lo que, probablemente desconocen los riesgos que esto implica.. Se diseñó un estudio del tipo revisión narrativa. Metodológicamente se indagaron en las bases de datos EBSCO y el buscador Google Académico, empleando la metodología PRISMA, usando los términos: "nivel de conocimiento en ciberseguridad en usuarios" y "conocimiento en ciberseguridad". De las 47 fuentes inicialmente buscadas, se analizaron 7 documentos (5 artículos originales y 2 trabajos de graduación). Estas publicaciones proporcionan una base sólida para futuras iniciativas que mejoren la seguridad digital a nivel personal y organizacional. Los resultados destacan la importancia de aumentar la conciencia sobre la seguridad en línea y establecer programas educativos para contrarrestar la falta de preparación de los usuarios para enfrentar desafíos de seguridad cibernética. Además, se destaca la falta de conciencia y la falta de medidas de seguridad por parte de los usuarios de medios electrónicos, que son los principales factores que contribuyen al aumento de los delitos informáticos. Las publicaciones seleccionadas revelan disparidades en percepciones y conocimientos, la influencia del entorno social, la paradoja de la seguridad de contraseñas y la importancia de métodos educativos adaptados en relación con el nivel de conocimiento en ciberseguridad para usuarios.

Palabras Clave: Ciberseguridad, nivel de conocimiento, seguridad digital, concienciación, educación en ciberseguridad, ataques cibernéticos.

ABSTRACT.
Cybersecurity has become a growing concern in today's society, since the use of information and communication technologies has increased exponentially in recent years, therefore, an increasing number of people use these technologies, exposing their personal information online, so they are probably unaware of the risks involved. A narrative review type study was designed. Methodologically, the databases Scopus and the Google Scholar search engine were searched, employing the PRISMA methodology, using the terms: "level of knowledge in cybersecurity in users" and "knowledge in cybersecurity". Of the 47 sources initially searched, 7 documents were analyzed (5 original articles and 2 graduate papers). These publications provide a solid foundation for future initiatives to improve digital security at the personal and organizational level. The results highlight the importance of increasing awareness of online security and establishing educational programs to counteract the lack of preparation of users to face cybersecurity challenges. In addition, it highlights the lack of awareness and lack of security measures by users of electronic media, which are the main factors contributing to the increase in cybercrime.The selected publications reveal disparities in perceptions and knowledge, the influence of the social environment, the paradox of password security and the importance of tailored educational methods in relation to the level of cybersecurity knowledge for users.

Key Words: Cybersecurity, knowledge level, digital security, awareness, cybersecurity education, cyber attacks.

Introducción.

En la era digital, donde la interconexión y la dependencia de la tecnología son omnipresentes, la ciberseguridad ha emergido como un pilar fundamental (Astorga-Aguilar & Schmidt-Fonseca, 2019). A medida que la sociedad se vuelve más dependiente de las redes, las amenazas cibernéticas se desarrollan simultáneamente y presentan desafíos cada vez más complejo. (Suárez, 2020),(Galán, 2023) de manera que, los seres humanos están constantemente creando y almacenando información en cantidades astronómicas (Florez et al., 2020).

Según Kettles (2023),a nivel mundial se estima que los ciberataques costarán 8 billones de dólares en 2023. Este costo incluye daños a la infraestructura, pérdida de datos e interrupciones de operaciones, por lo que medir el nivel de conocimientos en ciberseguridad de las personas es un componente crucial para reducir los peligros. La falta de una técnica estandarizada y efectiva para medir el nivel de conocimiento de ciberseguridad en las personas sigue siendo un problema que merece atención inmediata, a pesar de los esfuerzos y avances significativos en investigación y desarrollo de medidas de seguridad informática (Pérez et al., 2023). La identificación y evaluación de los conocimientos necesarios es un desafío único debido a la complejidad inherente de la naturaleza dinámica de las amenazas cibernéticas y la diversidad de los usuarios.

