ESCUELA NAVAL DE CADETES
"ALMIRANTE PADILLA"
Honor y Tradición

OnBoard Knowledge Journal

*Article*

# Professional Ethics and Cybersecurity Education: A Strategy to Promote Sustainable Development

# Ética Profesional y Educación en Ciberseguridad: Una Estrategia para Promover el Desarrollo Sostenible

**Marena Vitola Quintero [1]* Isaac Yamith Guzmán Paternina [2] and Ulises Herrera Bustillo [3]**

[1] Corporación Universitaria Rafael Nuñez, Cartagena, 130014, Colombia; marena.vitola@curnvirtual.edu.co; isaac.guzman@curnvirtual.edu.co; ulises.herrera@curnvirtual.edu.co

* Correspondence: marena.vitola@curnvirtual.edu.co

**Citation:** Vitola, M.;Guzmán, I.; Herrera, U. Professional Ethics and Cybersecurity Education: A Strategy to Promote Sustainable Development. *OnBoard Knowledge Journal* **2025**, *1*, 3. https://doi.org/10.70554/OBJK2025.v01n02.03

Received: 05/06/2025, Accepted: 12/07/2025, Published: 26/08/2025

**DOI:** https://doi.org/10.70554/OBJK2025.v01n02.03

**Abstract:** This article explores the intersection between ethics, cybersecurity and sustainable development. First, a systematic literature review of various databases is presented in order to establish the theoretical framework and identify the main trends in the field, the information found was filtered and analyzed, allowing us to highlight that cybersecurity is essential to protect the online information and foster trust in a digital world and that education on this topic helps prevent cybercrimes, comply with regulations and laws, and promote digital inclusion. In addition, the importance of professional ethics in technology is highlighted to guarantee that decisions related to it are made ethically, considering the social and environmental impacts that they may generate. Notorious examples, such as the Cambridge Analytica scandal, are mentioned to highlight the importance of ethics in technology. Next, the methodology used is described, which includes a multiple case study of leading organizations in the technology sector. The results of this study are presented in the third section, where the ethical cybersecurity practices implemented by these organizations are analyzed. In the fourth section, a strategy to promote cybersecurity education and professional ethics in Colombia is discussed as a means to address specific cybersecurity challenges in the country, such as ransomware attacks and cybercrimes and their impact on sustainable development, highlighting the need to make ethical decisions in technology to balance economic growth, social inclusion and environmental protection. Finally, the conclusions are presented and recommendations are made to promote ethics in cybersecurity and sustainable development at the organizational and societal level.

**Keywords:** Cybersecurity education; Data protection; Professional ethics; Sustainable development.

**Resumen:** Este artículo explora la intersección entre la ética, la ciberseguridad y el desarrollo sostenible. En primer lugar, se presenta una revisión sistemática de la literatura diversas bases de datos con el fin de establecer el marco teórico e identificar las principales tendencias en el campo, se filtró y analizó la información encontrada permitiendo destacar que la ciberseguridad es esencial para proteger la información en línea y fomentar la confianza en un mundo digital y que la educación en este tema ayuda a prevenir ciberdelitos, cumplir con regulaciones y leyes, y promover la inclusión digital. Además, se subraya la importancia de la ética profesional en tecnología para garantizar que las decisiones relacionadas con ella se tomen de manera ética, considerando los impactos sociales y ambientales que puedan generar. Se mencionan ejemplos notorios, como el escándalo de Cambridge Analytica, para resaltar la importancia de la ética en la tecnología. Seguidamente, se describe la metodología empleada, que incluye un estudio de caso múltiple de organizaciones líderes en el sector tecnológico. Los resultados de este estudio se presentan en la tercera sección, donde se analizan las prácticas éticas en ciberseguridad implementadas por estas organizaciones. En la cuarta sección, se discute una estrategia para promover la educación en ciberseguridad y ética profesional en Colombia como medio para abordar desafíos específicos en ciberseguridad en el país, como los ataques de ransomware y los delitos cibernéticos y su impacto en el desarrollo sostenible, destacando la necesidad de tomar decisiones éticas en tecnología para equilibrar el crecimiento económico, la inclusión social y la protección del medio ambiente. Finalmente, se presentan las conclusiones y se formulan recomendaciones para promover la ética en la ciberseguridad y el desarrollo sostenible a nivel organizacional y societal.

**Palabras clave:** Desarrollo sostenible; Educación en ciberseguridad; Ética profesional; Protección de datos.

## 1. Introduction

In the current stage of the digital era and the widespread adoption of disruptive technologies, cybersecurity has gained renewed relevance. This evolution has also raised a fundamental question that transcends the mere protection of information stored and processed within digital systems: how can ethics and integrity be ensured in an increasingly complex technological landscape? The accelerated pace of technological advancement has generated the need to articulate cybersecurity not only as a technical discipline, but also as an ethical and social responsibility.

