Preservado en Zenodo: DOI: https://doi.org/10.5281/zenodo.12572001 Los autores son los responsables de las informaciones de este artículo

La seguridad, competencia digital esencial de los usuarios que ingresan a la red

Claudia Esmeralda Villela Cervantes[1]*: https://orcid.org/0000-0002-8577-4376
Barbara Rubí Velásquez Monroy[1]: https://orcid.org/0000-0002-2649-9730

[1]Universidad de San Carlos de Guatemala

*Autor para correspondencia: villelaclaudiaesmeralda@gmail.com

Recibido: 15/03/2024 *Aceptado: 15/06/2024* *Publicado: 27/06/2024*

Resumen. Introducción: En la era digital, el acceso a la red es fundamental en la vida diaria de millones de personas, pero conlleva riesgos significativos para la privacidad y la seguridad. **Objetivo**: Explorar la importancia crítica de la seguridad como una competencia digital esencial para los usuarios en línea. **Metodología:** Se realizó una revisión de literatura y un estudio descriptivo con 163 profesionales asistentes a un congreso realizado en julio de 2023 en el Colegio de Humanidades de Guatemala. **Resultados**: El 80.4% de los docentes se han sentido vulnerables al navegar en la red y un 19.6% no. **Conclusión:** La seguridad en línea es crucial para proteger la información personal y crear un entorno digital confiable. Con la digitalización creciente, entender y practicar la seguridad en línea es esencial. La competencia digital y el uso seguro de herramientas tecnológicas son fundamentales para una sociedad más segura.
Palabras clave: seguridad, red, competencia digital, ciberseguridad

Security, the essential digital competence of users who enter the network

Abstract. Introducción: In the digital age, network access is fundamental in the daily lives of millions of people, but it entails significant risks to privacy and security. **Objective:** To explore the critical importance of security as an essential digital competence for online users. **Methodology:** A literature review and a descriptive study were conducted with 163 professionals attending a conference held in July 2023 at the College of Humanities in Guatemala. **Results:** 80.4% of teachers have felt vulnerable while browsing the web, and 19.6% have not. **Conclusion:** Online security is crucial to protecting personal information and creating a trustworthy digital environment. With increasing digitalization, understanding and practicing online security is essential. Digital competence and the safe use of technological tools are fundamental for a safer society.

Keywords: security, web,digital competence, cybersecurity

Publicações científicas sobre educação a distância e suas características

Resumo. Introdução: Na era digital, o acesso à rede é fundamental na vida diária de milhões de pessoas, mas traz riscos significativos para a privacidade e a segurança. **Objetivo:** Explorar a importância crítica da segurança como uma competência digital essencial para os usuários online. **Metodología:** Foi realizada uma revisão de literatura e um estudo descritivo com 163 profissionais participantes de um congresso realizado em julho de 2023 no Colégio de Humanidades da Guatemala. **Resultados:** 80,4% dos docentes sentiram-se vulneráveis ao navegar na rede e 19,6% não. **Conclusão:** A segurança online é crucial para proteger a informação pessoal e criar um ambiente digital confiável. Com a crescente digitalização, entender e praticar a segurança online é essencial. A competência digital e o uso seguro de ferramentas tecnológicas são fundamentais para uma sociedade mais segura.

Palavras-chave: segurança, web, competência digital, cibersegurança

Introducción

La seguridad en línea abarca una serie de prácticas y medidas destinadas a proteger la información personal y los datos sensibles de los usuarios. Estas prácticas van desde el uso de contraseñas fuertes y la autenticación de dos factores hasta la actualización regular de software y la identificación de estafas en línea. Una competencia sólida en seguridad en línea no solo implica la adopción de estas prácticas, sino también la comprensión de los riesgos asociados con el phishing, el malware y la pérdida de privacidad.

Dentro del contexto actual, la seguridad protege a los usuarios contra amenazas cibernéticas, mientras que la competencia digital permite utilizar la tecnología de manera efectiva y responsable. Ambos aspectos son cruciales en la sociedad del siglo XXI, donde gran parte se desarrolla en línea.