.En la literatura existente destaca el ensayo de Rodríguez (2022) que establece que "las empresas y agencias gubernamentales han estado trabajando arduamente en estrategias para fortalecer las medidas de ciberseguridad, estas no han sido suficientes..." p. 5. Según lo planteado se sugiere que las medidas actuales no han logrado abordar de manera efectiva los desafíos, tendencias y amenazas cibernéticas, a pesar de los esfuerzos dedicados a este fin. Este problema plantea dudas sobre la efectividad de las tácticas actuales y destaca la importancia de determinar las publicaciones relacionadas al nivel de conocimientos en ciberseguridad para usuarios, este artículo se construye sobre los cimientos de investigaciones previas, integrando aspectos encontrados en fuentes primarias y secundarias.

Los hallazgos obtenidos en el artículo titulado Estudio preliminar sobre conocimiento de Ciberseguridad en usuarios de PYMES: Caso estudio de Riobamba, establecen que los usuarios de PYMES deben seguir aprendiendo sobre ciberseguridad y que las investigaciones consultadas para la confección de los antecedentes de este artículo se orientan hacia el cumplimiento de políticas y a la adquisición de equipos, que a la medición del conocimiento en esta área. (Maggi & Gómez, 2021). El objetivo principal del presente artículo es realizar una revisión bibliográfica narrativa sobre publicaciones relacionadas a la medición del nivel de conocimientos sobre ciberseguridad en los usuarios, que permita establecer desafíos y tendencias. Además, se busca crear un marco teórico que pueda evidenciar las tendencias y desafíos en el nivel de conocimiento sobre ciberseguridad en los usuarios de diversas tecnologías, aspectos necesarios en el panorama actual de la ciberseguridad. Este artículo se enfoca en realizar una revisión narrativa de aspectos relacionados al nivel de conocimiento en ciberseguridad desde el punto vista de los usuarios, tomando de referencia algunos componentes de la declaración PRISMA. Para el análisis de las publicaciones se limitó a artículos que se publicaron entre 2018 y 2023.
Además, a través de este artículo de revisión se busca responder a las siguientes interrogantes: ¿Qué revelan las publicaciones académicas actuales sobre el nivel de conocimiento y comprensión de ciberseguridad entre los usuarios comunes? ¿Cuáles son los hallazgos clave y las conclusiones principales de los estudios recientes en el ámbito del nivel de conocimiento en ciberseguridad para usuarios? ¿Cuáles son las tendencias y desafíos en el campo del conocimiento en ciberseguridad para usuarios según la literatura reciente?
Cabe señalar que, a través de este artículo de revisión se indaga sobre publicaciones que permiten comprender, medir los conocimientos y habilidades en ciberseguridad en usuarios, proporcionando una base sólida para futuras iniciativas en la mejora de la seguridad digital a nivel personal y organizativo.

METODOLOGÍA

Para el desarrollo de esta revisión se utilizaron las herramientas detalladas en la Tabla 1.

Tabla 1. *Materiales y recursos utilizados*

Material
Computadora
Bases de datos académicas
Software de procesador de texto, Microsoft Word
Software gestor de referencias bibliográficas, Mendeley
Método de selección PRISMA
Descriptores, palabras claves y operadores booleanos

Además de lo anterior se adaptó los parámetros de PRISMA (Page et al., 2021), como metodología para la selección de la literatura que se utilizó para determinar el estado del arte relacionado al tema principal de la revisión, el Nivel de conocimiento en Ciberseguridad en usuarios. La revisión de la literatura se realizó durante el mes de diciembre de 2023, utilizando para esto las bases de datos académicas: Google Scholar y EBSCO.
Durante el proceso de búsqueda se aplicó el uso de descriptores o palabras claves que combinadas con los operadores booleanos AND, OR y NOT (Tabla 2), permitieron crear una estrategia de búsqueda en las distintas fuentes de información consultadas, además de las opciones de exportación que proporciona las bases de datos empleadas, esto último con la finalidad de poder analizar adecuadamente las publicaciones encontradas.