In this regard, cybersecurity constitutes a cornerstone for safeguarding information and digital infrastructures. It is commonly defined as the set of practices, technologies, and processes designed to protect computer systems, networks, and data against cyber threats and attacks, playing a critical role in contemporary societies [6]. However, in a globalized environment where information flows across borders and technological dependence is ubiquitous, data protection alone is no longer sufficient to address emerging risks.

Within this context, professional ethics emerges as a moral guide in the field of cybersecurity, promoting the adoption of principles and standards of conduct that extend beyond technical safeguards [2]. In general terms, professional ethics refers to the set of moral principles and values that guide the actions and decisions of professionals in their respective disciplines [38]. In cybersecurity, these ethical principles are essential for ensuring responsible decision-making in the design, deployment, and management of technological solutions.

Ethical conduct in cybersecurity does not arise spontaneously; it is cultivated through education and continuous training. This process is reinforced by the dissemination of clear cybersecurity policies, which together contribute to building a solid ethical foundation capable of ensuring the fundamental attributes of information integrity, confidentiality, and availability. In this sense, ethical awareness becomes crucial, as professional decisions and technological actions entail social, economic, and environmental consequences [19].

At the same time, as technological innovation continues to accelerate, sustainable development has emerged not merely as an objective, but as a global imperative [21]. Sustainable development seeks to ensure that present actions do not compromise the ability of future generations to meet their own needs [41]. At the intersection of professional ethics, cybersecurity education, and sustainable development lies a unique opportunity to foster a safer, more responsible, and more equitable digital future [1].

Accordingly, this article explores the convergence of professional ethics, cybersecurity, and sustainable development, emphasizing their interdependence in contemporary digital societies. This intersection becomes particularly relevant as digital technologies increasingly contribute to addressing environmental, social, and economic challenges. The objective is not only to encourage reflection, but also to outline pathways toward a more ethical, secure, and sustainable digital ecosystem [1].

To facilitate understanding of the scope and organization of this study, the article is structured as follows. Section 2 presents the main contributions of the research. Section 3 describes the methodological approach, including the systematic literature review and qualitative analysis procedures. Section 4 reports and discusses the results derived from the documentary analysis and case studies. Finally, Section 5 summarizes the main findings and highlights their implications for cybersecurity education, professional ethics, and sustainable development.

## 2. Contributions

This research presents the following contributions:

i. A systematic literature review is conducted to analyze the interrelationship between professional ethics, cybersecurity education, and sustainable development, identifying key trends, challenges, and conceptual frameworks relevant to the Colombian and Latin American context.
ii. The role of cybersecurity education is examined as a foundational mechanism for protecting information, fostering digital trust, and preventing cybercrime, highlighting its impact on social inclusion, regulatory compliance, and long-term sustainability.
iii. An ethical perspective on technological decision-making is articulated, emphasizing how professional ethics in cybersecurity contributes to the protection of citizens' rights, corporate responsibility, and the balanced integration of economic growth, social equity, and environmental protection.
iv. A strategic framework is proposed to promote cybersecurity education and professional ethics in Colombia, aligning educational initiatives, public–private collaboration, and regulatory measures with the Sustainable Development Goals (SDGs).

## 3. Methodology

The present study was conducted under a projective and qualitative approach, aimed at formulating a cybersecurity education and professional ethics strategy as a mechanism to promote sustainable development [29]. To ensure methodological rigor, a systematic literature review process was incorporated, following the guidelines proposed by [18] and the principles of the PRISMA framework, adapted for qualitative and documentary research.

The bibliographic review was carried out through exhaustive searches in academic databases and specialized repositories, including Scopus, Web of Science, Google Scholar, SciELO, Redalyc, Dialnet, and Semantic Scholar. Boolean combinations of search terms in Spanish and English related to professional ethics, cybersecurity education, sustainable development, digital governance, and data protection were employed.

The identification process resulted in the retrieval of more than 80 potentially relevant documents. Subsequently, explicit inclusion and exclusion criteria were applied, considering thematic relevance, academic traceability, language (Spanish and English), the currency of sources (with an average publication age of five years), and their applicability to the Colombian and Latin American context. After the screening process, an approximate final corpus of 45 studies was consolidated, serving as the basis for qualitative analysis and the development of the strategic proposal.

The selected studies were characterized using descriptive bibliometric indicators, such as publication time frame, document type, area of knowledge, methodological approach, and geographical context. Finally, data analysis was conducted through thematic analysis, following the guidelines of [5], which enabled the identification of recurring patterns and emerging categories.

The methodological process is described in Table 1.

## 4. Results

This documentary research was supported by an exhaustive bibliographic review encompassing a wide range of academic and professional sources. Several specialized databases were consulted to identify relevant studies on professional ethics, cybersecurity education, and sustainable development.

