

Ciberseguridad: formando ciudadanos digitales responsables en las Instituciones Educativas

Gabriela Fernanda Jurado López

Universidad de Nariño

Licenciatura en Informática

X Semestre

gabydehae@gmail.com

La ciberseguridad se ha convertido en un tema de creciente importancia en la actualidad, y su relevancia se extiende a un amplio espectro de sectores, incluyendo el ámbito educativo. Las instituciones educativas enfrentan una serie de desafíos y amenazas en el entorno digital que requieren una atención cuidadosa y estratégica.

Según Arroyo Guardoño, D., Gayoso Martínez, V. & Hernández Encinas, L. (2020):

De forma más precisa, podemos definir la ciberseguridad como el conjunto de técnicas, procedimientos y protocolos encaminados a la protección de la información vinculada a los usuarios de las cibertecnologías. Esta protección demanda la custodia no solo de la información en sí, sino también de todos los elementos precisos para su correcta gestión. (p.12)

La ciberseguridad ha adquirido un carácter esencial en la educación, no solo con el propósito de proteger la información crítica de las instituciones, que pueden estar expuestas a ciberataques que

ponen en riesgo dicha información, sino también para dotar a los estudiantes de las competencias necesarias que les permitan destacar en un entorno digital en constante evolución.

La educación en ciberseguridad marca el comienzo fundamental en la preparación de estudiantes como ciudadanos digitales responsables; en este proceso, la generación de conciencia desempeña un papel de vital importancia. Esto implica no solo identificar problemas comunes como el robo de información personal, el intento de adultos de manipular a menores y el envío de contenido inapropiado, sino también entender bien por qué compartir datos personales en línea puede ser peligroso. El objetivo es que los estudiantes estén al tanto de las amenazas y sepan cómo proteger su información para mantenerse seguros en internet.

En este contexto, la educación en ciberseguridad busca proporcionar a los estudiantes las capacidades esenciales para adoptar una actitud proactiva en la protección de sus datos y dispositivos, esto incluye aspectos como la creación y gestión de contraseñas robustas, la aplicación de medidas de seguridad en línea y la comprensión de los principios fundamentales de la privacidad. Además de las prácticas mencionadas, se sugiere fomentar la conciencia sobre la importancia de las actualizaciones regulares del software y sistemas operativos para mantener la protección ante las últimas amenazas. Es imprescindible enseñar a los estudiantes a discernir y evitar la descarga de aplicaciones o software de fuentes no verificadas, así como a ser cautelosos con los enlaces o archivos adjuntos en correos electrónicos que podrían ser potenciales vectores de ataques cibernéticos. La promoción del uso de autenticación de dos factores

para añadir un nivel adicional de seguridad a las cuentas en línea es fundamental. Estas medidas adicionales ayudarán a fortalecer la seguridad cibernética de los estudiantes, ofreciéndoles un panorama más amplio y eficaz para protegerse en el entorno digital. Además, la instrucción debe estimular una mentalidad crítica que promueva el análisis y la evaluación de la información y recursos disponibles en línea, lo que habilita a los estudiantes para tomar decisiones fundamentadas y seguras en un entorno digital que se encuentra en constante evolución.

Parrish, A., Impagliazzo, J., Raj, R., Santos, H., Asghar, M., Jøsang, A., Pereira, T. & Stavrou, E. (2018) afirman "The cost to society of not having the capacity to meet emerging cybersecurity challenges is simply too high."(p.51)

Los estudiantes actualmente están expuestos a diversos peligros en la red. Uno de los riesgos más destacados es la exposición a contenido inapropiado o peligroso en línea, lo que puede afectar su bienestar emocional y psicológico, además, pueden ser víctimas de ciberacoso, lo que amenaza su seguridad emocional y social. La pérdida de privacidad y el robo de datos personales también son preocupaciones significativas, ya que los estudiantes a menudo comparten información en línea sin conocer los riesgos. Adicionalmente, niños y adolescentes están expuestos a estafas y fraudes en línea que puede afectar negativamente su economía y seguridad financiera.

