Aurum
EDITORA

CYBERSECURITY IN THE INFORMATION AGE:

Challenges, Strategies, and Perspectives for Data Protection in Digital Environments

DAVID AGUIAR

Aurum
EDITORA

CYBERSECURITY IN THE INFORMATION AGE:

Challenges, Strategies, and Perspectives for Data Protection in Digital Environments

DAVID AGUIAR

AURUM EDITORA LTDA - 2025
Curitiba – Paraná - Brasil

EDITOR-IN-CHIEF
Lucas Gabriel Vieira Ewers

AUTHOR OF THE BOOK
David Aguiar

TEXT EDITING
Stefanie Vitoria Garcia de Bastos

ART EDITION
Aurum Editora Ltda

COVER IMAGES
Freepik, Canva.

LIBRARIAN
Aline Graziele Benitez

AREA OF KNOWLEDGE
Education Sciences

The author is solely responsible for the content, accuracy, and veracity of the data presented in this text, which does not necessarily reflect the official position of the Publisher. The work may be downloaded and shared, provided that credit is given to the author, but modification of the content in any way or its use for commercial purposes is not permitted.

All manuscripts underwent a blind peer review by members of the Editorial Board and were approved for publication based on criteria of impartiality and academic objectivity.

Aurum Editora is committed to maintaining editorial integrity at all stages of the publication process, preventing plagiarism, fraudulent data or results, and ensuring that financial interests do not affect the ethical standards of the publication. Any suspicion of scientific misconduct will be investigated with attention to ethical and academic principles.

International Cataloguing in Publication (CIP) Data (Brazilian Book Chamber, São Paulo, Brazil)

Aguiar, David
Cybersecurity in the information age [e-book] : challenges, strategies, and perspectives for data protection in digital environments / David Aguiar ; [translation Daniel Rodrigues da Silva]. -- 1. ed. -- Curitiba, PR : Aurum Editora, 2025.
PDF

Original title: Cybersecurity in the Information Age : challenges, strategies, and perspectives for data protection in digital environments.
ISBN 978-65-83849-30-4

1. Computer science 2. Cybernetics - Security measures 3. Digital culture 4. Internet - Security measures 5. Protection of personal data 6. Data protection - Legislation - Brazil 7. Information society - Legal aspects 8. Technology I. Title.

25-317437.0 CDD-005.8

Indexes for systematic catalog:

Internet: Security measures: Computer science 005.8

Aline Graziele Benitez - Librarian - CRB-1/3129

DOI: 10.63330/livroautoral182025-

Aurum Editora Ltda
CNPJ: 589029480001-12
contato@aurumeditora.com
(41) 98792-9544
Curitiba - Paraná

AUTHOR

David Aguiar
He holds a degree in Information Technology Management from the Estácio de São Paulo University Center (2017), a degree in Public Safety Management from the Faveni University Center (2025), and a Bachelor's Degree in Theology from the Kerygma Bible Institute (2021). He holds a master's degree in Computer Science and Knowledge Management from Universidade Paulista (2021), with a master's and doctorate in Theology from the Peniel Theological Seminary (2025). He works mainly in the following areas: data protection, prevention, evangelism, Christianity, and society. He holds an honorary doctorate in Evangelism, awarded for his merit and recognition in the field.
Lattes: http://lattes.cnpq.br/7762455825681361

ABSTRACT

This study aims to analyze the challenges, strategies, and future perspectives of cybersecurity in the information age, considering the impact of digital transformation, the evolution of cyber threats, and the need for data protection in digital environments. With the advancement of information technologies such as cloud computing, the Internet of Things (IoT), blockchain, and artificial intelligence, the cybersecurity landscape has become increasingly complex, demanding new approaches to governance and risk management. This research, of a qualitative and exploratory nature, was conducted through bibliographic and documentary review based on authors such as Stallings (2019), Dhillon (2021), Whitman and Mattord (2022), and Silveira, Lunardi and Cerqueira (2023), among others. The analysis revealed that effective information protection depends on the integration of technology, legislation, and organizational culture. International standards such as ISO/IEC 27001, NIST, and COBIT, along with legal frameworks like the Brazilian General Data Protection Law (Law No. 13.709/2018) and the European Union's General Data Protection Regulation (GDPR), constitute essential pillars for strengthening informational security. It was also found that the application of Artificial Intelligence and Machine Learning represents a significant advancement in threat detection and prevention but also raises ethical challenges related to algorithmic transparency and control. The study concludes that cybersecurity is a continuous and multidimensional process that requires innovation, responsibility, and global cooperation to ensure data protection and the sustainability of the digital society.

Keywords: Cybersecurity; Data protection; Artificial intelligence; Machine learning; Digital governance.

DEDICATION

I dedicate this work to my children, Luke and Emma, who are the reason for my daily efforts and the inexhaustible source of love and inspiration. May this work serve as an example that with faith, perseverance, and dedication, it is possible to turn dreams into reality.

ACKNOWLEDGMENTS

I first thank God for the wisdom, strength, and serenity granted at every moment of this journey. Without His constant presence, none of this would be possible.

To my family, who always believed in me and stood by my side during the most challenging days. Especially to my dear wife Gabriela, my faithful companion, whose love, patience, and encouragement were essential for me to reach this point.

To my friends, for their sincere friendship, words of support, and the laughter that made the path lighter—especially Reinaldo Thomé, for his partnership and companionship at all times.

To the professionals in the field of technology, who inspired me with their knowledge and dedication. And in a very special way to Dr. Rosângela Thomé, for her generosity in sharing knowledge and her tireless willingness to help others. Her work is an example of humanity and professionalism.

To all who, directly or indirectly, contributed to the realization of this dream, I extend my deepest gratitude.