**Table 1.** Methodological process adopted for the systematic review and qualitative analysis.

| Stage | Description | Main Output |
|---|---|---|
| Identification | Exhaustive search of academic and institutional literature in databases such as Scopus, Web of Science, Google Scholar, SciELO, Redalyc, Dialnet, and Semantic Scholar using boolean combinations of keywords related to professional ethics, cybersecurity education, and sustainable development. | Initial set of more than 80 potentially relevant records |
| Screening | Application of explicit inclusion and exclusion criteria based on thematic relevance, academic traceability, language (Spanish and English), publication date (average of five years), and applicability to the Colombian and Latin American context. | Filtered corpus of approximately 45 selected studies |
| Characterization | Descriptive bibliometric analysis of the selected studies, considering publication time frame, document type, area of knowledge, methodological approach, and geographical context. | Bibliometric profile of the selected literature |
| Qualitative Analysis | Thematic analysis of the selected documents following the guidelines of [5], allowing the identification of patterns, themes, and emerging categories. | Thematic categories and analytical framework |
| Synthesis and Interpretation | Narrative synthesis integrating findings from the systematic review to support the formulation of a cybersecurity education and professional ethics strategy oriented toward sustainable development in Colombia. | Strategic proposal and interpretative conclusions |

Source: The authors.

### *4.1. Information Protection*

Cybersecurity is essential for protecting the integrity, confidentiality, and availability of online information. Personal and corporate data are valuable assets and must be safeguarded against cyber threats. Cybersecurity education helps individuals and organizations understand cyber risks, implement appropriate security measures, and respond effectively to incidents. Data loss or the exposure of confidential information can lead to serious financial and reputational consequences, which in turn may undermine an organization's sustainability [6].

Furthermore, cybersecurity contributes to the creation of online trust, a fundamental element for sustainable development. Commercial transactions, communications, and collaborations depend on confidence in the integrity and security of online systems and data. Cybersecurity education fosters an online environment in which users can trust that their interactions are secure. This is particularly important for the adoption of emerging technologies, such as artificial intelligence and the Internet of Things, which can drive sustainable development in sectors such as healthcare and energy [8].

It is also important to note that collaboration between the public and private sectors is essential for strengthening online trust. Companies bear the responsibility of implementing effective security measures and informing users about data protection practices. At the same time, governments can work with the private sector to establish security standards and share information on cyber threats [11].

Technological innovation likewise plays a crucial role in fostering online trust. The development of advanced technologies for encryption, user authentication, and threat detection enhances the protection of online data and personal information. In addition, advances in artificial intelligence can be leveraged to identify and prevent cyberattacks more efficiently [11].

To further promote online trust, most countries have implemented strict regulations on data protection and cybersecurity. These regulations impose significant obligations on organizations to ensure data privacy and security [32]. Consequently, cybersecurity education and professional ethics are essential to help organizations understand and comply with these regulations, as failure to do so may result in substantial fines and reputational damage [23].

Additionally, cybersecurity education plays a key role in the prevention of cybercrime. Online fraud, identity theft, cyberbullying, and other cyber offenses can have a significant impact on individuals and organizations. Training individuals to recognize warning signs, protect themselves against threats, and report incidents to the appropriate authorities not only protects victims but also contributes to the economic and social sustainability of a nation [22].

A notable example of the importance of cybersecurity education and cybercrime prevention is the WannaCry ransomware attack in May 2017. This attack affected thousands of organizations worldwide, including hospitals, companies, and governments. WannaCry spread by exploiting a vulnerability in unpatched Windows systems. Although Microsoft had released a security patch for this vulnerability months before the attack, many organizations had not applied the update due to a lack of awareness regarding the importance of keeping systems up to date [17].

This incident highlighted the urgent need for broader cybersecurity education. Had organizations and individuals been better informed about the importance of maintaining updated systems and avoiding suspicious files, the spread of WannaCry and its devastating consequences could have been prevented [17].

It is important to emphasize that cybersecurity education not only involves understanding cyber threats and best practices for protection, but also fostering a cybersecurity culture in which all Internet users are aware of risks and take proactive measures to mitigate them. In an increasingly digital world, the prevention of cybercrime through education is essential to ensure online security and the sustainability of our societies [21].

### 4.2. Professional Ethics in the Technological Domain

As expressed by Adela Cortina in an interview, professional ethics refers to the set of norms and moral principles that guide individuals' behavior in their professional practice [3].

Within the technological domain, professional ethics focuses on decision-making related to the ethical development and use of technology. This includes considering the social, environmental, and ethical impacts of technological solutions. Education in this area fosters responsibility and informed decision-making. Moreover, technology professionals must take into account issues such as privacy, algorithmic discrimination, and fairness in the design of systems and applications. Ethical decision-making is essential for sustainable development, as it can prevent unintended and harmful consequences for society and the environment [36].

A concrete example of the importance of professional ethics in technology is the Facebook Inc.Cambridge Analytica scandal in 2018. In this case, the company used Facebook users' data without their consent to influence political elections. This raised serious ethical concerns regarding data privacy, information manipulation, and the misuse of technology to influence democratic processes [40]. This incident illustrates how ethical decisions can have a significant impact on society and underscores the need for technology professionals to carefully consider the ethical implications of their work [4].

