

Ciberseguridad y su Impacto en el Desarrollo Sostenible y la Ética Profesional: Un Análisis de la Literatura

Cybersecurity and its Impact on Sustainable Development and Professional Ethics: A Literature Review

Marena Vitola-Quintero*

Corporación Universitaria Rafael Núñez - Colombia
ORCID iD: <https://orcid.org/0000-0001-5219-3615>
marena.vitola@curnvirtual.edu.co

Fecha de recepción: 13/11/2024

Fecha de evaluación: 10/02/2025

Fecha de aceptación: 04/03/2025

Andrés F. Benavides-Ramírez

Corporación Universitaria Rafael Núñez - Colombia
ORCID iD: <https://orcid.org/0009-0004-1804-1641>
abenavidesr21@curnvirtual.edu.co

Cómo citar: *Vitola-Quintero, M., Benavides-Ramírez, A., & Quintana-Porras, O. (2025). Ciberseguridad y su Impacto en el Desarrollo Sostenible y la Ética Profesional: Un Análisis de la Literatura. Revista Científica Anfibios, 8(1), 88-98. <https://doi.org/10.37979/afb.2025v8n1.176>*

Oscar D. Quintana-Porras

Corporación Universitaria Rafael Núñez - Colombia
ORCID iD: <https://orcid.org/0009-0007-8676-7964>
oquintanap21@curnvirtual.edu.co

*Autor a quien debe ser dirigida la correspondencia



[Atribución-NoComercial-CompartirIgual 4.0 Internacional](https://creativecommons.org/licenses/by-nc-sa/4.0/)

Resumen

El presente artículo tiene por objetivo realizar un análisis del impacto que tiene la ciberseguridad sobre el desarrollo sostenible y la ética profesional, para ello, se realizó una búsqueda, recopilación y análisis de información sobre cada tema y la relación que existe entre ellos. Se llevó a cabo una revisión exhaustiva de la literatura en diversas bases de datos como Scielo, Redalyc y Google Academic, lo que permitió recopilar diferentes artículos, trabajos de grado, informes gubernamentales, documentos de organizaciones internacionales, blogs, páginas oficiales, posibilitando documentar la implementación de estrategias y sus resultados con relación a los Objetivos de Desarrollo Sostenible (ODS). También se pudo evidenciar que, con la llegada de la industria 5.0 se asocia con mejoras en eficiencia, calidad y sostenibilidad, pero también plantea nuevos desafíos en ciberseguridad debido a la gran cantidad de datos sensibles involucrados. resaltando la importancia de la ciberseguridad en una sociedad altamente conectada y mencionando las regulaciones éticas que existen actualmente en estos campos. Además, se pudo analizar que (ODS) de las Naciones Unidas se presentan como un marco para abordar problemas globales, y se enfatiza la interconexión entre estos objetivos. La UNESCO reconoce la importancia de los ingenieros y el papel fundamental que cumplen en la consecución de estos objetivos al proponer soluciones a los ODS como el acceso a agua limpia, energía sostenible y ciudades sostenibles. Finalmente, se puede concluir que, la implementación adecuada de la ciberseguridad se presenta como una solución esencial para garantizar un entorno digital seguro y ético, basado en la confianza y la responsabilidad, siendo el núcleo de las estrategias para lograr un desarrollo sostenible y ético, lo que garantiza un futuro protegido contra amenazas cibernéticas y al mismo tiempo inclusivo y éticamente responsable

Palabras clave

Ciberseguridad; desarrollo sostenible; ética Profesional; ODS; análisis de la Literatura

Abstract

The objective of this article is to carry out an analysis of the impact that cybersecurity has on sustainable development and professional ethics. For this purpose, a search, compilation and analysis of information on each topic and the relationship that exists between them was carried out. An exhaustive review of the literature was carried out in various databases such as

Scielo, Redalyc and Google Academic, which allowed the compilation of different articles, degree works, government reports, documents from international organizations, blogs, official pages, making it possible to document the implementation of strategies and their results in relation to the Sustainable Development Goals (SDGs). It was also evident that, with the arrival of industry 5.0, it is associated with improvements in efficiency, quality and sustainability, but it also poses new challenges in cybersecurity due to the large amount of sensitive data involved. highlighting the importance of cybersecurity in a highly connected society and mentioning the ethical regulations that currently exist in these fields. In addition, it was possible to analyze that the United Nations (SDG) are presented as a framework to address global problems, and the interconnection between these objectives is emphasized. UNESCO recognizes the importance of engineers and the fundamental role they play in achieving these goals by proposing solutions to the SDGs such as access to clean water, sustainable energy and sustainable cities. Finally, it can be concluded that the adequate implementation of cybersecurity is presented as an essential solution to guarantee a safe and ethical digital environment, based on trust and responsibility, being the core of the strategies to achieve sustainable and ethical development. which guarantees a future protected against cyber threats and at the same time inclusive and ethically responsible.

Keywords

Cybersecurity; sustainable development; professional ethics; SDGs; literature review

Introducción

A lo largo de la historia se ha evidenciado el uso constante de las tecnologías, con el fin de ir progresivamente satisfaciendo las necesidades de los seres humanos (Velandia, 2016), mejorando permanentemente el bienestar, la salud, la alimentación y alcanzando logros personales y familiares (Alonso-García et al., 2021); por lo anterior, se ha presentado una sinergia positiva y estrecha entre las evoluciones de la sociedad y la tecnología, es por ello que, se pueden observar ligadas en muchos ámbitos de la vida moderna, por ejemplo, en la forma de comunicarse y relacionarse con las personas u otras cosas que los rodean.