David Aguiar

SUMMARY

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

AI – Artificial Intelligence
ML – Machine Learning
ANPD – National Data Protection Authority
CCPA – California Consumer Privacy Act
CIA – Central Intelligence Agency
COBIT – Control Objectives for Information and Related Technologies
DDoS – Distributed Denial of Service (Distributed Denial of Service Attack)
DPO – Data Protection Officer (Data Protection Officer)
ENISA – European Union Agency for Cybersecurity
GDPR – General Data Protection Regulation (European Union General Data Protection Regulation)
HIPAA – Health Insurance Portability and Accountability Act
IA – Artificial Intelligence
IDS – Intrusion Detection System (Intrusion Detection System)
IEC – International Electrotechnical Commission
IoT – Internet of Things
IPS – Intrusion Prevention System (Intrusion Prevention System)
ISACA – Information Systems Audit and Control Association
ISO – International Organization for Standardization
LGPD – General Data Protection Law
MFA – Multi-Factor Authentication
MLP – Multi-Layer Perceptron
NIST – National Institute of Standards and Technology
OECD – Organization for Economic Cooperation and Development
PDCA – Plan-Do-Check-Act
PNCiber – National Cybersecurity Policy
RNA – Artificial Neural Networks
ISMS – Information Security Management System
SNCiber – National Cybersecurity System
SVM – Support Vector Machines
TDS – Traffic Distribution System

Technological advancement and the digital transformation of recent decades have profoundly redefined the way society communicates, produces, and shares information. The growing dependence on interconnected systems, the proliferation of smart devices, and the expansion of internet usage have driven the emergence of new business and management models, but have also increased the vulnerability of organizations and individuals to cyber threats. In this context, cybersecurity has become a central theme of the information age, assuming a strategic role not only in the protection of data and critical infrastructures but also in ensuring privacy and maintaining trust in digital environments. Thus, understanding the challenges, strategies, and perspectives related to data protection in virtual environments is essential for the sustainability of human and institutional relationships in an increasingly digitized world.

Several authors emphasize the growing importance of cybersecurity in light of technological transformations. Stallings (2019) observes that the evolution of information systems is directly related to the increasing complexity of threats, requiring more integrated and preventive approaches. For Whitman and Mattord (2022), cybersecurity has ceased to be merely a technical issue and is now understood as a strategic management process involving policies, organizational culture, and social responsibility. Dhillon (2021) argues that true digital protection is only achieved when there is integration between technology, governance, and human behavior, reinforcing the need for a multidimensional approach to the subject. Brazilian authors such as Silveira, Lunardi, and Cerqueira (2023) also highlight that information security depends on the internalization of ethical values and the creation of an organizational culture committed to data protection. In this sense, the contemporary debate on the subject is not limited to the technical sphere but encompasses legal, ethical, and educational dimensions.

The consolidation of specific laws for data processing and protection underscores the relevance of the topic today. In Brazil, the enactment of the General Data Protection Law (Law No. 13.709/2018) represented a historic milestone by establishing principles and guidelines aimed at ensuring privacy and the security of personal information. As pointed out by Almeida and Soares (2022), the LGPD not only regulates data processing within the national territory but also promotes a cultural and institutional shift in how organizations handle information, drawing inspiration from international legislation such as the European Union's General Data Protection Regulation (GDPR). This convergence between legal norms and international security standards, such as ISO/IEC 27001 and the NIST Cybersecurity Framework, has contributed to strengthening information governance and raising the maturity level of organizational practices.

Given this scenario, the present study is guided by the following research problem: How can organizations strengthen their cybersecurity policies in the face of the growing complexity of digital threats and the rapid evolution of information technologies? From this question, the hypothesis was

formulated that effective protection of digital data depends on the integration of three fundamental dimensions: the ethical and intelligent use of emerging technologies, compliance with legal and normative frameworks, and the strengthening of an organizational culture focused on information security and digital responsibility. This hypothesis guides the investigation and supports the critical analysis of cybersecurity strategies adopted in the contemporary context.

The general objective of this study is to analyze the main challenges, strategies, and perspectives of cybersecurity in the information age, considering the technological, legal, and cultural transformations that shape data protection in digital environments. The specific objectives are to identify the most recurrent threats and vulnerabilities associated with new technologies such as cloud computing, the Internet of Things (IoT), and blockchain; to examine the contributions of international standards such as ISO/IEC 27001, NIST, and COBIT to the strengthening of security policies; to evaluate the impact of the LGPD and other related legislation on information governance; and to reflect on the role of education, ethics, and organizational culture as pillars of sustainable cybersecurity.

The justification for this study lies in the urgency of understanding the risks and opportunities that permeate the digital universe. In a reality where information is the main asset of organizations, cybersecurity is no longer optional but has become a strategic necessity. Recent reports from ENISA (2023) and (ISC)² (2022) point to an alarming increase in the number of cyber incidents, data breaches, and ransomware attacks, while also highlighting a global shortage of qualified professionals in the field. These challenges, combined with global technological interdependence, reinforce the need for investment in innovation, education, and regulation. In this sense, this work aims to contribute to the expansion of academic debate on information security, promoting critical reflection on digital protection policies and practices and encouraging the development of strategies that combine technological efficiency, ethical responsibility, and social commitment.

The research was developed through a qualitative and exploratory approach, based on an extensive bibliographic and documentary review. Reference works, scientific articles, national and international legislation, technical reports, and institutional publications addressing information security from multiple perspectives were consulted. This methodology allowed not only for an understanding of the theoretical and practical foundations of the topic but also for an analysis of its evolution and its impacts on organizational and social behavior. The work is structured into five chapters, organized to ensure cohesion and clarity throughout the investigative process. The first chapter presents the topic, objectives, hypotheses, and justification of the study. The second addresses the theoretical foundation, discussing the main concepts and contributions of national and international authors. The third describes the methodological aspects and procedures used in the development of the research. The fourth chapter is dedicated to the analysis and discussion of results, highlighting contemporary cybersecurity strategies and

challenges. Finally, the fifth chapter presents the final considerations, summarizing the conclusions and suggesting directions for future research on the topic.

In this way, the study seeks to contribute to the strengthening of scientific knowledge about cybersecurity, understanding it as an interdisciplinary field that unites technology, law, and human behavior. By reflecting on the challenges and future perspectives, it aims to demonstrate that true digital protection is not limited to the adoption of technological tools but requires critical awareness, ethics, and global cooperation to build a safer, fairer, and more sustainable informational environment.