### 4.3. Digital Inclusion

It is crucial that cybersecurity education and professional ethics be accessible to everyone, regardless of their level of technological experience. Digital inclusion is closely related to ensuring that all individuals have access to education in these areas. This enables marginalized and disadvantaged communities to benefit from technology in a safe and ethical manner. Digital inclusion is essential for achieving sustainable and inclusive development, as it helps prevent the digital divide and promotes equity in access to technological opportunities.

Moreover, digital inclusion is closely linked to individual empowerment. By providing cybersecurity knowledge, people can navigate cyberspace with confidence and protect their personal and financial data. This not only results in a higher level of online security but also fosters greater participation in the digital economy.

Digital inclusion is not limited to education alone; it also encompasses access to technological infrastructure. Access to high-speed Internet and appropriate devices is fundamental for individuals to fully leverage digital opportunities. Ensuring affordable and reliable connectivity is a core component of digital inclusion, as it facilitates participation in the global economy and access to essential services such as online healthcare and distance education [12].

### *4.4. The Role of Professional Ethics in Promoting Sustainable Development in Colombia*

Once the role of professional ethics in the technological domain has been clearly established, it is important to understand that cybersecurity and professional ethics are inextricably intertwined in today's digital world, with each gaining increasing relevance. This relationship directly affects how organizations and professionals handle information and data, as well as their commitment to sustainable development [14]. Below are some situations in which this interaction becomes evident:

### *4.5. Trust and Sustainable Development*

Trust is a fundamental pillar of sustainability. A lack of confidence in information and data security can have a significant impact on the adoption of digital technologies and the development of the digital economy in Colombia. When citizens and companies do not trust the security of their online data, they become reluctant to use digital services and share personal information, which can limit economic growth and innovation [34].

Professional ethics in cybersecurity implies a commitment to data protection, privacy, and information integrity. When professionals in this field rigorously adhere to a code of ethics that prioritizes these values, a solid foundation of trust is built in cyberspace. This, in turn, can encourage the adoption of digital technologies, foster investment, and promote a healthy and reliable business environment [34].

### *4.6. Protection of Citizens' Rights*

Professional ethics in cybersecurity is also closely linked to the protection of citizens' rights. In an increasingly digital world, access to information and privacy are fundamental rights. Cybersecurity professionals, by adhering to professional ethics, ensure that these rights are not violated. This not only benefits individuals but also supports sustainable development by creating a safe and respectful online environment [20].

### *4.7. Corporate Responsibility*

Companies play a crucial role in sustainable development, and professional ethics in cybersecurity translates into greater corporate responsibility. Organizations that value ethical data management and cybersecurity practices not only protect their assets and reputation but also demonstrate their commitment to society and the environment in which they operate. Promoting high ethical standards in cybersecurity reinforces corporate responsibility in sustainable development and strengthens companies' positive contributions to Colombian society [26].

### *4.8. Corporate Social Responsibility (CSR)*

Corporate Social Responsibility is an additional element that can play a significant role in promoting sustainable development in Colombia within the context of cybersecurity and professional ethics. CSR refers to the practice whereby companies make ethical decisions and take actions that consider not only their economic objectives but also their social and environmental impact.

In relation to cybersecurity and professional ethics, CSR can be manifested in various ways:

i. Investment in Cybersecurity Education: Companies can invest in cybersecurity education programs not only for their employees but also for the broader community. Offering free or affordable workshops and training on online security and ethical best practices can empower individuals and organizations to protect themselves in cyberspace [16].

ii. Collaboration with Civil Society Organizations: Companies can collaborate with civil society organizations focused on promoting cybersecurity and online ethics. Funding projects and campaigns that foster digital security and responsible online behavior can contribute to community well-being and strengthen online trust [31].

iii. Transparency in Data Management: Companies can commit to managing customer and user data in a transparent and ethical manner. This involves not only complying with privacy regulations but also effectively communicating how data are handled and protected against cyber threats [30].

iv. Active Community Engagement: Companies can actively participate in community initiatives that promote online safety and ethical practices. This may include sponsoring cybersecurity awareness events, supporting charitable organizations focused on cybersecurity and sustainable development, or even donating technological resources for educational purposes [24].

v. Setting an Example Through Best Practices: Companies can serve as role models by rigorously adhering to best practices in cybersecurity and professional ethics. This not only protects their assets and reputation but also inspires other organizations to follow an ethical and sustainable path [10].

Corporate Social Responsibility (CSR) is not only about doing good; it also brings tangible business benefits, such as enhancing corporate image, improving customer and employee retention, and building stronger relationships with the community. Ultimately, CSR in the context of cybersecurity and professional ethics can contribute to sustainable development by fostering a culture of responsibility and ethical behavior within both the business environment and society at large [12].