Tabla 2. *Estrategia de búsqueda*

Cadena de búsqueda utilizada en Google Scholar	Cadena de búsqueda utilizada en EBSCO
{"nivel de conocimiento" +"conciencia" +("ciberseguridad" OR "seguridad informática") +"usuarios" -"Infraestructura" -"corporativo" -"institución"}	“Conocimiento” AND “ciberseguridad” NOT “infraestructura NOT “institución”

En la tabla 3 se aprecia las diferentes bases de datos académicas consultadas, su dirección URL, y la cantidad de artículos obtenidos de cada una. El proceso de búsqueda arrojó un total de 47 artículos, 37 de Google Scholar y 10 de EBSCO.

Tabla 3. *Lista de Bases de datos consultadas*

Nombre	Dirección	Cantidad de artículos encontrados
Google Scholar	https://scholar.google.com/	37
EBSCO	https://www.ebsco.com/es	10

En la tabla 3 se aprecia las diferentes bases de datos académicas consultadas, su dirección URL, y la cantidad de artículos obtenidos de cada una. El proceso de búsqueda arrojó un total de 47 artículos, 37 de Google Scholar y 10 de EBSCO.

Tabla 3. *Lista de Bases de datos consultadas*

Nombre	Dirección	Cantidad de artículos encontrados
Google Scholar	https://scholar.google.com/	37
EBSCO	https://www.ebsco.com/es	10

Además, se establecieron los criterios de inclusión y exclusión a los cuales se someterá la literatura encontrada, con el fin de identificar las publicaciones académicas que contengan información relevante relacionada al tema principal. En la tabla 4 se detallan los criterios aplicados en el proceso de revisión.

Tabla 4. *Criterios de inclusión y exclusión*

Criterios de inclusión	
Criterio	**Criterio de inclusión**
Tema	La literatura debe abordar temas relacionados al nivel de conocimiento de los usuarios en diferentes áreas de la ciberseguridad o seguridad informática.
Longitud	Los documentos deben tener 6 o más páginas.
Fecha de publicación	la literatura debe haber sido publicada entre 2018 – 2023.
Idioma	Los documentos deben estar escritos en español o inglés.
Disponibilidad	Los documentos deben ser de acceso abierto.
Criterios de exclusión	
Artículos duplicados.	
Documentos cuyo contenido completo no sea accesible.	
Literatura que hagan referencia a formación en ciberseguridad, pero no relacionada con el uso de conocimientos, habilidades y competencias.	
Escritos sobre formación y concienciación en ciberseguridad que no están orientados al personal no TI de empresas y organizaciones.	

La figura 2 muestra el diagrama de flujo del proceso de selección de la literatura aplicando los parámetros adaptados de PRISMA.

La figura 2 muestra el diagrama de flujo del proceso de selección de la literatura aplicando los parámetros adaptados de PRISMA.