FUNDAMENTALS OF CYBERSECURITY

Information Security is a relatively recent discipline within human knowledge, but it has gained significant prominence in recent decades due to the exponential growth in technology use. According to Araujo and Ferreira (2009), it is an essential area that requires the development and implementation of effective policies, particularly aimed at protecting the confidentiality of information. The authors propose a practical guide for security policies, classifying information systems into levels of access and control—from the most restricted to the most basic. However, they acknowledge that other principles of information security, such as integrity and availability, still require deeper exploration.

Complementing this perspective, Fontes (2006) emphasizes the role of the user in information security, adopting an organizational approach. He argues that investing in user training and awareness is fundamental, as improper data handling can compromise the entire security structure. His focus on user education aims to ensure responsible information management, thereby promoting a safer digital environment.

In the same vein, CERT.br (Brazilian Center for Studies, Response, and Treatment of Security Incidents) provides practical guidance through its educational booklet on the main risks faced by internet users. The booklet describes common scams, attacks, and vulnerabilities, while also presenting tools and best practices for safe internet use.

Laudon and Laudon (2014) highlight that understanding information systems is vital for strengthening competitive businesses, managing global corporations, and delivering useful services and products. Their work presents information systems in a practical and didactic manner, with real-life examples and an ethical approach, emphasizing the importance of privacy and digital security in the business context.

Spyman (2000) addresses a controversial yet necessary topic: the emergence of hackers and the vulnerability of companies and users connected to the internet. In Complete Hacker Millennium Manual, the author introduces key names and terminologies from the hacker universe, explaining their motivations, methods, and how to avoid them. The book also provides an introduction to programs and scripts available online, showing how they can be used offensively or defensively.

From a legal standpoint, Clough (2010) analyzes the principles of cybercrime from the perspective of different jurisdictions—Australia, Canada, the United Kingdom, and the United States. His work is a landmark for those seeking to understand the legal and investigative challenges related to cybercrime, offering practical examples and comparative analyses of legal systems.

In this context, Gragido et al. (2013) provide a specialized approach to cybersecurity, investigating the actions of virtual criminal organizations, industrial espionage, and the economic and geopolitical

impacts of cybercrimes. The authors combine their expertise to build a comprehensive encyclopedia of digital threats, covering everything from state-coordinated attacks to so-called cyber wars.

When discussing cybercrimes, it is important to differentiate between cybercrimes and computer crimes. Computer crimes encompass any illegal conduct related to data processing, whether in storage, compilation, or transmission. Cybercrime, more specifically, refers to offenses committed through information technology with the intent to harm others. Such illicit conduct can be legally classified as virtual crimes, already typified by the Brazilian Penal Code.

Schmidt (2014) categorizes cybercrimes into three main types: pure, mixed, and common crimes. Pure crimes directly affect the physical (hardware) or logical (software) structure of computer systems, such as the Melissa virus, which in 1999 caused losses exceeding 80 million dollars by compromising Microsoft Word users. Mixed crimes use technology as a means to commit criminal acts, such as fraud via Internet Banking. Common crimes use the internet merely as a channel to disseminate illicit content, as seen in cases of child pornography.

According to Schmidt (2014), cybercrimes can also be classified as proper—when both the target and the tool of the crime are computer systems, such as network intrusions by hackers—and improper, when the computer is merely a means to reach human victims or institutions, as in cases of fraud, defamation, or digital pedophilia.

The increasing sophistication of these crimes underscores the importance of cybersecurity as a key issue on the contemporary international agenda. Until the end of the 20th century, major security concerns focused on armed conflicts, human security, and the environment. However, with the turn of the millennium, cybersecurity emerged as a new strategic axis, driven by the information revolution and the acceleration of digital transformation.

The report by the Organisation for Economic Co-operation and Development (OECD, 2012) highlighted the centrality of the internet for economic and social development, as well as the rise of digital threats. This concern was echoed by leaders such as Jean-Claude Juncker, who warned of risks to freedom, democracy, and institutional stability posed by cyberattacks. Nye (2018) emphasized that since 2013, digital risks have been considered the greatest threat to U.S. national security, a view supported by the Strategic Survey of the International Institute for Strategic Studies (IISS, 2018), which recognizes the impact of the digital revolution on all forms of global governance.

Economically, the damages are alarming. Boer and Vazquez (2017) point out that a large-scale cyberattack could result in losses exceeding 121 billion dollars. The Global Risks Report by the World Economic Forum (2018) estimates that between 2017 and 2022, the global cost of cybercrime to businesses could reach 8 trillion dollars.

Given this panorama, it becomes evident that understanding cyberspace operations and addressing cybersecurity challenges is essential for formulating effective policies and protecting individuals, businesses, and governments from the risks of the digital age.

CYBER THREATS

Cyber threats have become one of the greatest challenges of the digital age, in a context marked by increasing dependence on information and communication technologies. These threats range from malicious attacks on systems and networks
to sophisticated strategies of digital espionage and sabotage, directly impacting the economy, politics, and societal security (Stallings, 2019).

Among the most common types are malware, such as viruses, trojans, and ransomware, which compromise data and can paralyze entire operations. Ransomware, in particular, has gained significant attention in recent years for hijacking information from companies and public agencies, demanding ransom payments in cryptocurrencies to release the files (Kaspersky, 2023). Another frequent threat is phishing attacks, which exploit social engineering techniques to trick users into revealing login credentials or sensitive personal information, endangering both individuals and financial institutions (Alkhalil et al., 2021).

The strengthening of organized cybercrime highlights how technology also supports illicit activities on a global scale. According to Interpol (2022), transnational criminal groups have exploited vulnerabilities in strategic sectors such as healthcare, energy, and transportation, increasing social risks and significantly raising cybersecurity defense costs. Estimates indicate that in 2021 alone, damages caused by digital crimes exceeded 6 trillion dollars, establishing cybercrime as one of the most lucrative illicit activities worldwide (Morgan, 2021).