Por consiguiente, los usuarios que ingresan a la red sin una comprensión adecuada de la seguridad en línea están expuestos a una serie de amenazas potenciales, desde la pérdida de datos personales y financieros hasta la exposición a fraudes y ataques cibernéticos, los riesgos son variados y reales. Sin embargo, cuando los usuarios adquieren habilidades de seguridad en línea, pueden tomar medidas proactivas para protegerse a sí mismos y a sus datos. Las amenazas comunes en ciberseguridad que pueden afectar la vida son: la ignorancia, ingenuidad y ser excesivamente confiados o descuidados, malware, cuentas hackeadas por phishing, spam o correo no deseado, hogares inseguros con redes inalámbricas, datos perdidos, ataques por Wi Fi, entre otros, como lo expresan (Contreras, 2023; González Fung, 2017; Molina, 2013; Vallejo, 2015, Universidad Veracruzana, s.f).

La seguridad en línea también tiene un impacto más amplio en el ecosistema digital. Cuando los usuarios practican una navegación segura y evitan la propagación de información falsa, contribuyen a la construcción de una comunidad digital más confiable y saludable. Es un componente clave para la construcción de la confianza en la red, lo que a su vez fomenta la participación activa y productiva en línea. Aunado a ello, la competencia digital se refiere a la capacidad para el uso y comprensión tanto de habilidades técnicas, alfabetización digital a través de la utilización de evaluación en línea, identificar uso de fuentes confiables, comunicación y creatividad digital por medio de las TIC siendo flexibles y conscientes de la constante evolución tecnológica a la cual el profesional se debe adaptar.

Metodología

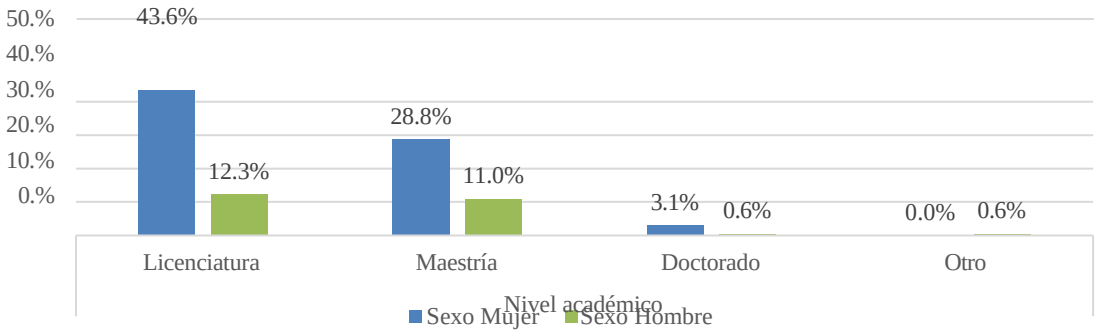
Para esta investigación, se realizó un estudio descriptivo permitiendo así proporcionar una descripción detallada y precisa del fenómeno estudiado; además, la temporalidad se cataloga como transversal, puesto que la recopilación de datos se realizó en un solo momento; también, el enfoque utilizado es el mixto contando así con datos cualitativos y cuantitativos para una mayor comprensión e interpretación de resultados. Aunado a ello, se utilizó el método deductivo partiendo de lo general a lo específico con una población de 163 profesionales que asistieron al congreso realizado en el mes de julio 2023 en el Colegio de Humanidades de Guatemala

Resultados

Para el proceso de información se utilizó la estadística descriptiva, permitiendo analizar los datos procesados por medio de Excel y SPSS versión 29 para la vinculación de datos demográficos y de la variable ciberseguridad de los usuarios que ingresan a la red. Para el proceso de investigación se consideraron a participantes de un congreso pedagógico con niveles de pregrado en adelante en julio del año 2023. A continuación, se presenta en la figura 1, la distribución de sujetos de estudio según nivel académico y sexo.