Como una consecuencia de lo anterior, se ha originado el término de Sociedad 5.0, que fue presentada por primera vez por el Gobierno japonés en el marco del 5° Plan Básico de Ciencia y Tecnología para 2016-2021(Ortega, 2019), y en la cual se utilizan las tecnologías desarrolladas por la industria 4.0, esta es conocida como la 4° revolución industrial, en la que como resultado se han producido las actuales tecnologías emergentes que están provocando cambios disruptivos en el quehacer diario tanto laboral como personal, entre estas se encuentran: El internet de las cosas (IoT), inteligencia artificial (AI), robótica, sistemas autónomos, blockchain, comunicación 5G, bioinformática, realidad aumentada (Moreda, 2020).

El concepto anterior, pretende ser un aporte al mundo para transformarlo en un planeta súper inteligente, y también ayudar al cumplimiento de los Objetivos de Desarrollo Sostenible para el año 2030 (Ortega, 2019), esto muestra una visión

donde se integren todas las tecnologías digitales antes mencionado con todos los aspectos de la vida cotidiana, buscando mejorar la calidad de vida de las personas, y afrontar retos complejos, como el cambio climático, la gestión de recursos de manera eficiente, para así poder encontrar una posible solución.

Toda esta situación, trae consigo una serie de retos y desafíos, debido a la gran cantidad de datos sensibles que se manejan, a consecuencia de lo anterior se requiere nuevos algoritmos y capas de seguridad para asegurar la integridad de los datos. Esto ha logrado que la ciberseguridad obtenga un papel fundamental en todo el proceso de transformación (Castellanos, 2019). Esta industria tiene varios puntos que la hacen importante, mayor eficiencia y productividad lo que permite a las empresas optimizar sus procesos de producción y operaciones, mejora en la calidad con La automatización, debido a esto reducen los errores humanos y garantizan una mayor consistencia en la calidad del producto. La industria 4.0 puede contribuir a la sostenibilidad al permitir un uso más eficiente de los recursos (Universidad Carlemany, 2022).

En el año 2012, la Organización de las Naciones Unidas introdujo por primera vez los 17 Objetivos de Desarrollo Sostenible (ODS) también llamados objetivos mundiales, pero no fue hasta el 2015 donde fueron adoptados por los Estados perteneciente, con las metas de poner fin a la pobreza, proteger el planeta y garantizar que todas las personas gocen de paz y prosperidad para el año 2030. Los ODS se originaron con el propósito de hacer un llamado urgente a un cambio hacia un camino más sostenible, estos 17 objetivos

son interdependientes uno del otro, lo que implica que el cumplimiento de uno afecta al de otros (Navarro Romero & Rojas Cruz, 2020).

Adicionalmente, a todos los avances en el campo de las tecnologías, es importante tener claro que la información es el activo más importante de una compañía y una pieza fundamental en la vida de las personas (Ospina Reyes, 2023), por lo tanto, esta nueva súper sociedad debe mantener unos protocolos eficientes para salvaguardar, proteger y mantener las tres características de la está, por ello, se presenta el término ciberseguridad, tal como indica Kaspersky, tiene como objetivo garantizar la seguridad de la información digital en un entorno de sistemas interconectados, en la cual implica proteger la integridad de computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos contra posibles ataques maliciosos llevados a cabo por cibercriminales, mediante la defensa activa que involucran el uso de tecnologías y herramientas específicas diseñadas para identificar, prevenir, mitigar y responder a ataques cibernéticos (LISA Institute, s.f.).

Por otro lado, en una sociedad donde la información se gestiona principalmente a través de Internet, la exposición a ciberataques, son más propensos a ocurrir, como lo es el robo de datos, la suplantación de identidad, la propagación de virus y los fraudes, se vuelve una amenaza constante. En este contexto, la ciberseguridad se convierte en un factor esencial para salvaguardar la integridad de los datos que circulan en la red (Mosquera Amancio, 2019). Otro aspecto relevante es la necesidad de establecer regulaciones éticas para el uso de la inteligencia artificial y los sistemas autónomos, estas normas deben regular los sectores de aplicación de la IA y sus limitaciones, así como su impacto en la vida de las personas, la tecnología y los datos (Castellanos, 2019).

En cuanto al informe de los Objetivos de Desarrollo Sostenible (ODS) del 2019, presentado por las Naciones Unidas donde revela un panorama alarmante de deterioro ambiental con aumento del nivel del mar, acidificación de los océanos, degradación del suelo y amenazas a la biodiversidad (Martínez-Duque et al., 2021). A consecuencia de lo anterior surge una pregunta fundamental: ¿Qué estrategias pueden implementar los ingenieros para ayudar al cumplimiento de los ODS? En este contexto, los ingenieros de sistemas sostenibles pueden desempeñar un papel clave al ofrecer soluciones alineadas con

los ODS, como el acceso a agua limpia y saneamiento, energía asequible y no contaminante, crecimiento económico, ciudades sostenibles y producción responsable (Martínez-Duque et al., 2021). Además, la UNESCO reconoce la importancia de la ingeniería para el desarrollo sostenible y estableció el Día Mundial de la Ingeniería para el Desarrollo Sostenible el 4 de marzo para crear conciencia sobre el papel esencial de los ingenieros en la mitigación del cambio climático y el avance hacia un futuro sostenible (UNESCO, 2023).