Beyond the economic aspect, the geopolitical dimension of digital security deserves attention. Conflicts between nations now incorporate cyberattacks as strategic weapons, whether for espionage or destabilization of critical infrastructures. The case of the Stuxnet virus, which in 2010 affected nuclear facilities in Iran, became a landmark by demonstrating how digital attacks can have impacts as devastating as conventional military operations (RID, 2020).

In this scenario, economic theory applied to information security helps to understand the incentives (or lack thereof) that shape the behavior of organizations and individuals. Anderson (2001 apud Cortez; Kubota, 2013) highlights how network externalities and the lack of direct accountability hinder progress in digital protection. Varian (2004 apud Cortez; Kubota, 2013) reinforces this argument by analyzing Distributed Denial of Service (DDoS) attacks that occurred in 2000. He argues that holding

institutions accountable for leaving vulnerabilities in their networks would be a significant incentive for strengthening security.

DDoS attacks are designed to overwhelm system resources, rendering them inaccessible. Common methods include amplification, bandwidth saturation, and exhaustion of computational resources, all capable of causing serious financial and reputational damage to affected organizations (Cloudflare, [n.d.]). Phishing attacks are among the most popular forms of social engineering, encompassing practices such as blind phishing, clone phishing, website spoofing, and pharming, all aimed at deceiving users and capturing confidential data (Malwarebytes, [n.d.]).

Another concerning example is ransomware, a type of malware that locks or threatens to destroy data unless a ransom is paid. Initially targeting individual users, this type of attack has evolved to affect corporations and public institutions, often using sophisticated methods that include accessing internal documents to determine ransom amounts (Microsoft, [n.d.] apud Cândido; Florian; Borges, 2023). Criminals frequently use spam emails and fake websites to spread the virus, relying on social engineering techniques to induce victims to click. Exploiting vulnerabilities in operating systems and using Traffic Distribution Systems (TDS) are other common propagation methods (Afrikatec, 2017; Tecnoblog, 2017 apud Cândido; Florian; Borges, 2023).

The analysis of these various attacks reveals that the costs of digital insecurity are not only technical but also economic and social. Anderson (1994 apud Cortez; Kubota, 2013) shows, for example, how legal responsibility in cases of bank fraud varies between countries and directly influences security levels. In European nations, where responsibility fell on customers, banks had fewer incentives to invest in protection, whereas in the United States, by assuming greater responsibility, financial institutions significantly reduced the incidence of fraud.

Therefore, it becomes evident that mitigating cyber threats requires more than technological solutions. It is necessary to invest in public policies, effective regulation, and social awareness, forming a triad that strengthens both the technical apparatus and the preventive posture of users (Tankard, 2011). In this regard, digital education is fundamental, as many attacks still rely on psychological manipulation of victims.

DEFENSE STRATEGIES AND PROTECTION TECHNOLOGIES

The intensification of digital threats in the global landscape has led governments, companies, and individuals to seek increasingly sophisticated protection strategies. Information security has evolved beyond a purely technical concern to become a strategic element of national sovereignty, institutional preservation, and the safeguarding of fundamental rights (Stallings, 2017). In this context, traditional mechanisms such as firewalls and intrusion detection and prevention systems (IDS/IPS) remain

indispensable tools. While firewalls act as barriers that filter network traffic, IDS and IPS operate more actively, monitoring and responding to intrusion attempts in real time, forming a first line of defense against unauthorized access. Another essential resource is encryption, which ensures the confidentiality and integrity of information, whether in storage or during transmission over open networks. The use of robust algorithms such as AES and RSA has become standard across various sectors, particularly in banking operations, e-commerce services, and digital communications (Tanenbaum; Wetherall, 2011).

In parallel, the evolution of authentication mechanisms has brought significant advancements, with multi-factor authentication (MFA) standing out as one of the most important. Unlike the exclusive use of passwords—which is considered a vulnerable practice—MFA integrates different elements such as biometrics, physical tokens, and mobile devices, ensuring greater reliability in identity verification (Bosworth; Kabay; Whitman, 2014). Biometric authentication, in particular, has gained traction in banking and governmental systems, as it reduces the possibility of credential forgery or misuse. However, investing solely in technological solutions is not sufficient. The specialized literature emphasizes the importance of risk management and security policies, which form the foundation for preventive and organized action against digital threats. According to the ISO/IEC 27005 standard (2018), risk management involves identifying, assessing, and mitigating vulnerabilities based on the criticality of assets, while security policies define clear responsibilities and usage rules, consolidating an organizational culture of protection (Whitman; Mattord, 2022).

In Brazil, the legal framework for cybersecurity has significantly advanced in recent decades. Law No. 12.737/2012, known as the "Carolina Dieckmann Law," criminalized acts such as unauthorized access to computer devices and digital data theft (Brazil, 2012). More recently, Law No. 14.155/2021 increased penalties for cybercrimes, expanding measures against system intrusions and tampering (Brazil, 2021). These legal developments were also driven by high-profile international incidents. The revelations by Edward Snowden in 2013 exposed that communications of the Brazilian government, including those of then-President Dilma Rousseff, had been surveilled by the United States, prompting a strong political response at the United Nations General Assembly (Brazil, 2013; Cepik, 2018). Similarly, Nunes (2021) reports that Brazil was monitored through the Swiss company Crypto AG, which collaborated with the CIA and German intelligence, revealing vulnerabilities in the country's digital security landscape.

These events spurred the creation of more robust regulatory frameworks, such as the Marco Civil da Internet, established by Law No. 12.965/2014, which set principles for internet governance in Brazil (Brazil, 2014). Additionally, public policies such as the National Defense Strategy and the National Cybersecurity Strategy, instituted by Decree No. 12.573 of August 4, 2025, began to define guidelines for protecting critical national infrastructure and public and private institutions (Brazil, 2025; Hurel; Lobato, 2018). In parallel, Brazil has sought to expand its international engagement, participating in debates on

cyberspace regulation and, in 2023, joining the Budapest Convention on Cybercrime, committing to global standards of legal cooperation (Council of Europe, 2022; Brazil, 2021).