Los docentes desempeñan un papel esencial en la educación de los estudiantes sobre la importancia de la ciberseguridad en la era digital. Además de impartir conocimientos académicos, los docentes

tienen la responsabilidad de guiar a sus estudiantes en el uso seguro y ético de la tecnología, ellos sirven como modelos a seguir al enseñar prácticas seguras en línea, la protección de datos personales y la prevención de riesgos cibernéticos. Su papel va más allá de la enseñanza de habilidades técnicas; se trata de empoderar a los estudiantes para que puedan navegar en el mundo digital con confianza, asegurando su propia seguridad y respetando la de los demás; la labor de los docentes en la formación de ciudadanos digitales responsables es fundamental para preparar a las generaciones futuras en un entorno cibernético cada vez más complejo y necesario para su desarrollo.

La importancia de la ciberseguridad, así como la formación de ciudadanos digitales responsables desde edades tempranas, resulta indiscutible en la sociedad actual. La formación en ciudadanía digital no solo se trata de cómo evitar peligros en línea, sino también de promover valores éticos, respeto por la privacidad y la responsabilidad en el uso de la tecnología, esto les ayuda a comprender cómo las acciones en línea pueden tener consecuencias en el mundo real y cómo deben comportarse de manera responsable y ética en el ciberespacio.

Zambrano Macías, M. (2018) afirma que "Es imprescindible por ello, que las instituciones y profesionales que interactúan con jóvenes, familiarizarse con el impacto de estas tecnologías sobre la cultura digital del adolescente por lo que se hace imprescindible hablarles de ciberseguridad". (p. 11)

A medida que la tecnología continúa desempeñando un papel central en la vida cotidiana y en el mundo laboral, la formación en ciberseguridad y ciudadanía digital se convierte en una habilidad

crítica. Los estudiantes que adquieren estas habilidades estarán mejor preparados para enfrentar los desafíos tecnológicos en sus futuras carreras y para contribuir a una sociedad digital más segura y ética.

Es de vital importancia que las instituciones educativas integren la ciberseguridad en una amplia variedad de disciplinas académicas, que incluyen desde la tecnología e informática hasta aquellas enfocadas en la ética y las ciencias sociales. Esta integración es de gran importancia en la formación de los estudiantes, ya que les permite comprender a un nivel más profundo cómo la ciberseguridad impacta en su vida diaria y en las oportunidades que les depara el futuro.

Según Manson, D., & Pike, R. (2014) “Developing capabilities that meet the ever growing and changing demands of the cybersecurity discipline requires a new approach to the process of educating students”. (p.51)

En conclusión, la ciberseguridad se ha convertido en un pilar fundamental en la sociedad moderna, y la formación de ciudadanos digitalmente responsables es un imperativo ineludible. El mundo en línea ofrece innumerables oportunidades, pero también plantea amenazas significativas que van más allá de lo digital y afectan la vida cotidiana de las personas. La educación en ciberseguridad no solo protege a los individuos de los peligros cibernéticos, sino que también promueve un uso ético y consciente de la tecnología, fomenta la privacidad y la seguridad de la información y fortalece la resiliencia frente a amenazas cibernéticas en constante evolución.

Las instituciones educativas tienen la responsabilidad de cultivar ciudadanos digitales informados y responsables, brindando a los estudiantes las herramientas necesarias para navegar con seguridad en un mundo digital en constante cambio. Esta formación no solo beneficia a los individuos, sino que también contribuye a la construcción de una sociedad en línea más segura y ética. Es fundamental reconocer que la ciberseguridad y la educación digital ya no son opciones, sino requisitos esenciales para el bienestar y la prosperidad en el siglo XXI.

REFERENCIAS BIBLIOGRÁFICAS

- Arroyo Guardeño, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020). *Ciberseguridad..* Editorial CSIC Consejo Superior de Investigaciones Científicas.
<https://elibro.net/es/lc/udenaar/titulos/172144>
- Manson, D., & Pike, R. (2014). The case for depth in cybersecurity education. *ACM Inroads*, 5(1), 47–52.
<https://doi.org/10.1145/2568195.2568212>
- Parrish, A., Impagliazzo, J., Raj, R., Santos, H., Asghar, M., Jøsang, A., Pereira, T. & Stavrou, E. (2018). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. En *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*.
<https://doi.org/10.1145/3293881.3295778>
- Zambrano Macías, M. (2018). *Ciberseguridad: Riesgo y amenazas de los jóvenes en las redes sociales. Caso: Colegio Fiscal Mixto Camilo Ponce (Tesis de pregrado)*. Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador. [Enlace de la tesis:
<https://repositorio.uleam.edu.ec/handle/123456789/1756>]