Metodología

Para el desarrollo de este artículo se utilizó una metodología exploratoria-descriptiva, ya que esta permite comprender un tema o fenómeno mediante la recopilación y descripción de datos (Universidad Veracruzana, s.f.). Además, tiene un enfoque cualitativo, que busca analizar e interpretar el significado de los textos y discursos relacionados con la ciberseguridad, el desarrollo sostenible y la ética profesional. Para ello, se emplea una técnica de análisis de contenido, que consiste en identificar, clasificar y comparar las unidades de información relevantes que se encuentran en las fuentes seleccionadas (Pita-Fernández y Péreztegas-Díaz, 2002).

El proceso se realizó de la siguiente manera: primero, se hizo una revisión exhaustiva de la literatura en bases de datos reconocidas tales EBSCO, SCIELO, Sistema de Gestión de Conocimiento de la Escuela Naval (SGC), Google Libros, Google Académic, esto arrojó como resultado diferentes, artículos, trabajos de grado, informes gubernamentales, documentos de organizaciones internacionales, blogs, páginas oficiales y otras fuentes relevantes, con el objetivo de comprender la Ciberseguridad y su impacto en la ética profesional y el desarrollo sostenible (ODS) y sus metas asociadas, esto incluyó investigar las definiciones, alcances y desafíos relacionados con cada uno (Hernández-Sampieri, Fernández-Collado y Baptista-Lucio, 2010).

Luego, se seleccionaron casos representativos de proyectos relacionados con estas áreas, estos se sometieron a un estudio detallado, que incluyó un análisis documental y revisión de datos de desempeño, con el fin de documentar cómo se implementaron las estrategias para contribuir a los ODS y cuáles fueron los resultados alcanzados.

Resultados

Para llevar a cabo esta investigación, se consultaron y revisaron 50 referencias bibliográficas provenientes de diversas fuentes durante el proceso de revisión de la literatura. En la tabla 1 se puede observar detalladamente la muestra seleccionada, la

cual, fue fundamental para la fase de organización y análisis de la información encontrada que se utilizó como base para la investigación. En ella, se incluyeron los nombres de los autores, los títulos de los artículos o libros, el año de publicación, las revistas académicas o editoriales, y un breve resumen.

Tabla 1. Referencias Bibliográficas

#	Nombre	Autor(es)	Resumen
1	Tecnología educativa para la agenda 2030: Objetivos de Desarrollo Sostenible (ODS) ante la pandemia	<u>Alonso García, Santiago; Romero Rodríguez, José María; Marín Marín, José Antonio; Sadio Ramos, Fernando José (2021)</u>	Este artículo hace mención a cómo la sociedad de la información ha transformado varios aspectos de la vida cotidiana, incluyendo la educación, la familia, lo social, lo cultural y lo político. Se enfoca particularmente en el papel central de las tecnologías de aprendizaje en la educación del siglo XXI, especialmente acentuado durante la pandemia
2	La cuarta revolución industrial y las tecnologías disruptivas	Castellanos, Carlos (2019) https://www.unab.edu.sv/la-cuarta-revolucion-industrial-y-las-tecnologias-disruptivas/	El artículo explora la llegada de la Cuarta Revolución Industrial (i4.0) y su impacto en la sociedad y la economía. Se destaca cómo la i4.0 fusiona el mundo físico, digital y biológico, alterando la forma en que las personas se relacionan, trabajan y viven.
3	Guía metodológica para elaborar trabajos de grado V. 1.0.	Gómez Torregrosa-SA, Cedrid (2019)	En este documento, se presenta una guía detallada de metodología diseñada para orientar a estudiantes para llevar a cabo investigaciones académicas de alta calidad. La guía abarca desde la formulación de la pregunta de investigación hasta la presentación de los resultados.
4	Diferencia entre Ciberseguridad, Seguridad Informática y Seguridad de la Información	Lisa Institute (n.d) https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion	En el artículo se examinan y definen los principios básicos relacionados con la ciberseguridad, Seguridad Informática y Seguridad de la Información. Además, que se realiza un análisis detenido de cada término, detallando sus definiciones específicas y resaltando las diferencias clave entre ellos.
5	4ta REVOLUCIÓN INDUSTRIAL: INDUSTRIA 4.0	Moreda, Pablo (2020) http://sedici.unlp.edu.ar/handle/10915/97921	Este artículo aborda temas relacionados con la 4ta revolución industrial, cuáles fueron los países que impulsaron a que se llevase a cabo, además trata de cómo se dio la evolución de los sistemas productivos, industria 4.0 y Lean Management
6	Ciberseguridad En Colombia	Valoyes <u>Mosquera</u> , Amancio (2019) http://repository.unipiloto.edu.co/handle/20.500.12277/6370	Este artículo se centra en el contexto de la ciberseguridad en Colombia, donde se definen conceptos esenciales de ciberseguridad y seguridad informática. Además, se aborda la problemática de los delitos informáticos en el país, resaltando la importancia de comprender las diferencias entre estos conceptos en el contexto colombiano.
7	Objetivos de desarrollo sostenible en Colombia	Navarro Romero, Mónica Alejandra; Rojas Cruz, Angie Carolina (2021) https://hdl.handle.net/10983/25595	El objetivo principal de este párrafo es informar sobre los 17 objetivos de desarrollo sostenible (ODS) presentados ante la Organización de las Naciones Unidas en 2012, y destacar la importancia de conocer lo que se ha realizado en Colombia en términos de implementación y evolución de estos objetivos, ya que su impacto debe ser evidente para el año 2030.