Other recent measures include the execution of the Cyber Guardian Exercise, considered the largest in Latin America, which simulates attack scenarios on critical infrastructure and strengthens cooperation among the Armed Forces, public institutions, and the private sector (Brazil, 2025). Additionally, the formulation of the National Cybersecurity Policy (PNCiber) and the National Cybersecurity System (SNCiber) is underway, aiming to unify governance and bolster Brazil's digital resilience (Brazil, 2021). These developments reveal that cyber defense has become a strategic priority, not only technical but also political, economic, and military.

International experience reinforces this understanding. China, for example, created the Strategic Support Force and consolidated its cyber defense doctrine as part of national security, combining active and offensive defense strategies (China, 2019; Creemers, 2016). The United States, from the National Cybersecurity Initiative of 2008 to the recent National Cyber Strategy of 2023, has strengthened its stance against state-sponsored threats and organized groups (United States, 2018; Biden White House, 2023). Portugal, in turn, incorporated cyber defense into the mission of its Armed Forces and enhanced cooperation with international organizations such as NATO and the European Union Agency for Cybersecurity (ENISA), demonstrating an integrated protection perspective (Nunes, 2018; Portugal, 2023).

Thus, it is evident that the consolidation of cybersecurity as a political and legal priority is a direct reflection of the growing global interdependence of digital systems and the exponential increase in threats. In Brazil, legislative advances, public policies, and participation in international treaties indicate a trajectory of strengthening, albeit still marked by challenges related to the effectiveness of actions and the development of a national culture of information security. Comparisons with countries such as China, the United States, and Portugal show that, despite different paths, all recognize the centrality of cyber defense in the 21st century—whether for the protection of critical infrastructure or for the maintenance of sovereignty and social stability (Hurel; Lobato, 2018; Creemers, 2016).

SECURITY IN DIFFERENT DIGITAL ENVIRONMENTS

Security in different digital environments has become one of the main concerns of contemporary organizations, as information has come to represent one of the most valuable assets in the digital age. In corporate networks in particular, the increase in interconnectivity and technological dependence has brought with it a complex array of risks and vulnerabilities that demand a systematic, strategic, and culturally consolidated approach to information security. According to Silveira, Lunardi, and Cerqueira (2023), informational security within companies is not limited to technical aspects but also involves

organizational culture and employee behavior, with the human factor being a critical element for the success of data protection policies. The authors emphasize that in specific cultural contexts, such as Brazil, informal practices and behavioral flexibility—popularly known as the "Brazilian way"—can pose threats to system integrity and undermine the effectiveness of implemented security standards.

Thus, the consolidation of an information security culture in corporate networks depends on the alignment between technology, processes, and people. Silveira, Lunardi, and Cerqueira (2023) argue that the adoption of international standards, such as ISO/IEC 27001, provides a structured foundation for risk management and the establishment of security controls, but only its application accompanied by effective cultural changes can ensure lasting results. Organizations that adopt a merely reactive stance toward incidents tend to develop fragmented security policies that fail to integrate employee awareness and training practices. In this regard, corporate education and clear communication about individual responsibilities are fundamental strategies for strengthening internal network security and reducing vulnerabilities arising from negligence or lack of knowledge.

Moreover, modern corporate networks have become hybrid environments, composed of local infrastructures and cloud-based solutions, which significantly expand the spectrum of cyber threats. Santos et al. (2022) highlight that Brazil's National Information Security Policy follows a global trend of standardizing practices, aligning with frameworks such as NIST and ISO standards, enabling organizations to establish more robust risk management guided by indicators. This perspective underscores that the protection of corporate systems should be viewed as a continuous process, in which the identification, assessment, and mitigation of risks constitute a permanent cycle of improvement.

Strengthening security in corporate networks also requires an integrated approach to the protection of personal data, especially following the enactment of the General Data Protection Law (LGPD). According to Almeida and Soares (2022), the LGPD redefined the landscape of corporate responsibility, imposing legal obligations that span from data collection to storage and sharing. Compliance with best practices described in ISO/IEC 27001 and 27002 standards, combined with legal adherence to the LGPD, is now an indispensable requirement for institutional credibility and the digital sustainability of organizations.

In this context, cloud security emerges as a natural extension of corporate network security, representing both opportunities and challenges. Cloud computing has radically transformed the way companies store, process, and share data, promoting greater operational flexibility and scalability. However, as Cândido and Araújo Júnior (2022) point out, the growing use of cloud computing imposes new demands on information management, as data migration to external environments alters the nature of control and responsibility. The authors emphasize that the development of cloud solutions requires the

establishment of security policies adapted to this context, encompassing aspects such as authentication, encryption, and access auditing.

Although cloud computing offers advantages in terms of efficiency and cost, it exposes organizations to specific vulnerabilities, such as Distributed Denial of Service (DDoS) attacks, account hijacking, and unauthorized access. According to Castro and Alves (2021), the adoption of security and digital preservation standards, such as the PREMIS model, contributes to the integrity and authenticity of data stored on cloud platforms, being an essential element for the long-term reliability of digital information. Digital preservation, in this context, is directly linked to information governance and compliance with technical and legal requirements.

According to Cândido and Araújo Júnior (2022), the effectiveness of cloud security is strongly tied to the maturity of information management within organizations. The cloud should not be seen merely as a data repository but as a strategic environment that requires access control, continuous monitoring, and clearly defined contingency policies. Identity management and the use of multi-factor authentication protocols are indispensable mechanisms for mitigating unauthorized access risks. Furthermore, reliance on external providers necessitates specific contractual clauses regarding confidentiality, integrity, and availability of information, ensuring that responsibilities are clearly defined.

Discussions on cloud security are also directly related to data sovereignty. The physical location of servers and the legal jurisdiction governing information processing are factors that significantly impact organizational compliance with the LGPD and the European Union's General Data Protection Regulation (GDPR). Vetis-Zaganelli and Binda Filho (2022) assert that in the context of digital health, the transfer of sensitive data to international providers must be accompanied by impact assessments and risk mitigation measures, considering technical, ethical, and legal aspects. This analysis reinforces the importance of ethical information management that ensures individual privacy and protection.

