https://repository.uaeh.edu.mx/revistas/index.php/jas/issue/archive

Journal of Administrative Science

Biannual Publication, Vol. 7, No. 13 (2025) 12-15

ISSN: 2683-2119

Cybersecurity: an emerging topic for tourism professional training

La ciberseguridad un tema emergente para la formación profesional turística

Nancy Testón Franco [a], Cristopher Antonio Muñoz Ibáñez [b.]

Abstract:

Cybersecurity is a growing challenge in the digital era, particularly in the tourism sector, where technology plays a pivotal role in developing smart destinations. This essay examines how higher education institutions offering tourism programs must adapt to prepare future professionals for security challenges. The aim is to identify professionalization needs in the tourism sector, focusing on cybersecurity. Emphasizing the importance of continuous updates security, both in academic training and professional practice, ensures graduates are equipped to address the demands of future tourism, where technology and digital security are fundamental components.

Keywords:

Cybersecurity, Tourism professionalization, Higher education

Resumen:

La ciberseguridad es un desafío creciente en la era digital, especialmente en el sector turístico, donde la tecnología juega un papel clave en la creación de destinos inteligentes. Este ensayo explora cómo las instituciones de educación superior con programas en turismo deben adaptarse para preparar a los futuros profesionales ante los retos de la seguridad. El objetivo es identificar las necesidades de profesionalización en el sector turístico, con un enfoque en ciberseguridad. Se destaca la importancia de la actualización constante en temas de seguridad en la industria, tanto en la formación académica como en la práctica profesional, para garantizar que los egresados estén preparados para enfrentar los desafíos del turismo del futuro

***Palabras Clave**:*

Ciberseguridad, Profesionalización turística, Educación superior

Introduction

Tourism has undergone significant transformation in recent decades, driven by technological advances that have enabled more personalized, efficient, and accessible experiences. The emergence of smart destinations, extensive use of Big Data, and the integration of technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT) have redefined how tourists plan and enjoy their trips and how destinations are managed. These innovations have enhanced sustainability, mobility, and traveller interaction, making technology a cornerstone of the sector. However, these advancements have also introduced new risks, with cybersecurity becoming one of the most pressing challenges today.

The increasing use of personal and financial data, coupled with reliance on complex technological infrastructures, makes tourism an attractive target for attacks and breaches. Protecting sensitive information, both for tourists and operators, has become an urgent priority, highlighting the need for future tourism professionals to receive robust training in cybersecurity. Higher education institutions offering tourism programs must recognize this new landscape and adapt to ensure their graduates are prepared to tackle the challenges posed by the sector's growing digitalization.

This research aims to identify professionalization needs in the tourism sector, focusing on cybersecurity. It underscores the importance of equipping tourism students not only with management and operational knowledge but

[a] Corresponding Author, Universidad Autónoma del Estado de Hidalgo | ICEA | Pachuca, Hidalgo | México, https://orcid.org/0000-0003-3043-5294, Email: nteston@uaeh.edu.mx

[b] Universidad Autónoma del Estado de Hidalgo | ICEA | Pachuca, Hidalgo | México, https://orcid.org/0000-0002-3088-2599, Email: cristopher_antonio@hotmail.com

Received: 21/11/2024, Accepted: 26/11/2024, Published: 05/07/2025

DOI: https://doi.org/10.29057/jas.v6i12.14268.

also with insights into emerging technologies and their associated risks. Specifically, it emphasizes the need to integrate cybersecurity competencies into educational programs, enabling future professionals to respond effectively to the challenges of future tourism. Such preparation is crucial to maintaining trust in tourism services and ensuring the sector's long-term sustainability in an increasingly technology-dependent world.

The Need to Integrate Cybersecurity into Tourism Education

The digitalization of the tourism sector necessitates adapting professional training to address emerging challenges, particularly those related to cybersecurity. With the rise of smart destinations and widespread adoption of digital technologies, risks associated with data protection and system integrity have become critically important [1]. Various studies indicate a growing number of cyberattacks in tourism, impacting both businesses and travellers [2]. Consequently, tourism academic programs must incorporate content addressing digital vulnerabilities and best practices in cybersecurity. Failure to prepare professionals in this area could undermine industry trust, affecting its growth and sustainability in the long term [3].