Figura 1

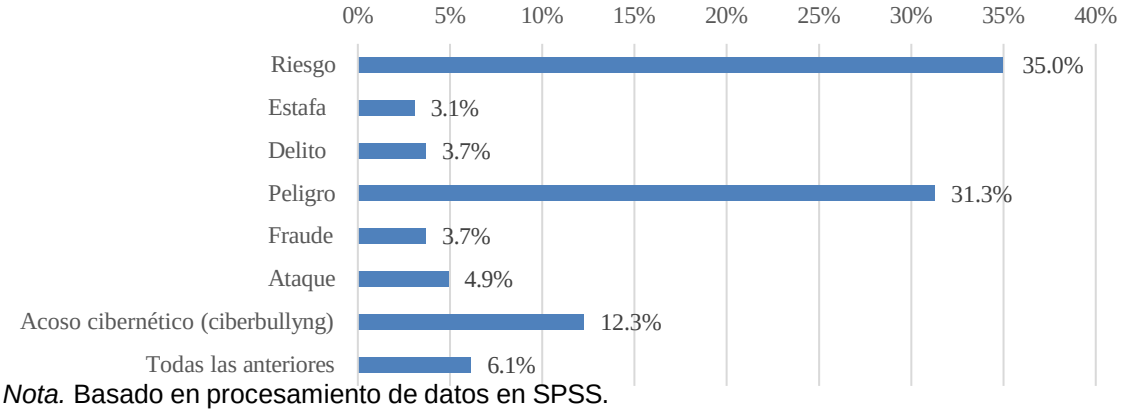
Distribución de docentes sujetos de estudio según ciclo que cursan y promedio general



Nota. Basado en procesamiento de datos en SPSS.

En la figura 1, los docentes sujetos de estudio destacan con 43.6% con un nivel de licenciatura siendo la mayor parte mujeres, el 12.3% del mismo nivel siendo hombres; seguidamente el 28.8% poseen maestría, destacando la preparación de los docentes en área en que se desenvuelven, así mismo, más del 50% es comprendida en la generación X, el cual es caracterizado por ser más selectivos en el uso de medios sociales y experiencia mixta en la tecnología y conciencia de la privacidad en red. A continuación, en la figura 2 se analiza la percepción de los docentes acerca de la seguridad en red.

Figura 2
Percepción de la expresión seguridad en la red

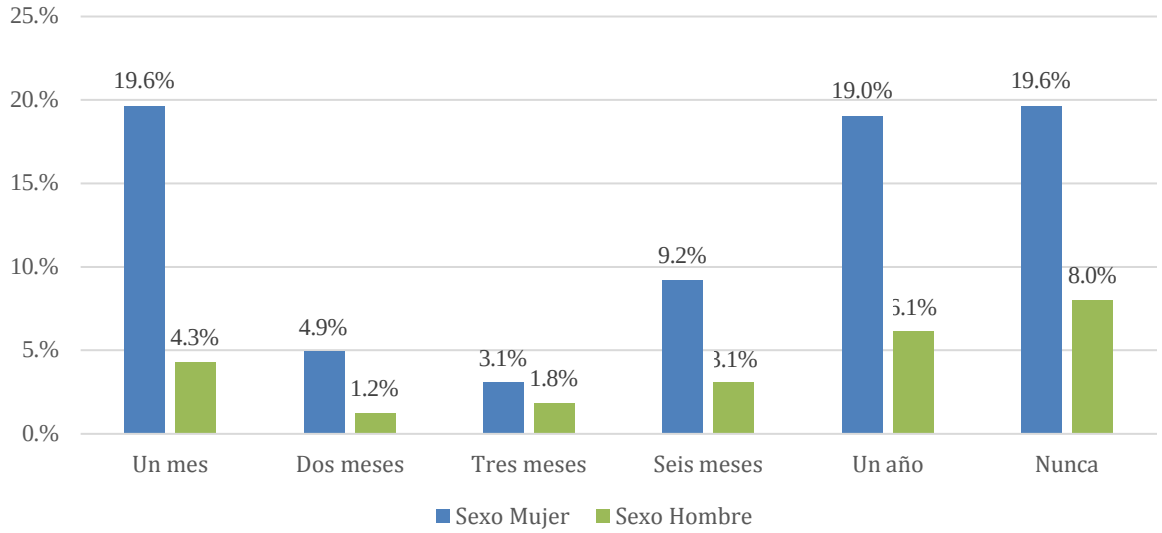


Nota. Basado en procesamiento de datos en SPSS.