The integration between cloud security and data protection legislation demonstrates that information security transcends technological boundaries and reaches the realm of organizational governance. For Cândido and Araújo Júnior (2022), security should be understood as part of institutional strategy, not merely as a technical component. Organizational culture, in this sense, must incorporate values oriented toward security and privacy from the earliest stages of system and process planning. This approach, known as "privacy by design," implies that data protection is embedded in the very design of technological solutions, anticipating potential vulnerabilities before they become actual threats.

Finally, the transition of companies to hybrid environments combining local networks and cloud infrastructure demands an integrated security architecture, with policies encompassing both physical infrastructure and digital services. Santos et al. (2022) point out that the adoption of hierarchical risk assessment methodologies, based on models such as NIST, enables a comprehensive view of

vulnerabilities and prioritizes the efficient allocation of security resources. This alignment between governance, technology, and legislation creates the necessary conditions for mature cyber risk management, capable of proactively responding to emerging threats that characterize the contemporary digital landscape.

The expansion of global connectivity and the advent of the Internet of Things (IoT) represent a new frontier for information security. Sundmaeker, Guillemin, Friess et al. (2010) forecast between 50 and 100 billion connected devices by 2020 (cited in João, Souza, & Serralvo, 2019, p. 1117). IoT involves the integration of physical devices into the digital environment, enabling the constant exchange of data between sensors, machines, and control systems. Although this interconnection brings benefits in terms of efficiency and automation, it also significantly expands the attack surface, creating new vectors of vulnerability.

According to João, Souza, and Serralvo (2019), IoT—especially in the context of smart cities—requires more sophisticated and interoperable security policies capable of handling the volume, diversity, and sensitivity of the information generated. "Smart," in this context, refers to a city in which everything is environmentally responsive and which produces, consumes, and distributes vast amounts of information in real time (Demeri, 2013, cited in João, Souza, & Serralvo, 2019, p. 1118).

The authors emphasize that security in IoT must be conceived holistically, encompassing technical, ethical, and legal aspects to ensure data integrity and privacy.

Vashi, Ram, Modi et al. (2017) assert that a radical revolution of the internet is underway. It is no longer merely a network that interacts with connected objects and extracts information from the sensory environment; it also interacts with the physical world, detects patterns in the network, and provides information, new applications, and communication (cited in João, Souza, & Serralvo, 2019, p. 1117).

The incorporation of connected devices into critical sectors such as healthcare, transportation, and energy intensifies the need for robust protection mechanisms. Rosa, Souza, and Silva (2020) argue that in the healthcare sector, the use of smart devices for remote patient monitoring demands stringent standards of security and privacy, as the data collected are sensitive and subject to specific regulations. The collection, storage, and sharing of such information must comply with the guidelines of the General Data Protection Law (LGPD), ensuring that data processing is legitimate, transparent, and proportional to its intended purpose. Failure to comply with these principles can result in serious ethical and legal violations, undermining public trust in digital health technologies.

The challenge of securing IoT also relates to the heterogeneity of devices and the lack of global standardization. Many connected devices operate with embedded systems that have limited processing and storage capabilities, which hinders the implementation of complex encryption and authentication mechanisms. João, Souza, and Serralvo (2019) observe that to mitigate such limitations, it is essential to

adopt distributed and decentralized architectures, in which security does not rely solely on a central control point. In this context, blockchain technology emerges as a promising alternative, offering an immutable and verifiable ledger structure for transactions and communications between devices.

Originally conceived as the foundation for cryptocurrencies, blockchain has expanded its scope to various fields, including cybersecurity. According to Almada and Costa (2023), blockchain presents itself as an effective tool for enhancing transparency and traceability in digital operations, reducing reliance on intermediaries and strengthening trust among involved parties. Its application in IoT systems allows each transaction to be recorded in a decentralized manner, preventing unauthorized modifications and complicating data forgery attacks. This immutability is particularly valuable in environments where information integrity is critical, such as medical device control, logistics systems, and smart energy networks.

Furthermore, blockchain contributes to the strengthening of control and surveillance policies within digital capitalism. Almada and Costa (2023) analyze that the adoption of this technology by companies and governments has expanded not only due to its security potential but also because of its ability to track and audit activities in real time. However, the authors caution that such digital surveillance may reinforce dynamics of excessive control, raising ethical concerns about privacy and individual freedom. Therefore, the implementation of blockchain in corporate and public contexts must balance security, transparency, and fundamental rights, to prevent the transformation of protection into a tool of technological domination.

Renato Costa (2022) complements this discussion by examining the application of the LGPD in conjunction with ISO/IEC 27001 and 27002 standards in IoT security. The author emphasizes that integrating legislation with international standards is essential for creating a trustworthy digital ecosystem, where the use of blockchain can coexist with principles of data governance and social responsibility. Compliance with these normative frameworks ensures that security is not treated merely as a technical requirement but as an ethical and strategic dimension of organizational management.

The growing interdependence between IoT, cloud computing, and blockchain reflects the emergence of increasingly complex digital ecosystems that demand integrated cybersecurity policies. João, Souza, and Serralvo (2019) argue that smart cities and connected infrastructures require governance models that combine technological innovation with effective regulation. The use of blockchain to protect real-time communications and transactions, combined with advanced encryption and secure authentication protocols, provides a solid foundation for creating resilient digital environments. This integration not only reduces vulnerabilities but also enhances the trust of users and stakeholders in the technological solutions implemented.

Therefore, the management of security in different digital environments must be understood as an interconnected system, in which corporate networks, clouds, IoT devices, and emerging technologies coexist in synergy. João, Souza, and Serralvo (2019, p. 1119) reinforce this view by highlighting that Critical Infrastructures (CIs) are evolving toward an integrated and intelligent environment, where IoT is used to interconnect, interact, control, and provide insights into the various fragmented systems within cities. This integration, however, brings with it exposure to numerous threats, requiring that security be conceived in a holistic manner.

A fragmented approach to protection no longer meets the demands of the contemporary digital landscape, which is characterized by dynamic and sophisticated threats. According to Santos et al. (2022), the adoption of hierarchical risk analysis methodologies and the continuous implementation of improvements based on performance indicators are essential practices for building an organizational culture oriented toward security. This culture must be sustained by employee awareness, data governance, and the ethical commitment of institutions.