Digitalization has profoundly revolutionized the industry, improving operations management, enhancing customer experiences, and promoting the creation of smart destinations. Technologies like Big Data, AI, and IoT have enabled greater personalization, improved decision-making, and optimized resource utilization [4]. However, these advancements have also exposed the industry to new cyber risks. The reliance on interconnected systems and the handling of significant volumes of personal and financial data on digital platforms—ranging from reservations to transactions—have increased web vulnerabilities [5].

For example, online booking platforms and hotel management systems are attractive targets for cybercriminals seeking to exploit security gaps to access sensitive information [6]. The growth of smart destinations, integrating interconnected technologies to improve mobility, sustainability, and tourist experiences, has further heightened cybersecurity risks [7]. While digitalization has facilitated a more efficient and competitive industry, it demands constant attention to security. Tourism professionals must be prepared to recognize and mitigate these risks, as any digital security breach can erode consumer trust and damage a company’s reputation.

Recent incidents highlight the significant impact of cyberattacks on businesses' reputations and customer trust. In 2018, British Airways suffered a breach compromising the financial data of 380,000 customers, resulting in hefty fines and reputational damage [8]. Similarly, the ransomware attack on TravelClick disrupted booking systems for several hotels, underscoring the fragility of technological services in the industry and their severe operational repercussions [9]. These examples underline the urgent need to strengthen cybersecurity in tourism through interdisciplinary collaboration to protect both businesses and consumers (see Table 1).

Table1. The Importance of Integrating Cybersecurity into Tourism Professionalization

Aspect	Importance in tourism professionalization	Examples/Impact
Data protection	Safeguards sensitive customer information such as payment details and personal data.	Prevents identity theft and financial fraud.
Reputation management	Ensures trust in tourism organizations by preventing data breaches.	Maintains customer confidence and brand loyalty.
Operational continuity	Protects systems from cyberattacks that can disrupt operations.	Prevents booking system outages and delays in customer services.
Regulatory compliance	Aligns with laws like GDPR or CCPA to avoid penalties and legal issues.	Reduces risks of fines and lawsuits.
Trust in smart destinations	Encourages adoption of digital tools in tourism while ensuring their security.	Enhances the appeal of tech-driven, secure travel experiences.
Risk mitigation	Identifies and reduces vulnerabilities to minimize potential damages.	Lowers the cost of recovery and risk of cyber incidents.
Innovation support	Promotes the safe integration of advanced technologies like AI and IoT in tourism.	Enables innovation without compromising security.
Global competitiveness	Ensures that tourism professionals meet international security standards.	Attracts international partnerships and collaborations.

Source: Own elaboration

Challenges in Academic Technology Training for Tourism

Cybersecurity has become a critical component of tourism professional training in an era of growing digitalization. Higher education institutions must recognize that preparing students for cybersecurity challenges involves more than teaching technical tools; it requires developing a deep understanding of data management and client information protection. This necessitates incorporating specific courses on cybersecurity into tourism academic

programs and fostering collaborations with experts to enrich curricula.

Studies have emphasized the importance of integrating cybersecurity competencies into tourism education to align with the increasing reliance on digital platforms and data systems in the sector [10]. Future professionals must acquire competencies in identifying and mitigating cyber risks and managing crises during incidents. These skills not only enhance student preparedness but also contribute to fostering a culture of security in the tourism sector. Reflecting on this topic, cybersecurity must be considered an essential, not supplementary, element in training future tourism professionals. The ability to adapt to and address cyber threats will be a key differentiator for tourism companies and their employees, strengthening client trust and ensuring sustainable development in the sector [11].

While cybersecurity is becoming a critical concern in the tourism industry, it is vital to analyses gaps in current tourism education programs. Many were designed before the digitalization boom, resulting in insufficient focus on cybersecurity and data management. According to Török & Barta [12], tourism curricula often lack modules directly addressing information security, leaving graduates unprepared for contemporary challenges in the sector. This gap has been further highlighted by Díaz-Fernández et al. [13], who argue that digital skills, including cybersecurity, are essential for maintaining competitive advantages and meeting consumer expectations in an increasingly technology-driven industry.