En la figura anterior, presenta que los docentes perciben el término como un 35% como un riesgo a través de la percepción de seguridad en red puede variar según su nivel de experiencia que posean con la tecnología; en segundo lugar, con un 31.3% se percibe como peligro y acoso cibernético (ciberbullying) con un 12.3% esto implica, que su rol como profesionales tiene que ser preventivo y consciente de la importancia de la digitalización. En la figura 3, se presenta la última vez que los docentes objeto de estudio cambian sus contraseñas.

Figura 3

Última vez que cambio contraseña al correo electrónico

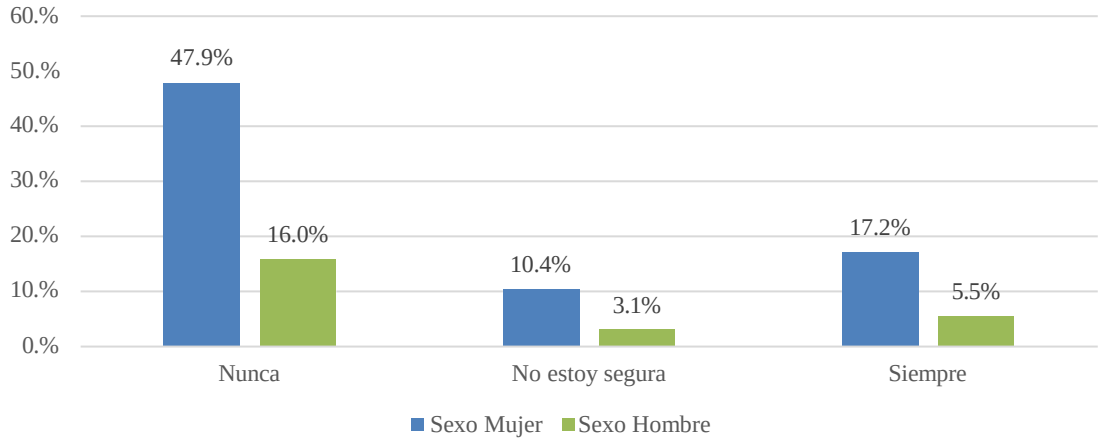


Nota. Basado en procesamiento de datos en SPSS.

Como se muestra en la figura anterior, la última vez que cambiaron la contraseña de su correo las docentes oscila entre un 19.6% que es cada mes, un 19.6% nunca y un 19% cada año; mientras que el profesor con un 8% no cambia su contraseña, con un 6.1% cada año y con un 4.3% cada mes; es necesario destacar que la conciencia de cambios de contraseñas y prácticas de seguridad en línea depende de la educación digital de la persona y no se estereotipa por géneros; pero, en este estudio al ser más del 54% los docentes de la generación X destaca en la coincidencia que son los que nunca cambian su contraseña por medio a ser olvidadas. A raíz de esto, en la figura 4 se presentan los docentes que han sido víctimas de hackeo de al menos una cuenta.