8	Sociedad 5.0: el concepto japonés para una sociedad superinteligente	Ortega, Andres (2019)	El objetivo de este artículo es presentar el concepto de Sociedad 5.0 desarrollado por Japón como una respuesta a sus desafíos demográficos y la necesidad de aprovechar los avances tecnológicos para mejorar la calidad de vida de las personas.
9	Diseño de un sistema de seguridad de la información basado en la Norma ISO 27001:2013 para el Fondo de Empleados Febimbo en el área de tecnología	Ospina Juan Carlos (2023) https://repository.unad.edu.co/handle/10596/56674	En el documento se destaca la importancia de garantizar la seguridad de la información en las organizaciones a través de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). En resumen, se aboga por la implementación de un SGSI como una medida esencial para proteger la información en un entorno empresarial en constante evolución.
10	Día Mundial de la Ingeniería para el Desarrollo Sostenible	Unesco (2023) https://www.unesco.org/es/days/engineering-sustainable-development	El mensaje transmitido por la directora general de la UNESCO se enfoca en el papel fundamental de la ingeniería en la búsqueda de soluciones sostenibles a los desafíos globales y la importancia de promover la educación y la colaboración en este campo.
11	Esta es la importancia de la Industria 4.0 en la sociedad actual	Universidad Carlemany (n.d.) https://www.universitatcarlemany.com/actualidad/blog/industria-4-0-importancia/	Este artículo publicado en el foro de la Universidad Carlemany explora cómo la Industria 4.0 está remodelando la sociedad actual al impulsar la innovación tecnológica, la eficiencia en la producción y la necesidad de abordar desafíos como la ciberseguridad en esta era digital.
12	La tecnología: ¿una ayuda para progresar o retroceder?	Velandia, Diana (2016) https://librepensador.uexternado.edu.co/la-tecnologia-una-ayuda-para-progresar-o-retroceder/	Este artículo explora los pros y contras que trae consigo la tecnología, planteando si esta es una herramienta que impulsa al progreso o si, en algunos casos, puede contribuir al retroceso de la sociedad.
13	La ingeniería en Colombia, ¿Educación de calidad?: cuarto objetivo de desarrollo sostenible	Valdiri Lugo, Luz Elena; Mahecha Hernández, Daniela Fernanda (2019) https://educacioneningenieria.org/index.php/edi/article/view/979/950	El artículo resalta la importancia de la educación en ingeniería para promover un mundo sostenible, y subraya cómo los organismos internacionales consideran el conocimiento como clave para mejorar las condiciones mundiales. El cuarto Objetivo de Desarrollo Sostenible (ODS) se enfoca en una educación inclusiva y equitativa de calidad para todos. El artículo tiene como objetivo evaluar la implementación del cuarto ODS en las facultades de ingeniería acreditadas en Colombia.
14	La ciberseguridad en la gestión inteligente del agua	Donoso, María C. (2022) https://www.cershi.org/images/nuestra-labor/publicaciones/PDF/2022/Inteligencia_artificial_SegHid.pdf#page=33	El objetivo de este artículo es presentar la gestión inteligente del agua como una estrategia que implica la recopilación, comparación y análisis de datos en tiempo real de equipos y redes de agua.
15	¿Cuán importante es la seguridad cibernética para lograr la seguridad hídrica?	Donoso, María C.(2022) https://doi.org/10.15359/rca.56-1.15	Este artículo busca resaltar la importancia de lograr la seguridad hídrica como parte integral del desarrollo sostenible. El artículo tiene como objetivo concienciar al sector del agua sobre la amenaza real de ataques cibernéticos y proponer acciones para fortalecer la ciberseguridad y garantizar la seguridad hídrica de manera sostenible.

Fuente: Elaboración propia

Impacto de la Ingeniería de Sistemas en la Consecución de los Objetivos de Desarrollo Sostenible

Los profesionales de Ingeniería de Sistemas desempeñan un papel crucial en la consecución de los Objetivos de Desarrollo Sostenible establecidos por las Naciones Unidas, contribuyendo de diversas formas significativas, debido a que estos comprenden y abordan problemas cotidianos y complejos, brindan soluciones que abordan varios ODS simultáneamente, como es el caso de la optimización de recursos naturales y energía, esencial para los ODS 12 (Producción y Consumo Responsables) y 13 (Acción por el Clima) (UNESCO, 2021).

La ingeniería de sistemas también impulsa la innovación tecnológica en áreas cruciales como energías renovables, tratamiento de agua, agricultura sostenible y atención médica, contribuyendo así a los ODS 3 (Salud y Bienestar), 6 (Agua Limpia y Saneamiento) y 7 (Energía Asequible y No Contaminante). Además, los ingenieros de sistemas desarrollan sistemas de información y tecnologías de datos para una gestión efectiva de datos, esencial para tomar decisiones informadas y medir el progreso hacia los ODS (UNESCO, 2021).

La planificación y diseño de infraestructuras sostenibles, incluyendo edificios ecológicos, redes de transporte eficientes y sistemas de gestión de residuos, también son áreas clave de la ingeniería de sistemas, contribuyendo a los ODS 9 (Industria, Innovación e Infraestructura) y 11 (Ciudades y Comunidades Sostenibles). En resumen, la ingeniería de sistemas desempeña un papel multifacético y esencial en la consecución de los ODS, ofreciendo soluciones integradas y sostenibles para los desafíos actuales y futuros. Los ingenieros de sistemas desempeñan un papel fundamental en el desarrollo del campo de la ciberseguridad debido a su profundo conocimiento de los sistemas informáticos y su capacidad para entender y abordar las complejidades de la tecnología. En el contexto de la ciberseguridad, estos ingenieros desempeñan un papel fundamental ya que, están especialmente capacitados para diseñar, implementar y mantener sistemas informáticos seguros y protegerlos contra posibles amenazas cibernéticas (MichaelPage, s.f.).