The intersection of professional ethics, cybersecurity, and sustainable development not only raises critical issues but also has a substantial impact on the pursuit of a more sustainable future. As societies become increasingly digitalized and technology continues to improve quality of life, it becomes imperative to strengthen the internalization of ethical values and principles and to identify how these, together with cybersecurity policy practices, influence the sustainable development of a nation [19].

It is important to recall that sustainable development involves achieving a balance between economic growth, social inclusion, and environmental protection. Technology is a powerful tool for advancing these objectives; however, it can also undermine them if it is not used in an ethical and secure manner. A clear example is the production and disposal of obsolete electronic devices, which generates electronic waste and contributes to environmental pollution. Professional ethics within the technology industry should therefore encompass sustainable production practices, the promotion of reuse and recycling of electronic equipment, and the reduction of the carbon footprint of data centers [19].

Moreover, cybersecurity is essential to ensure that technological advances are not compromised by harmful cyberattacks. Data loss or unauthorized access to critical systems can have a negative economic impact and ultimately undermine efforts toward sustainable development. Ethical cybersecurity involves protecting the digital infrastructure that supports healthcare systems, online education, and government services, thereby ensuring that these pillars of sustainable development are not threatened by insufficient cybersecurity measures [25].

Likewise, professional ethics in cybersecurity advocates for the protection of personal data and individual privacy, which are essential components of sustainable development. Online trust is crucial for encouraging the adoption of technologies that can improve people's lives and reduce inequalities [11]. Security breaches and unethical data collection practices can erode this trust and hinder progress toward a more sustainable future.

### *4.9. Professional Ethics and Cybersecurity Education: Strengthening Sustainable Development*

The strategy of integrating professional ethics and cybersecurity education within the context of sustainable development represents a highly beneficial and particularly relevant approach to addressing contemporary challenges in the field of cybersecurity. This approach indeed promises numerous benefits at both the individual and societal levels; however, it is also essential to consider its potential drawbacks [27].

The incorporation of professional ethics into the training of cybersecurity experts has a profound impact on professionals' awareness of the ethical implications of their actions. Such training promotes ethical decision-making, fostering personal responsibility and encouraging consideration of the moral dimensions of cybersecurity [27]. Cybersecurity professionals thus become not only guardians of digital security but also advocates for privacy, integrity, and online justice. This helps create a safer and more ethical cyber environment in which the protection of user rights and trust is valued [37].

Furthermore, combining cybersecurity education with sustainable development and professional ethics encourages the acquisition of advanced technical skills, resulting in a highly skilled and globally competitive workforce. These professionals are better equipped to address cybersecurity challenges ethically, effectively, and proactively. This generates benefits for both companies and organizations, as reducing the risk of cyberattacks protects not only digital assets and intellectual property but also ensures operational continuity and customer trust. Moreover, this integration can have a positive impact on the economy by stimulating innovation and secure growth for all citizens [27].

On the other hand, this triad also benefits society as a whole by protecting critical infrastructure, which is essential for well-being and sustainable development. Cybersecurity education promotes awareness and cyber resilience across society, contributing to stability and sustainable economic growth. The security of systems such as healthcare, energy, and finance becomes a fundamental pillar of quality of life and overall prosperity [15].

Nevertheless, it is important to acknowledge that the implementation of this strategy is not without challenges. It requires significant investment in cybersecurity training and education, as well as in the promotion of ethical values [35]. Keeping pace with constantly evolving cyber threats is a continuous and often costly effort. In addition, the integration of ethics and cybersecurity education must be addressed in an appropriate and equitable manner to avoid discrimination and promote inclusion, which may demand additional effort.

In summary, the strategy of integrating professional ethics and cybersecurity education with sustainable development is a valuable initiative that can deliver significant benefits at multiple levels. It promotes ethical responsibility, technical competence, and a safer and more trustworthy digital environment. However, its implementation requires sustained commitment and careful consideration of potential challenges. Ultimately, this strategy represents an essential step toward a more ethical and secure cyberspace, contributing to the advancement of sustainable development and the well-being of society.

### *4.10. Case Studies in Colombia*

In the Colombian context, the need for an effective strategy for cybersecurity education and professional ethics becomes evident through a series of cases that have directly impacted national cybersecurity and data protection. Below are several emblematic examples that underscore the importance of cybersecurity education as a fundamental tool for addressing these challenges:

#### 4.10.1. Petya/NotPetya Ransomware Case (2017)

In 2017, Colombia was not immune to the global spread of the Petya/NotPetya ransomware. This attack affected numerous organizations and companies worldwide, including several in Colombia. The malware encrypted computer systems and demanded ransom payments in Bitcoin for their release, resulting in significant financial losses and reputational damage for national companies. The lack of cybersecurity preparedness highlighted the urgent need for continuous education in this field, which could have enabled organizations to implement adequate security measures and avoid becoming victims of similar attacks [7].