Finally, security in digital environments should not be viewed merely as a technical barrier against attacks, but rather as a strategic pillar for innovation and organizational sustainability. Silveira, Lunardi, and Cerqueira (2023) emphasize that true security arises from the balance between technology and culture, with trust serving as the link that connects data protection, regulatory compliance, and human behavior. The consolidation of secure practices across corporate networks, cloud infrastructures, IoT systems, and blockchain technologies requires the internalization of ethical values, respect for privacy, and a permanent commitment to continuous improvement. In an increasingly interconnected world, digital security is not only a technical necessity but also an expression of social and organizational responsibility.

STANDARDS, FRAMEWORKS, AND LEGISLATION

The consolidation of standards, frameworks, and legislation in the field of cybersecurity represents one of the fundamental pillars for building an organizational culture focused on data protection and the efficient management of digital risks. International standards such as ISO/IEC 27001, security frameworks developed by the NIST (National Institute of Standards and Technology), and COBIT (Control Objectives for Information and Related Technologies) are essential tools for establishing standardized, measurable, and auditable processes. According to Stallings (2019), the adoption of these standards enables organizations to achieve a mature level of information security, creating mechanisms for incident prevention and response in a systematic and documented manner. Silveira, Lunardi, and Cerqueira (2023) emphasize that organizational culture directly influences adherence to ISO/IEC 27001 standards, stating that “information security depends not only on technology but also on shared behaviors

and values" (p. 144). They further assert that "information security awareness positively influences individuals' planned behavior and negatively affects the 'Brazilian way'" (p. 156), highlighting how cultural aspects can compromise the effectiveness of technical standards.

The ISO/IEC 27001 standard, developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), establishes requirements for the creation, implementation, and maintenance of an Information Security Management System (ISMS). According to Whitman and Mattord (2022), this standard proposes an approach based on the PDCA cycle (Plan, Do, Check, Act), enabling continuous improvement of security practices. This structure is widely used in public and private organizations as it promotes a management model that integrates technological, human, and procedural aspects. As emphasized by Dhillon (2021) and von Solms and van Niekerk (2013), compliance with ISO/IEC 27001 goes beyond implementing technical controls; it requires senior management commitment, policy definition, and the involvement of all employees in the security culture.

Complementing ISO/IEC 27001, the NIST Cybersecurity Framework has emerged as a reference, especially in North American contexts and increasingly on a global scale. Created in 2014 and revised in 2018, the framework organizes its recommendations into five core functions: Identify, Protect, Detect, Respond, and Recover (NIST, 2018).

This structure helps companies across various sectors map their assets, prioritize controls, and align security actions with strategic objectives. According to Peltier (2021), NIST offers a practical guide for managing cyber risks, being flexible and adaptable to different organizational realities. This flexibility makes it a valuable complement to ISO/IEC 27001, which sets certification requirements, while NIST provides guidelines that can be implemented incrementally and tailored to specific needs.

COBIT, developed by ISACA (Information Systems Audit and Control Association), is a framework focused on IT governance and management. According to Haes and Van Grembergen (2020), COBIT promotes integration between corporate goals and security practices, enabling organizations to monitor and evaluate the performance of their IT processes. By incorporating the concept of accountability, COBIT contributes to transparency in decision-making, reinforcing the role of information security as a strategic business factor. As Ross (2022) notes, the combination of ISO/IEC 27001, NIST, and COBIT offers a robust normative ecosystem that spans operational management to strategic alignment of digital security.

However, technological advancement and the exponential growth in personal data collection have driven the creation of data protection laws, such as Brazil's General Data Protection Law (LGPD), enacted by Law No. 13.709/2018. Inspired by international legislation, the LGPD establishes clear rules regarding the collection, storage, processing, and sharing of personal information. According to Doneda (2020), the law emerged in a context of growing concern over data misuse and digital surveillance. It

defines fundamental principles—such as purpose, adequacy, necessity, free access, data quality, and accountability—that guide business and governmental practices in handling personal information.

The LGPD also introduced the concepts of data controller and data processor, responsible for data handling, and established the role of the Data Protection Officer (DPO), who serves as a communication channel between the organization, data subjects, and the National Data Protection Authority (ANPD). According to Moraes (2021), the creation of the ANPD was essential for the law's effectiveness, enabling oversight and enforcement in cases of non-compliance. This institutionalization of privacy governance reinforces the understanding that information security transcends technical dimensions and enters ethical and legal domains.

Internationally, the General Data Protection Regulation (GDPR), implemented by the European Union in 2018, has become a global benchmark for privacy and data protection. As Kuner (2020) explains, the GDPR established a new regulatory paradigm by prioritizing the fundamental right to privacy and imposing strict responsibilities on organizations that process personal data. Its extraterritorial scope, applying to companies outside the EU that handle data of European citizens, underscores the global nature of contemporary cybersecurity challenges. Moreover, the regulation encourages preventive measures such as Data Protection Impact Assessments (DPIA) and the use of pseudonymization and encryption.

Other notable examples include the HIPAA (Health Insurance Portability and Accountability Act) in the United States, which regulates the handling of health data, and the CCPA (California Consumer Privacy Act), which expands consumer rights regarding transparency and control over their information. According to Cate and Mayer-Schönberger (2021), such legislation reflects a global movement toward digital accountability, encouraging companies to adopt ethical standards in data governance. Compliance with these regulations, though challenging, contributes to consumer trust and mitigates reputational and legal risks.

The dialogue between technical standards and legislation underscores the need for a holistic approach to digital security. As Solms (2021) observes, the effectiveness of information protection depends on the integration of normative frameworks and legal instruments that regulate organizational behavior. In this regard, ISO/IEC 27001 and NIST provide methodological and operational foundations, while LGPD and GDPR establish ethical and legal guidelines. Thus, information governance should be understood as an interconnected ecosystem, where standards, frameworks, and laws complement each other to strengthen institutional cyber resilience.