Objetivos de Desarrollo Sostenible Relacionado con la Ciberseguridad

De los ODS que tienen relación con la ciberseguridad, se puede evidenciar que el número 6 - “energía asequible y no contaminante” es uno de ellos, como lo explica Lázaro-Trasobares (2022), quien asegura que uno de los desafíos que afrontará el ser humano en un futuro es desarrollar un modelo energético sostenible, seguro y eficiente. A pesar de que el sol es una fuente de energía inagotable, su potencial apenas ha sido aprovechado. Sin embargo, con la expansión y descentralización de las fuentes de energía y la creciente integración de dispositivos inteligentes en el sistema, aumenta el riesgo de ciberataques. La red eléctrica, siendo una de las infraestructuras más complejas creadas por el ser humano y vital para el funcionamiento de un país, necesita ser protegida contra posibles ataques externos.

A su vez la integración de una gran cantidad de plantas de energía solar fotovoltaica en un sistema eléctrico interconectado, conlleva muchos retos que afectan a la “*estabilidad, confiabilidad y calidad de la energía del sistema debido a la naturaleza intermitente de la radiación solar y a los problemas de acceso físico a los lugares donde la mayoría de las plantas de energía fotovoltaica están ubicadas*” (Lázaro-Trasobares, 2022). Asegurar que las redes eléctricas funcionen de manera segura y confiable es esencial para la economía y la seguridad nacional de cualquier país (Lázaro-Trasobares, 2022).

Además, de lo anterior, la ciberseguridad juega un papel fundamental, en el objetivo #3, debido a que en el sector salud, se ha evidenciado una gran afectación por parte de ciberdelincuentes, dado que los ciberdelitos se producen en redes interconectadas, y las entidades de este sector cuentan con estas redes, siendo el internet el campo favorito para los atacantes. Por esta razón la ciberseguridad le daría un gran aporte a este ODS ya que se encargaría de la protección de ataques cibernéticos de los sistemas conectados a internet, incluidos hardware, software y los datos (Andrade-Vintimilla, 2023).

También, es importante este tema en el objetivo #16 “Paz y justicia”, que tiene como objetivo “*fortalecer las instituciones nacionales pertinentes, incluso mediante la cooperación internacional, para crear a todos los niveles, particular-*

mente en los países en desarrollo, la capacidad de prevenir la violencia y combatir el terrorismo y la delincuencia” (Organización de las Naciones Unidas, s.f.), dentro del grupo de ataque terrorista, se encuentra el ciberterrorismo el cual implica el uso del ciberespacio como herramienta para generar terror y miedo en las poblaciones, naciones y estados (Ministerio de Tecnologías de la Información y Comunicaciones de Colombia, s.f.). en consecuencia, la ciberseguridad es la encargada de prevenir estos atentados (Andrade, 2023).

Impacto de la Ciberseguridad en el Desarrollo Sostenible

Con base en lo anterior, se infiere que la ciberseguridad desempeña un papel fundamental en el desarrollo sostenible al impactar directamente en la economía, sociedad y medio ambiente, además garantiza la protección de datos personales y sensibles, promoviendo la confianza en tecnologías digitales esenciales para servicios en línea, comercio electrónico y gestión de datos en sectores como salud y educación. Igualmente, asegura la protección de infraestructuras críticas como centrales eléctricas y sistemas de transporte, siendo vital para el funcionamiento eficiente de las sociedades modernas (Domínguez, 2022).

También contribuye a la inclusión digital al hacer que las personas se sientan seguras en línea, aunque la falta de infraestructura sólida puede exponer a las personas a fraudes y robo de identidad, desalentando su participación en la economía digital (Domínguez, 2022).

Así mismo, la ciberseguridad es importante en varios aspectos del desarrollo sostenible, incluida la preservación del medio ambiente en un mundo cada vez más conectado. Con el auge de la Internet de las cosas (IoT), los dispositivos conectados, desde medidores inteligentes hasta sistemas de riego automatizados, han revolucionado nuestra interacción con el entorno (Ciberprotege, 2023).

Estos dispositivos desempeñan un papel fundamental en la conservación de recursos vitales como el agua y la electricidad. No obstante, en el caso de que estos no tengan protocolos de seguridad, se vuelven vulnerables a intrusiones cibernéticas. La ciberseguridad no solo protege estos dispositivos, sino que también reduce el tráfico de datos innecesario, disminuyendo así el consumo de energía asociado (Ciberprotege, 2023).

Adicionalmente, la ciberseguridad es esencial para cumplir con los ODS en el mundo digital actual, porque ayuda a asegurar un futuro sostenible, es indispensable invertir en tecnologías seguras que protejan sistemas y datos necesarios para monitorear y alcanzar metas relacionadas con la salud, educación y gobierno electrónico. Al garantizar la integridad y seguridad de estos datos, la ciberseguridad se convierte en un pilar fundamental para el progreso hacia un mundo más sostenible, donde la tecnología se utiliza para abordar desafíos globales de manera efectiva y eficiente.

Impacto de la Ciberseguridad en la Gestión del Agua

Una situación en la que la ciberseguridad tiene alta importancia es en la gestión inteligente del agua, debido a que esta implica recopilar, compartir y analizar datos de equipos y redes de agua utilizando tecnologías de información y comunicación avanzadas, como sensores, GIS, Internet de las Cosas y Big Data. Estas tecnologías permiten mejorar la gestión operativa y estratégica de los recursos hídricos (Donoso, 2022). Sin embargo, esta innovación tecnológica también conlleva riesgos asociados a la ciberseguridad, como ataques cibernéticos a bases de datos, servicios en línea y procesos operativos del sector hídrico. A su vez establecer regulaciones y políticas efectivas para garantizar la seguridad de los sistemas de agua en un entorno tecnológico en constante evolución.