Figura 4

Docentes víctima de hackeo de una cuenta

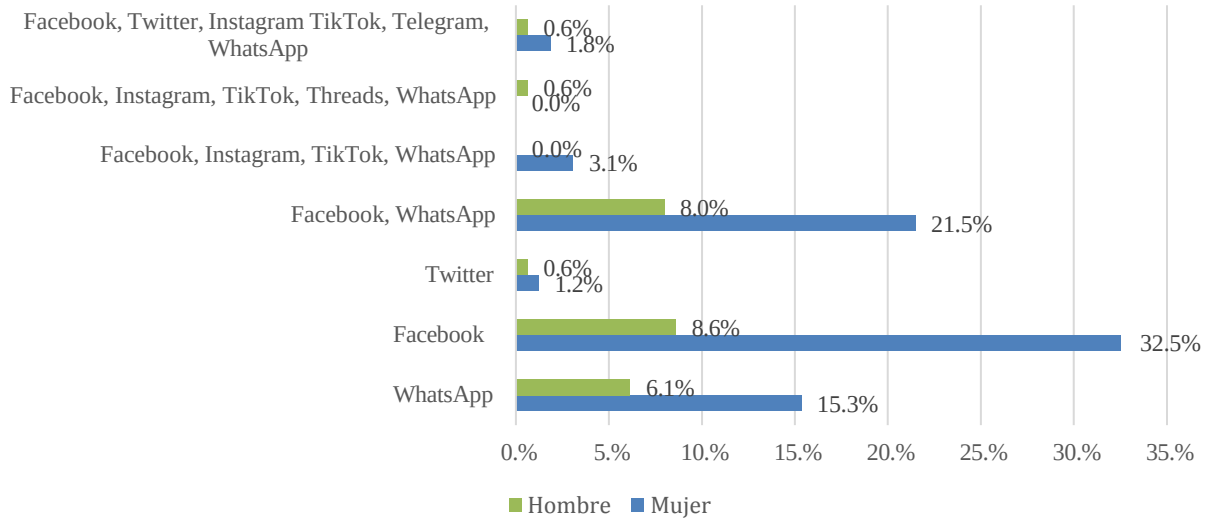


Nota. Basado en procesamiento de datos en SPSS.

En la figura 4, con un 47.9% las docentes nunca han sido víctimas de hackeo, en segundo lugar, con un 16% los profesores no lo han experimentado; sin embargo, el 17.2% de las mujeres y el 5.5% de los hombres si lo han sufrido, como consecuencia de un mal uso de sus cuentas al utilizar contraseñas muy sencillas y de muy alto riesgo, es necesario enfatizar que los docentes que han sufrido este flagelo son desde la generación X y los millennials, por lo que, todo depende de que tan educados están digitalmente y ser conscientes de las amenazas en línea buscando siempre conexiones seguras para dicho acceso. A continuación de la figura 5, se visualiza la frecuencia de uso de las redes sociales.

Figura 5

Redes sociales utilizadas con frecuencia

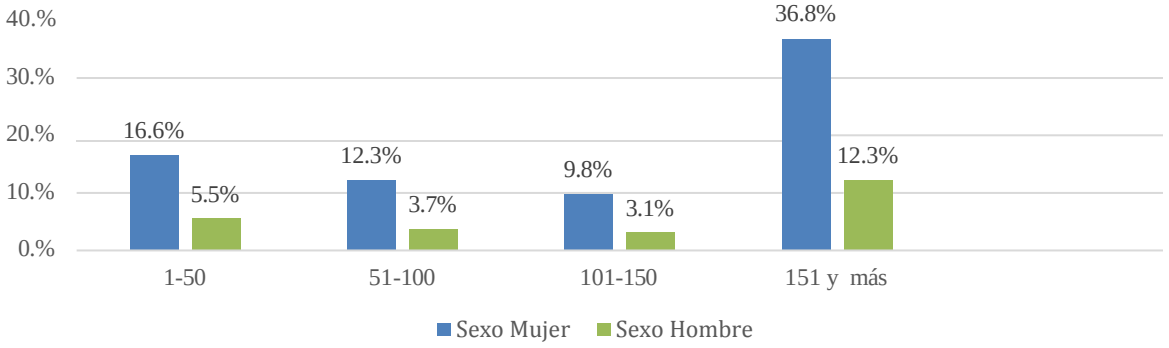


Nota. Basado en procesamiento de datos en SPSS.

En la figura anterior se visualiza que las redes más utilizadas por los docentes es el Facebook con un 32.5% tanto para mujeres y un 8.6% lo utilizan los hombres; en segundo lugar, los docentes utilizan tanto Facebook como WhatsApp representado por el 21.5% para mujeres y un 8% de hombres; estos datos son representativos, puesto, que la tendencia generacional X es utilizar este tipo de redes sociales. En este sentido en la figura 6 se presentan los seguidores que poseen en redes sociales.