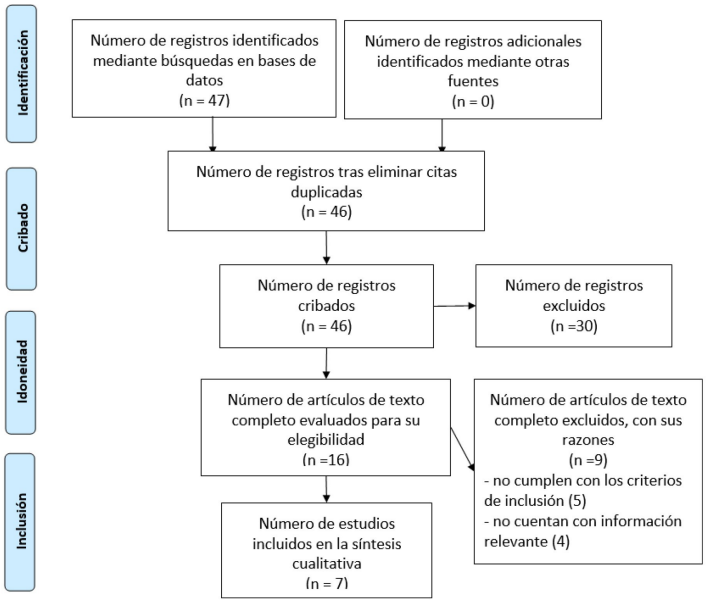

Figura 2. Diagrama de flujo del proceso de selección de la literatura para la revisión aplicando las recomendaciones de PRISMA 2020.

Se inició comparando los registros obtenidos con el objetivo
de eliminar aquellos que estuviesen duplicados. De los 47 registros encontrados, se descartó 1, quedando un total de 46 registros para la revisión. Seguidamente se revisó el título, objetivos, resumen, hallazgos y conclusiones de los documentos restantes. De estos, 30 fueron excluidos debido que no contenían información relacionada al tema.

Posteriormente se procedió a realizar la revisión de los 16 artículos aplicando los criterios de inclusión y exclusión
establecidos previamente. Quedando un total de 7 documentos,
los cuales se utilizaron para el desarrollo del articulo propuesto.

RESULTADOS Y DISCUSIÓN

Un resumen de los artículos seleccionados se presenta en la tabla 5. Los artículos seleccionados fueron publicados
en el período comprendido entre el 2018 y 2023.

Posteriormente se procedió a realizar la revisión de los 16 artículos aplicando los criterios de inclusión y exclusión
establecidos previamente. Quedando un total de 7 documentos,
los cuales se utilizaron para el desarrollo del articulo propuesto.

RESULTADOS Y DISCUSIÓN

Un resumen de los artículos seleccionados se presenta en la tabla 5. Los artículos seleccionados fueron publicados
en el período comprendido entre el 2018 y 2023.