#### 4.10.2. Cybercrime and Financial Fraud

Colombia has witnessed multiple cases of financial fraud and cybercrime, such as phishing scams and identity theft. These practices have directly affected individuals and businesses, leading to significant economic and personal consequences. Cybersecurity education emerges as a necessary shield to empower citizens to recognize warning signs and prevent such fraud, as well as to train financial institutions in the implementation of more effective security measures [42].

#### 4.10.3. Data Breaches in Government Institutions

Data breaches involving sensitive information in Colombian government institutions have raised serious concerns regarding the security of citizens' personal data. Although many of these incidents have not been publicly disclosed, the latent risk to cybersecurity is undeniable. A comprehensive cybersecurity education strategy could have provided government officials and employees with the necessary awareness to understand the importance of safeguarding citizens' data and to implement more robust security measures across governmental networks and systems [13].

#### 4.10.4. Attacks on Critical Infrastructure

Colombia's critical infrastructure has been exposed to threats due to insufficient security measures. Although no large-scale attacks have been officially recorded, the country's vulnerability to such risks persists. Cybersecurity education emerges as a fundamental pillar for protecting critical infrastructure and ensuring the continuity of essential services [9].

#### 4.10.5. Cases of Cyberbullying and Online Abuse

Cyberbullying and online abuse have also affected Colombian citizens. These behaviors, which have a profound impact on victims, highlight the need for cybersecurity education that incorporates aspects of online ethics and cyberbullying prevention. Such education would empower citizens to protect themselves and to report harmful behaviors effectively [23].

These Colombian cases demonstrate that cybersecurity is not merely a theoretical concept but an urgent imperative. Cybersecurity education, as part of a comprehensive strategy, is presented as a vital means to mitigate risks, protect sensitive data, and strengthen the path toward sustainable and secure development in Colombia [23].

### *4.11. Proposal for a Cybersecurity Education and Professional Ethics Strategy to Promote Sustainable Development in Colombia*

Like many other nations, Colombia faces significant challenges related to the promotion of sustainable development, data protection, and cybersecurity. However, implementing an effective strategy for cybersecurity education and professional ethics can be a key factor in addressing these challenges and strengthening the country's path toward a safer and more sustainable future.

**Strategic Steps:**

i. Integrating Cybersecurity Education into the Educational System: Colombia could begin by incorporating cybersecurity and professional ethics into national educational curricula [33]. From primary schools to universities, courses should be offered to teach students about the importance of online security, ethical technology use, and data protection [28].

ii. Continuous Training: In addition to formal education, continuous cybersecurity training programs should be promoted for professionals across different sectors, including businesses, government institutions, and non-profit organizations. Ongoing training would ensure that employees remain up to date with cybersecurity best practices [28].

iii. Public–Private Collaboration: Colombia could follow the example of other countries that have established strong collaborations between the public and private sectors. This involves companies sharing information on cyber threats with the government and working jointly to establish robust security standards [39].

iv. Regulation and Compliance: The implementation of clear and effective privacy and cybersecurity regulations is essential. The government must ensure that laws are kept up to date and that meaningful sanctions are applied in cases of non-compliance. This not only protects citizens but also fosters online trust [22].

### *4.12. Relationship Between the Cybersecurity Education Strategy and the Sustainable Development Goals (SDGs)*

Cybersecurity has evolved beyond being merely a technical protection mechanism; it has become a fundamental pillar for trust and sustainable development. Data protection and online privacy are essential for fostering innovation, economic growth, and social inclusion. By promoting a culture of security and ethics, cybersecurity education plays a crucial role in building more resilient and equitable societies.

Colombia, like many other countries, has faced a range of cybersecurity challenges, including ransomware attacks and data breaches involving sensitive information. These incidents have highlighted the urgent need to strengthen cybersecurity education at all levels. By training citizens and organizations, resilience against cyber threats can be enhanced, and national interests can be better protected.

Cybersecurity education is a key catalyst for achieving the Sustainable Development Goals (SDGs). By fostering trust in digital technologies, it stimulates innovation and economic growth. Furthermore, cybersecurity education helps protect critical infrastructure, ensure the security of personal data, and promote digital inclusion. In this sense, cybersecurity becomes a fundamental pillar for building more just, equitable, and sustainable societies (Table 2).

**Table 2.** Relationship between Cybersecurity Education Strategy and the SDGs

| **Cybersecurity Education Strategy** | **Related SDGs** |
|---|---|
| Integrating cybersecurity into the educational curriculum | SDG 4: Quality education; SDG 9: Industry, innovation and infrastructure |
| Continuous training for professionals | SDG 8: Decent work and economic growth; SDG 9: Industry, innovation and infrastructure |
| Public–private collaboration | SDG 17: Partnerships for the goals |
| Regulation and compliance | SDG 16: Peace, justice and strong institutions |

Source: The authors.