El texto anterior resalta de manera elocuente cómo las tecnologías avanzadas pueden revolucionar la gestión del agua, tanto en aspectos operativos como estratégicos. Al posibilitar la monitorización en tiempo real y el análisis de datos complejos, estas herramientas ofrecen una valiosa oportunidad para tomar decisiones fundamentadas y optimizar la utilización de los recursos hídricos.

Sin embargo, en medio de este panorama prometedor, surge una preocupación crucial planteada por Donoso (2022a) sobre la ciberseguridad: Analiza la urgencia de abordar los desafíos vinculados a la ciberseguridad, especialmente en el ámbito de la gestión inteligente del agua. La interconexión de sistemas, vital para la recopilación y análisis de datos en tiempo real, también crea vulnerabilidades significativas. Donoso ad-

vierte sobre posibles ataques cibernéticos que podrían comprometer bases de datos, servicios en línea y operaciones del sector hídrico. Esta advertencia cobra una relevancia particular en un contexto donde la infraestructura crítica, como el suministro de agua, se ha convertido en un objetivo atractivo para los ciberdelincuentes que buscan acceder a datos sensibles.

Así como, la necesidad imperante de establecer regulaciones y políticas efectivas en este campo no puede ser subestimada. La ciberseguridad implica no solo la implementación de medidas técnicas, sino también la formulación de políticas que garanticen la integridad de los sistemas de agua en un entorno tecnológico en constante evolución. La creación y aplicación de estándares rigurosos se vuelven esenciales para proteger la infraestructura crítica y mantener la confianza del público en la seguridad de su suministro de agua.

Así mismo, actualmente se resalta la importancia fundamental de la educación en ingeniería, porque se reconoce como fundamental para avanzar hacia un mundo sostenible, siendo enfatizada por organismos internacionales como una herramienta clave para mejorar las condiciones sociales globales. El 04 ODS se centra en asegurar una educación inclusiva y equitativa de calidad, así como promover oportunidades de aprendizaje a lo largo de la vida para todos (Valdiri-Lugo y Mahecha-Hernández, 2019).

El artículo plantea interrogantes fundamentales acerca de la calidad de la educación en ingeniería en Colombia. En un mundo donde la tecnología y la innovación desempeñan un papel vital en el desarrollo económico y social, es imprescindible que la educación en ingeniería cumpla con estándares de calidad excepcionales. Esta calidad no solo se relaciona con el conocimiento técnico impartido, sino también con la capacidad de los ingenieros para abordar problemas complejos, fomentar la innovación y contribuir a soluciones sostenibles.

La inclusión de la educación en ingeniería como el cuarto Objetivo de Desarrollo Sostenible (ODS) destaca su importancia a nivel global. Este ODS se enfoca en garantizar una educación inclusiva, equitativa y de alta calidad, así como promover oportunidades de aprendizaje a lo largo de la vida para todos. Este enfoque inclusivo y continuo no sólo capacita a las personas con

conocimientos y habilidades técnicas, sino que también desempeña un papel significativo en la construcción de sociedades más justas y sostenibles.

Adicionalmente, el artículo nos lleva a reflexionar acerca de la equidad en la educación en ingeniería. Asegurar que la educación en este campo sea accesible para todos, sin importar su origen socioeconómico, género o ubicación geográfica, es esencial para la creación de una sociedad justa y equitativa. La equidad en la educación en ingeniería no solo amplía las oportunidades individuales, sino que también enriquece el campo con diversas perspectivas y enfoques, lo cual puede fomentar la innovación y la creatividad en la resolución de futuros desafíos.

También, es importante la seguridad cibernética para lograr la hídrica, como lo evidencia la investigación llevada a cabo por Donoso (2022a), este explica por qué se debe alcanzar la seguridad hídrica para lograr un desarrollo sostenible, implicando acceso a agua en cantidad y calidad adecuadas, así como la preservación del recurso y la eficiencia en su uso. Sin embargo, señala que el sector del agua está vulnerable a ataques cibernéticos, que han aumentado significativamente en los últimos cinco años.

Lo anterior, la seguridad hídrica representa un pilar fundamental para el desarrollo sostenible, que va más allá del simple acceso al agua en cantidad y calidad adecuadas. Implica también conservar este recurso y utilizarlo de manera eficiente. No obstante, a pesar de la vital importancia del sector del agua, nos encontramos ante una creciente amenaza: los ataques cibernéticos. En los últimos años, esta vulnerabilidad ha aumentado de manera alarmante, como indican los datos que muestran un incremento significativo en estos tipos de ataques.

En resumen, la seguridad hídrica y la seguridad cibernética están intrínsecamente ligadas en esta era digital. Pasar por alto esta conexión puede resultar en consecuencias graves. No obstante, al aumentar la conciencia sobre este tema, comprender las amenazas y tomar medidas adecuadas, es posible fortalecer la seguridad hídrica y, por ende, avanzar hacia un futuro más sostenible y seguro para todos.

Impacto de la Ciberseguridad en la Ética Profesional

Con todos los actuales avances tecnológicos y su auge en el mundo en especial después de la emergencia sanitaria presentada en el año 2020, la ciberseguridad ejerce una influencia significativa en la ética profesional en diversas dimensiones. En primer lugar, implica la responsabilidad ética de proteger los datos y sistemas, cultivando la confianza del público y las organizaciones mediante medidas que aseguren la confidencialidad de la información. Sin embargo, la falta de ética, como el robo de datos o actividades ilegales, debilita esta confianza y amenaza la integridad profesional. Además, el respeto por la privacidad es fundamental; los profesionales de la ciberseguridad deben proteger los datos y garantizar que no sean objeto de acceso no autorizado (Ironhack, 2021).