Figura 6

Amigos o seguidores en redes

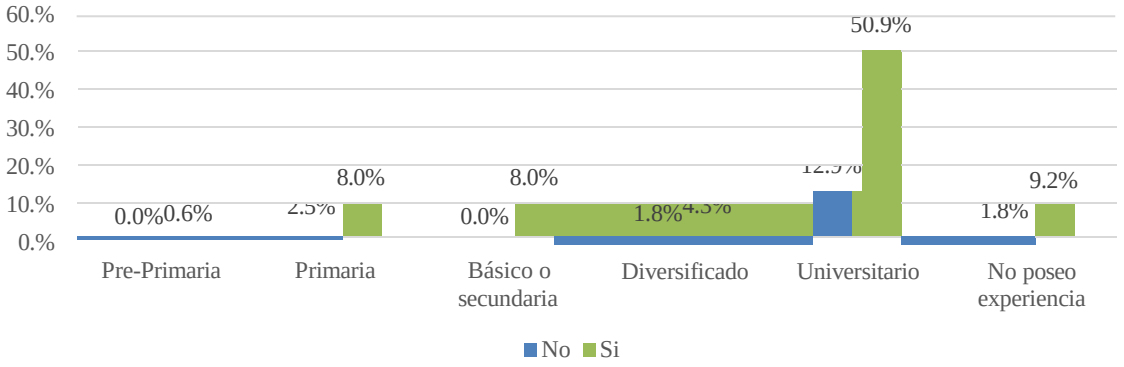


Nota. Basado en procesamiento de datos en SPSS.

La figura 6, presenta que las mujeres con un 36.8% tienen más de 151 amigos así como los hombres con un 12.3%, estos datos reflejan que los profesionales independientemente de su edad al trabajar alrededor con 67% en el sector universitario, se rodean con personas que cuentan con la mayoría de edad y estas lo siguen en sus redes sociales; en segundo lugar, con un 16.6% las mujeres objeto de estudio tienen alrededor de 1 a 50 amigos en redes al igual que los hombres con un 5.5%, estos datos evidencian que por pertenecer a la generación X son más reservados en sus redes sociales. A continuación, en la figura 7, se muestra la participación en la comunidad virtual de aprendizaje.

Figura 7

Participación en una comunidad virtual de aprendizaje (como organizador o participante) según el área que atiende como pedagogo.

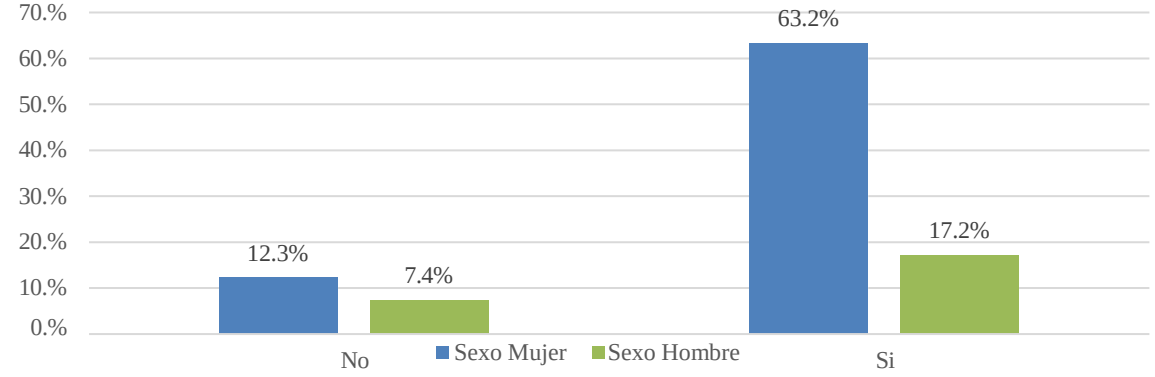


Nota. Basado en procesamiento de datos en SPSS.