Tabla 5

Hallazgos principales de las publicaciones seleccionadas

Autores y Titulo	Objetivo	Métodos	Principales Resultados
Hábitos y percepciones sobre Seguridad Informática en estudiantes universitarios pertenecientes a las generaciones Y,Z: Un estudio comparativo de dos universidades públicas en México.(López et al., 2022) México/español	Determinar cuáles son las similitudes y diferencias respecto a los hábitos y percepciones de seguridad informática de los estudiantes universitarios pertenecientes a las generaciones Y, Z.	Se aplicó un instrumento con 18 item, que fue revisado por expertos. Este fue respondido por un total de 124 estudiantes universitarios elegidos al azar, 62 de cada universidad. También se utilizó un paquete estadístico denominado Jamovi y luego se realizó la prueba de normalidad de Shapiro-Wilk. Finalmente se aplicó la prueba Shreirer _ Ray- Hare que es una alternativa a la ANOVA de dos vías.	Se concluye que los estudiantes de mayor edad (Generación Y) mencionan tener un conocimiento superior que los estudiantes de la Generación Z, pero de igual forma se detectaron debilidades que dan oportunidad para una formación más sólida de estos estudiantes, quienes en el corto plazo estarán en el mercado laboral, y sus decisiones y acciones pueden afectar el desarrollo de la empresa.
Comportamiento de los usuarios sobre los delitos informáticos en la Ciudad del Puyo. Limitaciones actuales en la legislación y normas. (Velastegui & Velastegui, 2023) Ecuador/español	Evaluar las actitudes y comportamientos de los usuarios en relación con la seguridad y Confiabilidad en la realización de Transacciones por medios electrónicos, así como analizar las limitaciones actuales en la legislación y normas que regulan estos delitos en el país	Los métodos empleados en esta investigación corresponden a la modalidad "cuali-cuantitativa", se desarrollaron procesos de búsqueda selectiva de información en libros, artículos y otros; para fundamentar el objeto de estudios de la presente investigación. También se aplicó un cuestionario en línea con 15 preguntas relacionadas a la temática, aplicadas a los distintos actores con una muestra representativa.	Los hallazgos sugieren que un número preocupante de personas han sido víctimas de fraudes y estafas electrónicas, lo que destaca la necesidad de tomar medidas para prevenir estos delitos. El estudio muestra la importancia de la educación y la sensibilización de los usuarios de medios electrónicos para prevenir y combatir estos delitos.
Percepción de riesgo online en jóvenes y su efecto en el comportamiento digital. (Ramos et al., 2018) Madrid/inglés	a) Analizar las diferentes tipologías de usuarios menores de edad derivadas de la percepción de riesgo; b) Describir el comportamiento online de los menores y la mediación familiar en cada tipología.	El universo objeto de estudio son los menores escolarizados en la Comunidad de Madrid. Se ha utilizado un cuestionario personal estructurado ad hoc como instrumento de recogida de información. El muestreo es polietápico y estratificado por conglomerados según los niveles de enseñanza y la tipología del centro educativo privado/concertado o público. Una muestra de 865 menores de 10 a 17 años.	Los menores con mayor percepción de riesgo en Internet tienen una mayor capacidad para protegerse de los peligros online, y al mismo tiempo son los que recibieron una mejor educación de sus padres, y también tienen unas prácticas en Internet más saludables. Estos datos refutan la hipótesis que afirma que los menores tienen una baja percepción del riesgo, tanto desde el punto de vista de la confianza en sí mismos para afrontar los peligros asociados a las TIC, como desde la capacidad para afrontar situaciones problemáticas.
Intervención didáctica para minimizar la ciber victimización de adolescentes. (Haz et al., 2022) Ecuador/español	Describir las características y las consecuencias de las diferentes formas de victimización en entornos virtuales, tales como grooming, sexting y ciberbullying	Se trata de describir las características y consecuencias de diferentes formas victimización en entornos virtuales, tales como grooming, sexting y ciberbullying. Esta investigación se realizó utilizando un enfoque cualitativo, diseño documental.	Hay una variedad de riesgos a los que están expuestos los niños y jóvenes en línea, una situación que se ha vuelto cada vez más clara en los últimos años. Sin embargo, este grupo de población confía en que sus conocimientos y experiencia en el uso de las TIC les permitirán afrontar cualquier situación en la web. Los niños y adolescentes creen que pueden publicar cualquier fotografía online sin que suponga ningún riesgo. El uso de TIC debe estar fundamentado en el conocimiento adecuado de los riesgos, implementar mecanismos y herramientas de seguridad informática.
Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. (Mendivil et al., 2022) España/Español	Explorar el uso de modelos de competencias en la elaboración de programas de formación y concienciación en ciberseguridad dirigidos al personal no técnico de las organizaciones.	Se realizó una revisión sistemática de la literatura (RSL), propuesta por Kitchenham. La búsqueda se realizó en IEEE Xplore, ACM Digital Library y SCOPUS.	Existe un elevado número de artículos y estudios que abordan de maneras muy diversas la formación y concienciación en ciberseguridad desde un punto de vista competencial, lo que demuestra el interés que suscita la materia. Los estudios relacionados de manera específica con la identificación y creación de modelos de competencias para trabajadores no TIC es significativamente bajo.
Nivel de Conocimiento que tienen estudiantes de Pregrado de Lima sobre mecanismos para el robo de información digital. (Leyva, 2018) Perú/español	Identificar el nivel de conocimiento que tienen los estudiantes de pregrado de una universidad privada de Lima sobre mecanismos tecnológicos que se usan de forma malintencionada para el robo de información	Investigación cuantitativa de diseño no experimental, se identificó la variable de nivel de conocimiento, Consideró una puntuación para una prueba, si el participante obtenía mayor o igual a 11 era considerado como aprobado sino desaprobado, y la muestra fue de 376 estudiantes universitario. El instrumento contenía 20 preguntas. La prueba fue revisada por un comité de expertos.	El nivel de conocimiento teórico que tienenlos estudiantes de pregrado de una universidad privada de Lima, sobre mecanismos tecnológicos que se usan de forma malintencionada para el robo de información, es en promedio mayor o igual a 11 puntos.
La falta de prevención de las personas cibernautas en los delitos informáticos.(Chacón, 2018) Costa Rica/español	Demostrar que la incidencia de delitos informáticos en Costa Rica, no se debe a una regulación insuficiente, sino a la falta de prevención de los cibernautas	Investigación cualitativa, se entrevistó a 15 personas. Se hicieron 12 preguntas con relación a delitos informáticos y la existencia de una ley en Costa Rica. Además, se realizó un análisis a las leyes en las que se incorpora distintos delitos informáticos.	La Internet ha venido a promover un cambio total en la forma de vida de las personas, debido a los beneficios que proporciona, no obstante, se debe de tener mucha precaución y procurar una navegación segura, al evitar realizar acciones que faciliten ser víctimas de la ciberdelincuencia