Asimismo, la ciberseguridad ética implica un compromiso con la legalidad, debido a que los profesionales deben operar dentro del marco legal y ético, evitando participar en actividades ilegales o poco éticas, como las prácticas maliciosas de hacking. En cambio, realizar actividades de manera ética, como el hacking ético que se lleva a cabo de manera legal y responsable, respetando la privacidad y la integridad de los sistemas informáticos.

La ciberseguridad también tiene un impacto significativo en la ética profesional en términos de responsabilidad, privacidad, educación, transparencia, legalidad, equidad y no discriminación. Los profesionales de la ciberseguridad desempeñan un papel fundamental en el mantenimiento de estándares éticos elevados y en la promoción de la confianza y la seguridad en el mundo digital en constante evolución (Hireline, s.f.). Su labor contribuye a una sociedad más justa y segura, donde las personas pueden confiar en que sus datos y sistemas están protegidos de manera ética y legal, promoviendo así la integridad y la confianza en el ámbito profesional y social (Ironhack, 2021).

Referencias

- Alonso-García, S., Romero-Rodríguez, J. M., Marín-Marín, J. A., & Sadio-Ramos, F. J. (2021). Tecnología educativa para la agenda 2030: Objetivos de Desarrollo Sostenible (ODS) ante la pandemia. *Texto Livre: Linguagem e Tecnologia*, 14(2) <https://www.redalyc.org/journal/5771/577168155001/577168155001.pdf>
- Andrade-Vintimilla, J. (2023). Ciberseguridad y Salud. Edición Especial: Enfoques Multidisciplinares Volumen 2, No 1, ISSN: 2773-7640. <https://www.itscs-cicc.com/ojs/index.php/inndev/article/view/47/17>

Conclusiones

En conclusión, este estudio ha proporcionado una visión profunda sobre la relación entre la ciberseguridad, el desarrollo sostenible y la ética profesional, explorando cómo la ingeniería de sistemas desempeña un papel fundamental en la consecución de los Objetivos de Desarrollo Sostenible (ODS). Los resultados de este demuestran la importancia que tiene la ciberseguridad en la sociedad y que no solo se debe abordar desde la perspectiva tecnológica sino también desde el punto de la ética profesional y de la sostenibilidad.

También se ha evidenciado que la ciberseguridad cuando se integra de manera adecuada en los sistemas de información y las prácticas profesionales, puede impulsar la confianza y la responsabilidad en todas las áreas de desarrollo, convirtiéndose en un pilar fundamental en la consecución de varios ODS, ya que protege los activos digitales, sistemas y la privacidad de los individuos. Sin embargo, al explorar las complejidades éticas que rodean la seguridad cibernética, se destaca la necesidad urgente de salvaguardar la privacidad, la equidad y la justicia en un mundo digital que va en constante evolución. En este contexto, la integración adecuada de la ciberseguridad en los sistemas y prácticas profesionales se presenta como una solución esencial para garantizar un entorno digital seguro y ético, donde la confianza y la responsabilidad sean los pilares de un progreso sostenible.

Finalmente, es necesario recalcar la necesidad de considerar la ciberseguridad como centro esencial de cualquier estrategia para lograr un desarrollo sostenible y ético. Pudiendo así avanzar hacia un futuro que no solo esté protegido contra amenazas cibernéticas, sino que también sea inclusivo, sostenible y éticamente responsable.