Strategies for Cybersecurity Training in Tourism

To address the challenges that cybersecurity poses to the tourism sector, it is essential for higher education institutions to develop training strategies that equip future professionals with the necessary skills. A key strategy is the inclusion of specialized cybersecurity courses within the curricula of undergraduate and graduate tourism programs. These courses should address not only the theoretical foundations of digital security but also provide practical training in the use of technological tools and the implementation of security protocols [14]. Additionally, establishing partnerships with industry experts and technology companies is recommended, enabling students to become familiar with the latest risks and learn how to address them in real-world scenarios [15]. Furthermore, simulating cyberattacks and resolving crises should be part of practical training, fostering the ability to respond immediately to critical situations. These strategies not only strengthen students' technical competencies but also promote a security culture that will be crucial for tourism.

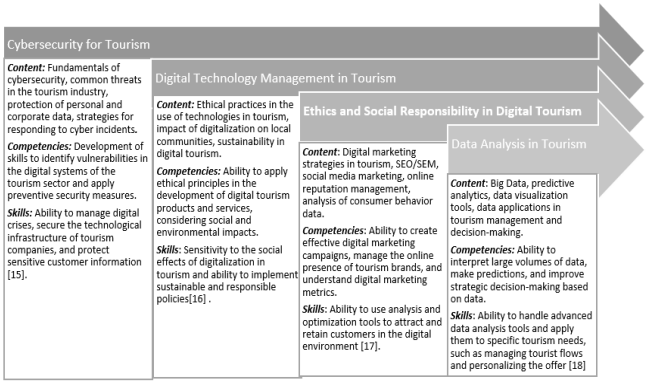
The integration of cybersecurity into tourism academic programs on a transversal level is an urgent necessity given the sector's increasing digitalization. To this end, it is crucial to develop curricula that not only offer specialized cybersecurity courses but also embed this knowledge into traditional subjects such as hotel management, digital marketing, and tourism administration. According to Lehto & Wang [16], an effective strategy involves introducing cybersecurity modules during the first semesters of undergraduate programs, allowing students to gain a foundational understanding early in their education. Moreover, in advanced stages, optional courses addressing emerging technologies and cutting-edge security protocols, such as data protection and cyber incident management, should be provided [17].

These measures will ensure that graduates possess not only managerial and operational knowledge but also the technical skills required to mitigate the risks associated with digitalization. This comprehensive approach will prepare professionals who are capable of protecting the industry from potential threats while simultaneously enhancing its resilience and competitiveness in an increasingly digital landscape.

Proposed subjects and content for tourism professionalization in the digital era

Tourism professionalization must be aligned with technological advancements and the current challenges of the sector, including cybersecurity and adaptation to new digital management methods. Aimed at training competent professionals in a globalized and digital environment, the proposed subjects cover both traditional aspects of tourism and emerging competencies related to digital transformation and cybersecurity (see Graphic 1).

Graphic 1. Proposed subjects and content for tourism professionalization in the digital era.



Source: Own elaboration

The integration of cybersecurity and digital technologies in tourism education is essential to meet the challenges of the rapidly evolving digital landscape. As the tourism industry continues to embrace innovation, it is crucial that academic programs evolve to equip future professionals with the skills necessary to navigate these new realities.

By incorporating subjects like cybersecurity, digital marketing, and data analytics, educational institutions can ensure that tourism professionals are prepared not only to protect sensitive information but also to enhance the customer experience in a secure and ethical manner. This proactive approach will strengthen the tourism sector, enabling it to thrive in the digital age while maintaining the trust and safety of both businesses and consumers.

Conclusions

The growing digital transformation in the tourism industry has brought significant benefits in terms of operational efficiency, personalization, and destination management. However, it has also exposed the sector to new risks, with cybersecurity standing out as one of the most pressing challenges. Addressing these risks is not only a necessity for businesses but also for higher education institutions tasked with training future professionals.

The analysis conducted in this essay underscores the urgent need for integrating cybersecurity into tourism education. This integration involves updating curricula to include technical and theoretical aspects of digital security, fostering collaborations with industry experts, and providing students with hands-on experience in managing cyber risks. By doing so, tourism professionals will be better equipped to safeguard sensitive data and maintain consumer trust, which are essential for the long-term sustainability of the sector.