## 5. Conclusions

In conclusion, this study highlights the crucial intersection between professional ethics and cybersecurity education within the context of sustainable development. In an increasingly technology dependent world, protecting online information and fostering trust in the digital environment are fundamental. Moreover, ethical decision-making in technology has become essential to prevent scandals and to address the social and environmental impacts associated with technological advancement.

The strategy of promoting cybersecurity education and professional ethics in Colombia serves as an inspiring example of how a country can address specific cybersecurity challenges while advancing toward a safer future. Collaboration between the public and private sectors, effective regulation, and corporate responsibility are key elements in achieving this objective.

Ultimately, this strategy not only contributes to enhanced online security but also represents a significant step toward sustainable development. Ethics in technology and cybersecurity serve as pillars for balancing economic growth with social inclusion and environmental protection. This approach not only benefits Colombia but can also serve as a model for other countries seeking a safer and more sustainable future in the digital era. Education and ethics are the tools through which a more trustworthy and ethical online world can be built, thereby driving sustainable development on a global scale.

Furthermore, this discussion underscores the impact that professional ethics and cybersecurity have on sustainable development, recognizing that ethical decisions and cybersecurity practices have significant consequences across areas ranging from environmental protection to the promotion of social equality and economic growth. The adoption of ethical practices and investment in cybersecurity are not only imperative from a business perspective but are also fundamental to achieving the United Nations Sustainable Development Goals and to building a more sustainable future for generations to come.

**Author Contributions: Ledesma, J.:** Writing – original draft, Supervision, Project administration, Funding acquisition. **De Los Ríos, E.:** Conceptualization, Methodology, Data curation. **Villanueva, J.:** Software, Visualization, Validation, Formal analysis. **Pérez, M.:** Investigation, Resources, Writing – review & editing.
All authors have read and agreed to the published version of the manuscript. Refer to the taxonomía CRediT for term explanations. Authorship should be limited to those who have contributed substantially to the work reported.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable, since the present study does not involvehuman personnel or animals.

**Informed Consent Statement:** This study is limited to the use of technological resources, so nohuman personnel or animals are involved.

**Conflicts of Interest:** Under the authorship of this research, it is declared that there is no conflict of interest with the present research.

## References

1. Alcalá-del Olmo, M. J. and Gutiérrez-Sánchez, J. D. (2019). El desarrollo sostenible como reto pedagógico de la universidad del siglo xxi. *ANDULI. Revista Andaluza de Ciencias Sociales*, (19):59–80.
2. Aldeco-Pérez, R., Gallegos-García, G., and Rodríguez-Henríquez, L. M. (2020). *Introducción a la Ciberseguridad y sus aplicaciones en México*. Academia Mexicana de Computación, A. C.
3. Asociación Editorial Bruño (2014). B-conferencia - Ética profesional (adela cortina). YouTube.
4. Bilbao, G., Fuentes, J., and Guibert, J. M. (2006). *Ética para ingenieros*. Desclée De Brouwer, Sevilla.
5. Braun, V. and Clarke, V. (2006). Uso del análisis temático en psicología. *Qualitative Research in Psychology*, 3(2):77–101.
6. Cisco (s.f.). ¿qué es la ciberseguridad? Recuperado el 27 de octubre de 2023.
7. Cloudflare (s.f.). ¿qué son petya y notpetya? | ataques de ransomware. Recuperado el 24 de octubre de 2023.
8. Díaz, N., Lozano, L., and Castaño, C. (2016). Implicación de la confianza en la sostenibilidad empresarial. *Inquietud Empresarial*, 16(1):83–114.
9. Díaz-Ardila, and Mendoza-Villamil, P. J. (2019). Ataques informáticos a la infraestructura crítica del sector eléctrico colombiano. Trabajo de grado, Especialización en Seguridad Informática.
10. Escuela Europea de Excelencia (2020). 10 mejores prácticas de ciberseguridad para las organizaciones.
11. Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (s.f.). Programa de fomento de la confianza. Recuperado el 24 de octubre de 2023.
12. Flores-Díaz, F. M. (2022). La responsabilidad social corporativa según los informes de sostenibilidad: Caso iberdrola.
13. Fung, B. (2021). La filtración de datos expone decenas de millones de registros privados de empresas y agencias gubernamentales.
14. Gil, C. (2015). El desarrollo sustentable y análisis de su impacto en los códigos de ética de ingeniería en dos países latinoamericanos. *Provincia*, (34):11–24.
15. González-Zamar, M. d. D. and Abad-Segura, E. (2022). Creatividad y educación artística para la transformación digital sostenible en la educación superior. *Revista FACES*, 3(1):130–146.
16. Impulso_06 (s.f.). La importancia de la educación en ciberseguridad. Recuperado el 23 de octubre de 2023.
17. Kaspersky (s.f.). ¿qué es el ransomware wannacry? Recuperado el 27 de octubre de 2023.
18. Kitchenham, B. (2004). *Procedimientos para realizar revisiones sistemáticas*. Keele University, Keele, Staffordshire, Reino Unido.
19. Longueira-Matos, S., Bautista-Cerro, M. J., and Rodríguez-Hernández, J. A. (2018). Educación en la sociedad del conocimiento y desarrollo sostenible: Xxxvii seminario interuniversitario de teoría de la educación.
20. Mendoza, M. (2016). Ética, el factor humano más importante en el ámbito de la ciberseguridad.
21. Miguel-de Santos, M. (2020). Monográfico: La ciberseguridad, una cuestión que nos incumbe a todos. *Boletic*, (87):53–59.
22. Ministerio de Tecnologías de la Información y Comunicaciones de Colombia (2016). Guía no. 2 elaboración de la política general de seguridad y privacidad de la información.
23. Ministerio de Tecnologías de la Información y Comunicaciones de Colombia (2022). Violencia digital de género, historias reales y lecciones contundentes.
24. Ministerio de Tecnologías de la Información y Comunicaciones de Colombia (s.f.). Modelo de seguridad y privacidad de la información. Recuperado el 21 de octubre de 2023.