A continuación, se muestra un breve resumen de cada artículo, destacando los puntos claves que contribuyen a esta investigación:
Los principales hallazgos del estudio sobre los hábitos y percepciones de seguridad informática en estudiantes universitarios de López et al. (2022) incluyen: Diferencias significativas en la autopercepción de conocimientos sobre informática y seguridad informática entre estudiantes pertenecientes a las generaciones Y y Z, mayor vulnerabilidad de los estudiantes de la Universidad Autónoma de Tamaulipas en cuanto al robo de identidad en comparación con los alumnos de la Universidad de Guadalajara, mayor riesgo de los estudiantes de la Universidad de Guadalajara en cuanto a compartir contraseñas, a pesar de reportar cambios en sus contraseñas con mayor frecuencia en comparación con los estudiantes de la Universidad Autónoma de Tamaulipas y la necesidad de incluir contenidos prácticos sobre ciberseguridad en los programas educativos para dotar a los estudiantes de las habilidades necesarias para enfrentar los desafíos del mercado laboral real .
Por otro lado, en la investigación de Velastegui & Velastegui (2023) destaca la falta de conciencia y medidas de seguridad por parte de los usuarios de medios electrónicos, principales causas del aumento de los delitos informáticos, además de que la mayoría de los encuestados tiene conocimientos sobre delitos informáticos, y un porcentaje significativo ha sido víctima de estafas o fraudes por medios electrónicos. En esta investigación se observó un bajo nivel de conocimiento y falta de medidas de protección por parte de los encuestados, lo que evidencia la necesidad de implementar medidas para prevenir estos delitos.
En la investigación titulada Percepción de riesgo online en jóvenes y su efecto en el comportamiento digital de Ramos et al. (2018), se encontró que la alta penetración del teléfono móvil intensifica las actividades online de los jóvenes, lo que les lleva a tomar decisiones no planificadas en su día a día en función de la información que reciben a través del teléfono, también que los menores con mayor percepción de riesgo en la red tienen mayores habilidades para protegerse frente a los peligros online y son, al mismo tiempo, los que cuentan con una mayor intervención educativa de los padres y tienen prácticas más saludables. Otro aspecto importante para señalar es que un porcentaje significativo de menores muestra escasa percepción de riesgo, lo que se relaciona con la falta de percepción de los padres y profesores como fuentes de autoridad, así como una percepción negativa de la ayuda que puedan brindarles.
Otro trabajo seleccionado concluye que se pueden utilizar diversos enfoques para abordar la sobreexposición de información personal de menores en Internet y las redes sociales, que puede conllevar riesgos para su intimidad, integridad, autoimagen y desarrollo de la personalidad. Las investigaciones seleccionadas para la confección del artículo indican que la ciber victimización está relacionada con factores como el estrés, la depresión, el comportamiento suicida, la baja autoestima, las dificultades académicas y los problemas en el entorno escolar. (Haz et al., 2022).
En el artículo de revisión de Mendivil et al (2022) concluyó que las actividades de formación y sensibilización en ciberseguridad, basadas en el desarrollo de competencias, son elementos cruciales que deben profundizarse, actualizarse y mejorarse constantemente. Para este autor, existe un elevado número de artículos y estudios que proporcionan información relevante en este campo.
El trabajo de graduación de Leyva (2018), muestra resultados interesantes sobre el nivel de conocimiento que tienen los estudiantes de pregrado de una universidad privada en Lima sobre mecanismos para el robo de información digital. En el documento de trabajo de graduación, el autor descubrió que es necesario aumentar la conciencia y la educación sobre la importancia de la seguridad digital para disminuir los casos de robo de identidad. Además, el estudio muestra las preocupaciones de los usuarios con respecto a la protección y seguridad de su información personal.
Finalmente, en el trabajo titulado La falta de prevención de las personas cibernautas en los delitos informáticos(Chacón, 2018), el autor menciona que los usuarios deben tomar las siguientes medidas: Implementación y participación de programas educativos, que permitan crear conciencia sobre el uso seguro de Internet, las comunicaciones y la seguridad cibernética, además recomienda que el Estado lleve a cabo campañas educativas para adultos en el que enseñen cómo protegerse y prevenir los delitos informáticos, por último se enfatiza sobre la importancia de educar a la sociedad costarricense sobre la forma de cómo proteger sus datos personales, tanto en línea como en persona, para evitar que se revelen información personal de manera imprudente.
Las publicaciones académicas actuales seleccionadas sobre el nivel de conocimiento de ciberseguridad entre los usuarios comunes revelan lo siguiente:

- Existencia de disparidad en las percepciones y conocimientos sobre seguridad informática entre diferentes grupos de usuarios, como las generaciones Y y Z.
- El impacto de factores sociales como la institución académica en la percepción de la seguridad informática, es decir, de acuerdo con el entorno en el que se desenvuelve el individuo repercute en la percepción de seguridad informática.
- La paradoja de la seguridad de contraseñas, que al realizar cambios periódicos se recurre a derivados de una misma contraseña., que acaban facilitando enormemente a los ciberdelincuentes la tarea de adivinarlas, así como otras prácticas inadecuadas.
- El valor de implementar métodos educativos adaptados a cada grupo de usuarios para abordar los problemas de seguridad en línea.

CONCLUSIONES

Las publicaciones seleccionadas resaltan la necesidad de adaptar estrategias educativas sobre seguridad informática y ciberseguridad dependiendo de las generaciones, cuyas percepciones difieren significativamente en cuanto a conocimientos y prácticas en línea. Los hallazgos subrayan la influencia de factores contextuales en la seguridad informática, evidenciando disparidades en la propensión al robo de identidad y el compartir contraseñas, lo que sugiere considerar el entorno social y cultural del individuo.
La complejidad de las interacciones entre la tecnología y el comportamiento se pone de manifiesto, lo que subraya la importancia de comprender cómo las tecnologías afectan las decisiones diarias de los usuarios, especialmente en lo que respecta a la percepción de riesgo en línea y las prácticas saludables.
Con relación a los desafíos que presentan las publicaciones seleccionadas destaca:

- Necesidad de aumentar la conciencia de seguridad en línea y la implementación de programas educativos para contrarrestar la falta de preparación de los usuarios, para enfrentar desafíos de seguridad cibernética, lo que resalta la consideración de la formación y sensibilización en ciberseguridad.
- Tomar acciones rápidas y constantes para mejorar la capacidad de la sociedad para resistir a los delitos informáticos.
- Que acciones rutinarias que realiza un adolescente o joven en las redes sociales o en la web no se considere un riesgo para él.
- El nivel de conocimiento en ciberseguridad inadecuado de un usuario repercute en las decisiones y acciones, afectando el desarrollo de la empresa para la que estos laboren en un futuro a corto plazo.