Such that, cybersecurity must be considered a fundamental element of the tourism professionalization process. The inclusion of this topic in educational programs will not only enhance the preparedness of graduates but also ensure that the tourism industry can thrive in a secure and resilient manner. Strengthening cybersecurity competencies is not merely a response to current challenges but a proactive step towards a sustainable future for the tourism sector.

References

[1] Gretzel, U., Sigala, M., & Koo, C. (2020). Smart tourism: Foundations and developments. Electronic Markets, 30(2), 161-172. https://doi.org/10.1007/s12525-020-00425-3

[2] Khan, F., Sadiq, M., Chang, Y., & Feng, Y. (2022). Cybersecurity in the tourism industry: Threats, impacts, and preventive measures. Tourism Management Perspectives, 42, 100956. https://doi.org/10.1016/j.tmp.2021.100956

[3] Buhalis, D. (2021). Smart tourism: Harnessing data and technology for the future of tourism. Journal of Tourism Futures, 7(3), 244-260. https://doi.org/10.1108/JTF-12-2019-0159

[4] Neidhardt, J., Werthner, H., & Wöber, K. (2017). Digital ecosystems in tourism. Tourism Management, 65, 348-362. https://doi.org/10.1016/j.tourman.2017.09.010

[5] Luo, J., & Bu, W. (2021). The impact of cybersecurity on the tourism industry: Vulnerabilities and solutions. Journal of Travel & Tourism Marketing, 38(5), 469-482. https://doi.org/10.1080/10548408.2021.1907673

[6] Tussyadiah, I. P., & Wang, D. (2016). Tourists' perceptions of risk and technology adoption: The case of travel planning. Journal of Travel Research, 55(7), 883-898. https://doi.org/10.1177/0047287515588723

[7] Shafiee, M., & Zegordi, S. (2020). Smart tourism and cybersecurity: Risks in the era of interconnected services. International Journal of Tourism Research, 22(4), 432-446. https://doi.org/10.1002/jtr.2341

[8] Griffin, A. (2019). British Airways fined record £183m for data breach affecting 380,000 customers. The Independent. https://www.independent.co.uk

[9] Frost, R. (2019). The impact of ransomware attacks on the hospitality sector: A case study of TravelClick. Cybersecurity Review, 7(2), 118-125. https://doi.org/10.1080/00000000.2019.120001

[10] Ivanov, S., & Webster, C. (2019). Adoption of robots, artificial intelligence, and service automation by travel, tourism, and hospitality companies – A cost-benefit analysis. International Journal of Contemporary Hospitality Management, 31(6), 2567-2585. https://doi.org/10.1108/IJCHM-11-2018-0925

[11] De Bruyn, A., Visser, G., & Olver, C. (2022). Cybersecurity readiness in tourism organizations: An exploratory study. Journal of Sustainable Tourism, 30(5), 915-933. https://doi.org/10.1080/09669582.2022.2056783

[12] Török, L., & Barta, G. (2020). Tourism education and digital transformation: Preparing students for the future. Tourism Economics, 26(8), 1299-1313. https://doi.org/10.1177/1354816619888671

[13] Beuran, R., Tang, D., & Pham, C. (2021). Cybersecurity education for tourism: Developing practical skills through simulation-based training. Journal of Tourism and Hospitality Education, 9(2), 45-58. https://doi.org/10.1007/s40593-020-00234-5

[14] Chen, Y. (2020). Collaborative learning in cybersecurity education: Partnerships between academia and industry in tourism training. Journal of Hospitality and Tourism Technology, 11(4), 321-334. https://doi.org/10.1108/JHTT-05-2020-0068

[15] Díaz-Fernández, M., López-Cruz, M., & Serrano-Sánchez, J. L. (2021). Digital skills for tourism graduates: Preparing for the industry's future needs. Tourism Management Perspectives, 38, 100821. https://doi.org/10.1016/j.tmp.2020.100821

[16] Lehto, X. Y., & Wang, Y. (2021). Cybersecurity in hospitality education: Integrating risk management in tourism curricula. Journal of Hospitality, Leisure, Sport & Tourism Education, 28, 100318. https://doi.org/10.1016/j.jhlste.2021.100318

[17] Huang, Y., & Kao, W. (2020). Enhancing cybersecurity education in tourism through interdisciplinary collaboration. Journal of Tourism and Hospitality Management, 8(3), 209-225. https://doi.org/10.15640/jthm.v8n3a18