25. Morales-Carrillo, J. J., Avellán-Zambrano, N., Mera-Cantos, J. S., and Zambrano-Bravo, M. (2019). Ciberseguridad y su aplicación en las instituciones de educación superior. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (20):438–448.
26. Navarro-Romero, M. A. and Rojas-Cruz, A. C. (2020). Objetivos de desarrollo sostenible en colombia. Trabajo de grado, Programa de Economía, Especialización en Administración Financiera, Bogotá, Colombia.
27. Olcott Jr., D., Carrera Farran, X., Gallardo Echenique, E. E., and González Martínez, J. (2015). Ética y educación en la era digital: perspectivas globales y estrategias para la transformación local en cataluña. *RUSC. Universities and Knowledge Society Journal*, 12(2):59–72.
28. Organización de los Estados Americanos (2020). Educación en ciberseguridad: Planificación del futuro mediante el desarrollo de la fuerza laboral.
29. Ortega, C. (s.f.). Técnicas proyectivas: Qué son, características y ventajas. Recuperado el 21 de octubre de 2023.
30. Osores, M. (2014). Transparencia en el manejo de datos: Esencial para empresas y gobiernos.
31. Pastor-Acosta, and Martínez-Herráiz, J. J. (2017). Capacitación profesional y formación especializada en ciberseguridad. *Cuadernos de Estrategia*, (185):291–350.
32. Piñar-Mañas, J. L. (2016). *Reglamento General de Protección de Datos*. Editorial Reus, Madrid, España.
33. Plaza-de-la Hoz, J. (2018). Cómo mejorar el papel de las tic para promover una educación empoderadora en el desarrollo sostenible. *Aloma: Revista de Psicologia, Ciències de l'Educació i de l'Esport*, 36(2):43–55.
34. Portal Colombia Aprende (s.f.). Confianza digital: Generación digital segura. Recuperado el 27 de octubre de 2023.
35. Pérez-García, M. R. (2014). Ingeniería del agua. *Ingeniería del Agua*, 18(1):ix.
36. Sarango-Aguirre, J. and Quishpe-Gaibor, J. S. (2018). Aplicación de la ética en el uso de la tecnología para la educación. *Revista Caribeña de Ciencias Sociales*.
37. Silva, N. and Espina, J. (2006). Ética informática en la sociedad de la información. *Revista Venezolana de Gerencia*, 11(36):559–580.
38. Universidad Técnica Nacional (s.f.). Objeto virtual de aprendizaje Ética profesional: Conceptos y definiciones. Recuperado el 27 de octubre de 2023.
39. Vega, J. (2023). Gobernanza público-privada de la ciberseguridad en américa latina: Momento agridulce.
40. Vercelli, A. (2018). La (des)protección de los datos personales: Análisis del caso facebook inc. - cambridge analytica. XVIII Simposio Argentino de Informática y Derecho (SID) - JAIIO 47, CABA.
41. Zarta-Ávila, P. (2018). La sustentabilidad o sostenibilidad: Un concepto poderoso para la humanidad. *Tabula Rasa*, (28):409–423.
42. Álvarez, C. (2023). Colombia registró un crecimiento de ataques informáticos en el Último año.

## Authors' Biography

**Marena Vitola Quintero** Systems Engineer, Specialist in Telecommunications, and Master's degree holder in Project Design, Management, and Direction.

**Isaac Yamith Guzmán Paternina** Student at the Corporación Universitaria Rafael Nuñez.

**Ulises Herrera Bustillo** Student at the Corporación Universitaria Rafael Nuñez.

**Disclaimer/Editor's Note:** Statements, opinions, and data contained in all publications are solely those of the individual authors and contributors and not of the OnBoard Knowledge Journal and/or the editor(s), disclaiming any responsibility for any injury to persons or property resulting from any ideas, methods, instructions, or products referred to in the content.