En resumen, los artículos seleccionados brindan a los lectores una comprensión completa y matizada de la ciberseguridad en usuarios, ya que hacen énfasis en la importancia de enfoques educativos integrales, el contexto y la comprensión de cómo la tecnología afecta el comportamiento humano.
Los hallazgos resaltan la importancia de crear estrategias efectivas para enfrentar los desafíos en constante cambio en el mundo digital. En base a lo anterior, las publicaciones seleccionadas permiten revelar las tendencias y desafíos relacionados con el nivel de conocimiento en ciberseguridad para usuarios.

REFERENCIAS BIBLIOGRÁFICAS

Astorga-Aguilar, C., & Schmidt-Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. Revista Electronica Educare, 23(3), 1-24. https://doi.org/10.15359/ree.23-3.17
Chacón, A. (2018). La falta de prevención de las personas cibernautas en los delitos informáticos. Universidad Latina de Costa Rica.
Florez Martinez, J., Mario, J., & Mosquera, R. (2020). Conocer el valor de la información(activo económico) para valorar la necesidad de la ciberseguridad. www.springeropen.com
Galán, C. (2023). Ciberseguridad en el ámbito sanitario. Universidad Politécnica de Catalunya.

Haz, L., Dávila, A., Domínguez, M., & Campuzano, M. G. (2022). Intervención didáctica para minimizar la ciber victimización de adolescentes. Pro Sciences: Revista De Producción, Ciencias e Investigación, 6(45), 119-135. https://doi.org/10.29018/issn.2588-1000vol6iss45
Kettles, M. (2023). Tendencias en ciberseguridad 2023. https://www.amcsgroup.com/es/blogs/tendencias-en-ciberseguridad-2023/.

Leyva, Y. (2018). Nivel de Conocimiento que tienen estudiantes de Pregrado de Lima sobre mecanismos para el robo de información digital. Universidad de San Ignacio de Loyola.
López, A., Roque, R., Prieto, M. T., & Salazar, R. (2022). Hábitos y percepciones sobre Seguridad Informática en estudiantes universitarios pertenecientes a las generaciones Y,Z: Un estudio comparativo de dos universidades públicas en México. Dilemas Contemporáneos: Educación, Política y Valores, 9(3), 1-19.
Maggi, G., & Gómez, O. (2021). Estudio preliminar sobre conocimiento de Ciberseguridad en usuarios de PYMES: Caso estudio de Riobamba. Perspectivas, 3(2), 46-53.
Mendivil, J., Sanz, B., & Gutiérrez, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. Pixel-Bit, 63, 197-225. https://revistapixelbit.com
Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw,
J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. En The BMJ (Vol. 372). BMJ Publishing Group. https://-doi.org/10.1136/bmj.n71
Pérez Perilla, D., Sánchez Villarreal, M., Clareth Tolods, I., & Nova Rodríguez, V. (2023). Análisis de la Percepción del cliente en la Seguridad implementada a los Servicios de la Banca Digital en Colombia: Una revisión sistemática. Fundación Universitaria del Área Andina, 1-28.
Ramos-Soler, I., López-Sánchez, C., & Torrecillas-Lacave, T. (2018). Percepción de riesgo online en jóvenes y su efecto en el comportamiento digital. Comunicar, 26(56), 71-79. https://doi.org/10.3916/C56-2018-07
Rodríguez, J. (2022). Análisis de la Ciberdefensa y Ciberseguridad en la Seguridad Ciudadana en Bogotá. Universidad Militar de Nueva Granada.
Suárez, L. (2020). Importancia de la Seguridad Informática y Ciberseguridad en el mundo actual. Seguridad Informática y Ciberseguridad, 1-11.
Velastegui, M. E., & Velastegui, M. A. (2023). Comportamiento de los usuarios sobre los delitos informáticos en la Ciudad del Puyo. Limitaciones actuales en la legislación y normas. Universidad y Sociedad, 15(52), 344-354.