- Castellanos, C. (13 de diciembre 2019). La Cuarta Revolución Industrial y las Tecnologías Disruptivas. Noticias Universidad Dr. Andrés Bello. UNAB. <https://www.unab.edu.sv/la-cuarta-revolucion-industrial-y-las-tecnologias-disruptivas/>
- Ciberprotege. (29 de septiembre 2023). ¿Sabías que? La Ciberseguridad Ayuda a un Medio Ambiente Sostenible. Centro Europeo de Empresas e Innovación de Castellón. <https://ceeicastellon.emprenemjunts.es/?op=8&n=30411>
- Domínguez, L. (24 de noviembre 2022). Ciberseguridad y Desarrollo Sostenible, Oportunidades en la Green Cloud - CyberSecurity News. <https://cybersecuritynews.es/ciberseguridad-y-desarrollo-sostenible-oportunidades-en-la-green-cloud/>
- Donoso, M. C. (2022). La Ciberseguridad en la Gestión Inteligente del Agua. Inteligencia Artificial y Transformación Digital para la Seguridad Hídrica. UNESCO-CODIA- Red Iberoamericana- CERSHI. 33-35. https://www.cershi.org/images/nuestra-labor/publicaciones/PDF/2022/Inteligencia_artificial_SegHid.pdf#page=33
- Donoso, M. C. (2022a). ¿Cuán Importante es la Seguridad Cibernética para Lograr la Seguridad Hídrica? Revista de Ciencias Ambientales, 56(1), 284–297. <https://doi.org/10.15359/RCA.56-1.15>
- Hernández-Sampieri, R., Fernández-Collado, C., y Baptista-Lucio, M.d.P. (2010). Metodología de la Investigación, 5ta Ed. McGraw-Hill <https://www.icmujeres.gob.mx/wp-content/uploads/2020/05/Sampieri.Met.Inv.pdf>
- Hireline. (s.f.). Perfil de Especialista en Ciberseguridad. Blog Hireline. Recuperado 28 de octubre 2023, desde <https://hireline.io/co/enciclopedia-de-perfiles-de-tecnologia/especialista-en-ciberseguridad>
- Ironhack. (24 de marzo 2021). ¿Qué Hace un Profesional de la Ciberseguridad?. Blog Ironhack. <https://www.ironhack.com/es/blog/que-hace-un-profesional-de-la-ciberseguridad>
- Lázaro-Trasobares, L. (2022). Análisis de Criterios de Ciberseguridad en una Planta de Generación Renovable. Repositorio de la Universidad Pontificia Comillas. <https://repositorio.comillas.edu/xmlui/handle/11531/62076>
- LISA Institute. (s.f.). Diferencia entre Ciberseguridad, Seguridad Informática y Seguridad de la Información. Recuperado 06 septiembre, 2023, desde <https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion>
- Martínez-Duque, D., Sánchez-Medina, I. I., Cabrera-Medina, J. M., & Clavijo-Bustos, N. (2021). Inclusion of Sustainable Engineering in the Regional Context. Formación Universitaria, 14(5), 11–18. <https://doi.org/10.4067/S0718-50062021000500011>
- MichaelPage. (s.f.). Perfil de Ingeniero de Ciberseguridad. Blog MichaelPage – Profesión -Tecnología. Recuperado 26 de octubre 2023, desde <https://www.michaelpage.es/advice/profesi%C3%B3n/tecnolog%C3%ADa/perfil-de-ingeniero-de-ciberseguridad>
- Ministerio de Tecnologías de la Información y Comunicaciones de Colombia. (s.f.). Ciberterrorismo. Recuperado 29 de octubre 2023, desde <https://www.mintic.gov.co/portal/inicio/Glosario/C/18728:Ciberterrorismo>
- Moreda, P. (2020). 4ta Revolución Industrial: Industria 4.0. SEDICI. Repositorio Institucional de la UNLP. Facultad de Ingenierías <http://sedici.unlp.edu.ar/handle/10915/97921>
- Mosquera Amancio, V. (28 de agosto 2019). Ciberseguridad en Colombia. Repositorio Institucional Universidad Piloto de Colombia. Facultad de Ingenierías, Especialización en Seguridad Informática <http://repository.unipiloto.edu.co/handle/20.500.12277/6370>

- Navarro Romero, M. A., & Rojas Cruz, A. C. (2020). *Objetivos de Desarrollo Sostenible en Colombia*. Universidad Católica de Colombia. Facultad de Ciencias Económicas y Administrativas. Programa de Economía. Especialización en Administración Financiera. Bogotá, Colombia. <https://repository.ucatolica.edu.co/server/api/core/bitstreams/de8c8277-4fc8-4a6c-88a4-95a99767828b/content>
- Organización de las Naciones Unidas. (s.f.). *Objetivos y Metas de Desarrollo Sostenible*. Recuperado 29 de octubre 2023, desde <https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/>
- Ortega, A. (2019). *Sociedad 5.0: el Concepto Japonés para una Sociedad Superinteligente*. Real Instituto Elcano Royal Institute. <https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/ari10-2019-ortega-sociedad-5-0-concepto-japones-sociedad-superinteligente.pdf>
- Ospina Reyes, J. C. (2023). *Diseño de un Sistema de Seguridad de la Información Basado en la Norma ISO 27001:2013 para el Fondo de Empleados FEBIMBO en el Área de Tecnología*. [Proyecto aplicado]. Repositorio Institucional UNAD. <https://repository.unad.edu.co/handle/10596/56674>
- Pita-Fernández, P., y Pértegas-Díaz, P. (2002). *Investigación Cuantitativa y Cualitativa*. Unidad de Epidemiología Clínica y Bioestadística. Complejo Hospitalario-Universitario Juan Canalejo. A Coruña (España). *Cad Aten Primaria* 2002; 9: 76-78 https://www.fisterra.com/gestor/upload/guias/cuanti_cuali2.pdf
- UNESCO. (2021). *Ingeniería para el Desarrollo Sostenible*. UNESCO Biblioteca Digital. https://unesdoc.unesco.org/ark:/48223/pf0000375634_spa
- UNESCO. (2023). *Día Mundial de la Ingeniería para el Desarrollo Sostenible* | UNESCO Biblioteca Digital. <https://www.unesco.org/es/days/engineering-sustainable-development>
- Universidad Carlemany. (14 de julio 2022.). *Esta es la Importancia de la Industria 4.0 en la Sociedad Actual*. Blog Universidad Carlemany – Tecnología e Innovación. <https://www.universitatcarlemany.com/actualidad/blog/industria-4-0-importancia/>
- Universidad Veracruzana. (s.f.). *Introducción a la Investigación: Guía Interactiva*. Recuperado 08 de abril 2023, desde: <https://www.uv.mx/apps/bdh/investigacion/unidad1/investigacion-tipos.html>
- Valdiri-Lugo, L., & Mahecha-Hernández, D. (2019). *La Ingeniería en Colombia, ¿Educación de Calidad?: Cuarto Objetivo de Desarrollo Sostenible*. *Revista Educación en Ingeniería*. Asociación Colombiana de Facultades de Ingeniería. <https://educacioneningenieria.org/index.php/edi/article/view/979/950>
- Velandia, D. L. (2016, Julio 22). *La Tecnología: ¿Una Ayuda para Progresar o Retroceder?* <https://librepensador.uexternado.edu.co/la-tecnologia-una-ayuda-para-progresar-o-retroceder/>