En la figura 7, se visualiza que el 50.9% del área que atiende es en el área universitaria, esto es entendible puesto que las actualizaciones tecnológicas están en constante cambio y para estar a la altura de las competencias tecnológicas es necesario actualizarse con cursos masivos en línea y grupos del área en que se es a fin, con el objetivo de propiciar y compartir conocimiento. En segundo lugar, 9.2% que a pesar que no posee experiencia en el campo laboral de la docencia, está en grupos virtuales de aprendizaje por temas específicos de su interés personal. A continuación, en la figura 8 se visualiza la percepción de la vulnerabilidad al navegar la red.

Figura 8

Percibe vulnerabilización al navegar en la red



Nota. Basado en procesamiento de datos en SPSS.

En la figura anterior se visualiza que el 63.2%. de las mujeres perciben vulnerabilización al navegar en la red al igual que los hombres con un 17.2% esto implica que el profesional utiliza contraseñas débiles, utiliza puertos abiertos al utilizar internet gratuito y no está protegido; así como, virus y todo tipo de malware al ingresar páginas sin conexión segura, los constantes correos falsos disfrazándose de bancos u otra institución queriendo estafar a los usuarios y obtener información confidencial. De seguir presentándose esta situación puede ser contraproducente para el profesional, por lo que debe ser cuidadoso y utilizar páginas seguras para su navegación.

Discusión

En un mundo cada vez más interconectado, la seguridad en línea se ha convertido en una competencia digital esencial para todos los usuarios en la red. Comprender y aplicar prácticas seguras en línea, no solo protege la información personal y los datos sensibles, sino que también contribuye a la creación de un entorno digital más seguro y confiable. Aquellos que dominan esta competencia no solo se protegen a sí mismos, sino que también fomentan una cultura digital más consciente y segura, no solo a nivel general sino también en contextos de los sistemas de salud. (Caján Villanueva, M., Calderón Torres , N. A., & Administrador, 2021)

La rápida evolución de la tecnología exige una constante adaptación y actualización de conocimientos. Los docentes, en particular, desempeñan un papel crucial en esta tarea, ya que su dominio de las competencias digitales no solo influye en su propia seguridad, sino también en la de sus estudiantes. Es fundamental que los educadores se mantengan al día con las mejores prácticas y herramientas de seguridad en línea, integrándolas en su enseñanza para preparar a los estudiantes para un mundo digital seguro.

Aunado a lo anterior, la educación en seguridad digital debe ser integral y continua, comenzando desde niveles educativos básicos y extendiéndose a lo largo de la vida profesional de los individuos. La capacitación y la sensibilización sobre la importancia de la seguridad en línea, deben ser parte de un enfoque educativo global que involucre a instituciones, gobiernos y empresas. Solo a través de un esfuerzo conjunto se puede lograr un entorno digital más seguro y resiliente, capaz de enfrentar los desafíos de un mundo en constante cambio y evolución.

Conclusiones

En última instancia, la seguridad en línea es un pilar fundamental para una participación en la red exitosa y sostenible. Para proteger nuestra seguridad y privacidad en línea, es crucial adoptar medidas preventivas y prácticas seguras. Por ejemplo, es recomendable no compartir las contraseñas de nuestras cuentas en línea con familiares o amigos y guardarlas en un lugar seguro. Esta precaución es vital, especialmente en el caso de que las relaciones personales cambien.

Adicionalmente, no se debe activar la memorización de contraseñas en computadoras compartidas o públicas, ya que esto aumenta el riesgo de que nuestras credenciales sean accesibles a terceros no autorizados, Tomar en serio nuestra privacidad implica no compartir ni permitir el acceso a nuestra información a menos que sea absolutamente necesario, minimizando así el riesgo de que caiga en manos indebidas.

Una estrategia efectiva para minimizar las amenazas y salvaguardar los datos en línea, combina el uso de productos de seguridad, como antivirus y gestores de contraseñas, con el sentido común y la educación continua en prácticas seguras. La concientización y la formación constante en seguridad son esenciales para mantenerse protegido en el entorno tecnológico en constante evolución. Así, no solo nos protegemos a nosotros mismos, sino que también contribuimos a la creación de un entorno digital más seguro y confiable para todos.

Referencias

Villanueva, M. C., & Torres, N. A. C. (2021). Los Metadatos, sistema de salud y regímenes pensionarios de artistas peruanos en el contexto del Covid-19: Metadatos, sistema de salud y regímenes pensionarios de artistas peruanos. GESTIONES, 1(1), 1-9. Recuperado a partir de https://gestiones.pe/index.php/revista/article/view/GESTIONES

Contreras, R. (4 de octubre de 2023). *Los 10 ciberataques más grandes de la década.* Digital Iberia 360. https://www.computing.es/seguridad/los-10-ciberataques-mas-grandes-de-la-decada/

González Fung, C. (2017). Un panorama completo de la seguridad de información en el mundo digital. [Tercer Congreso internacional de ingeniería e informática, retos y perspectivas del mundo digital]. PUCP. https://repositorio.pucp.edu.pe/index/handle/123456789/71344

Molina, J. (2013). *Visión estratégica de seguridad informática en el sector de telecomunicaciones.* [Primer Foro Nacional de seguridad de TI: el impacto de la seguridad en la estrategia de las compañías]. Dirección de operaciones TIC. Emtelco S. A. https://sistemas.uniandes.edu.co/en/foros-isis/temas-foros-isis/contenidos-digitales/foro-8?view=category&id=71

Vallejo, A. [TEDx Talks]. (29 de diciembre de 2015). Una aproximación a la ciberseguridad. [Video]. Youtube. https://www.youtube.com/watch?v=xQQdLKe9LXQ

Universidad Veracruzana. (s.f.). *Las 7 amenazas en ciberseguridad que pueden afectar su vida*. Noti_infosegura. https://www.uv.mx/infosegura/general/noti_ciberseguridad/

Sobre las autoras

Claudia Esmeralda Marisol Villela Cervantes
Editora de la Revista Ciencia Multidisciplinaria CUNORI, Revista Diversidad Científica, Revista Vida, una mirada compleja, y del libro Colectivo del CUNORI, también es encargada del arbitraje de las tres revistas y del libro colectivo de la Escuela de Estudios de Postgrados de la Facultad de Humanidades de la Universidad de San Carlos de Guatemala. Posdoctorante en Educación, Investigación y Complejidad, Doctora en Educación, Magíster en Administración de Recursos Humanos, Ingeniera en Sistemas de Información y Ciencias de la Computación. Investigadora de la Dirección General de Investigación DIGI de la Universidad de San Carlos de Guatemala, Docente en Maestrías y Doctorados en la Universidad de San Carlos de Guatemala. Se desempeña como editora de revistas científicas en la Universidad de San Carlos de Guatemala. Las áreas de interés en investigación, edición de revistas, educación superior, educación virtual, educación intercultural, calidad educativa, tecnología educativa, diseño curricular, paradigmas emergentes y complejidad.

Barbara Rubí Velásquez Monroy
Con Maestría en Docencia Universitaria con Orientación en Estrategias de Aprendizaje egresada del Centro Universitario de Oriente, con licenciatura en Administración de Empresas, egresada del Centro Universitario de Oriente “CUNORI”; labora en el mismo centro desde el año 2019 a la fecha, en la carrera de Ciencias Políticas en el área de economía e investigación. Investigadora de la Dirección General de Investigación DIGI de la Universidad de San Carlos de Guatemala, así mismo, ha realizado investigaciones en revistas de indexadas y de renombre como: Estrategias de aprendizaje y su relación con el rendimiento académico de los estudiantes de relaciones internacionales; Teoría del aprendizaje conectivista, sobresaliente del siglo XXI y la Educación virtual en tiempos de Covid-19.

Financiamiento de la investigación
Con recursos propios.

Declaración de intereses
Declara no tener ningún conflicto de intereses, que puedan haber influido en los resultados obtenidos o las interpretaciones propuestas.

Declaración de consentimiento informado
El estudio se realizó respetando el Código de ética y buenas prácticas editoriales de publicación.

Usabilidad