The integration of technical standards, national laws, and international regulations is one of the greatest contemporary challenges in cybersecurity. According to Silveira, Lunardi, and Cerqueira (2023), organizational culture directly influences adherence to ISO/IEC 27001 standards, as information security

depends not only on technology but also on shared behaviors and values. Compliance with ISO 27001, therefore, requires organizations to cultivate a strong "security culture," in which employees understand the impact of their actions on data confidentiality and integrity.

From this perspective, Santos et al. (2022) highlight the importance of integrating ISO 27001 with NIST guidelines, particularly regarding risk management and incident monitoring. The NIST model is widely used as a governance framework, providing guidance for identifying, protecting, detecting, responding to, and recovering information systems. As the authors emphasize, combining international standards with local regulations supports the development of robust policies adaptable to national realities.

Complementarily, COBIT is cited as an essential model of corporate governance focused on process control and IT practice maturity. The joint application of COBIT and ISO 27001 enables the alignment of information security with the organization's strategic objectives. This synergy is highlighted by Cândido and Araújo Júnior (2022), who stress the need to integrate security standards with information management practices, especially in cloud computing contexts, where data are constantly transferred across multiple digital environments.

In the legal domain, the LGPD, established by Law No. 13.709/2018, marked a regulatory milestone for personal data protection in Brazil. According to Almeida and Soares (2022), the LGPD aims to ensure transparency, security, and control in data processing, imposing responsibilities on both controllers and processors. This legislation aligns directly with the principles of ISO 27001 and NIST's risk-based approach, demonstrating Brazil's effort to harmonize with international cybersecurity standards.

Vetis-Zaganelli and Binda Filho (2022) observe that the LGPD shares several principles with the GDPR, particularly regarding consent, purpose limitation, and corporate accountability for data processing. However, the lack of interoperability limits the ability to connect different data flows or develop new applications to achieve greater value over time (Krishnamachari, Power, Kim et al., 2018, cited in João, Souza, & Serralvo, 2019, p. 1120).

This normative convergence reinforces the importance of global cooperation and interoperability among regulatory frameworks, as data flows do not recognize geographic boundaries. In this regard, the GDPR exerts strong influence on legislation in other countries, promoting the international standardization of privacy best practices.

Renato Costa (2022) emphasizes that applying the LGPD to the Internet of Things (IoT) requires direct alignment with ISO/IEC 27001 and 27002 standards. The technical complexity inherent in these ecosystems is highlighted by Batalla, Mastorakis, Mavromoustakis et al. (2017, cited by João, Souza, & Serralvo, 2019, p. 1117), who identify practical solutions for technical challenges including enhanced

sensor capabilities, sensor miniaturization, big data handling, efficient remote data management, and the implementation of open and secure processes for various IoT scenarios. Due to its distributed and hyperconnected nature, IoT increases the risk of breaches and demands specific protection strategies. Costa notes that ISO standards offer guidelines for access control, encryption, and auditing—essential elements for preserving the integrity of communications among smart devices. Thus, integrating technical standards and legislation ensures not only legal compliance but also operational resilience.

Beyond LGPD and GDPR, other international regulations deserve attention. The HIPAA, in force in the United States, establishes strict standards for protecting medical data and sensitive health information. This legislation shares principles with the LGPD, such as the need for informed consent and the obligation to adopt technical and administrative security measures. According to Rosa, Souza, and Silva (2020), the advancement of digitalization in healthcare—especially with the use of IoT—makes compliance with standards that ensure privacy and integrity of clinical information essential.

The interconnection between technical standards, national laws, and international regulations requires ongoing efforts in updating and integration. Almada and Costa (2023) argue that emerging technologies such as blockchain can contribute to regulatory compliance by providing traceability and immutability of digital records. This technology has the potential to enhance data auditing and control, reducing manipulation risks and strengthening trust in digital ecosystems. Therefore, blockchain represents a promising frontier between technological innovation and regulatory security.

Silveira, Lunardi, and Cerqueira (2023) reiterate that compliance with ISO standards and the LGPD should not be understood merely as a legal obligation but as part of a governance strategy and organizational culture. Information security is a value that must be embedded in corporate daily life, requiring awareness, training, and institutional commitment. The combination of technical standards, legislation, and ethical best practices creates a solid foundation for consolidating a cybersecurity culture—an essential element in the digital and globalized era.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN CYBERSECURITY

Machine Learning (ML) aims to develop programs capable of improving their performance based on examples, generating computational knowledge through hypotheses extracted from data (Mitchell, 1997). To achieve reliable results, a substantial amount of examples is required, as the accuracy of generalizations depends directly on the quality of the data provided. ML techniques are data-driven, learning automatically from large volumes of information. A central method in this process is inductive inference, used to generate new knowledge and predict future events, although its generalization capacity may be limited if the data are imprecise.

Machine Learning is divided into three main categories: supervised, unsupervised, and reinforcement learning. In supervised ML, each example provided to the algorithm is accompanied by a label indicating its class or desired value, allowing the system to learn to correctly categorize new examples. When labels are discrete, the problem is called classification; when continuous, regression. This is the most widely used method. In unsupervised learning, examples are presented without labels, and the algorithm must identify patterns and group data with similar characteristics, forming clusters that later require interpretation to determine their meaning in the problem context (Estudos Avançados, 2021). In reinforcement learning, the algorithm does not receive correct answers but rather reward or punishment signals indicating the quality of its hypotheses. This method is widely applied in robotics and games, as exemplified by AlphaGo.

The application of ML requires specific prerequisites, such as representative and up-to-date datasets, as well as techniques to improve data quality. Not all algorithms are suitable for all problems, requiring careful selection and proper parameter configuration, along with continuous monitoring to ensure the system remains effective amid data changes.

Among ML techniques, Artificial Neural Networks (ANNs) stand out for their success in solving complex problems. Inspired by biological neural networks, they process information through artificial neurons known as MCP models (McCulloch & Pitts, 1943). The Perceptron, developed by Rosenblatt in 1957, is the simplest form of ANN, applicable to linearly separable problems, consisting of a single layer of MCP neurons adjusted by error correction (Rosenblatt, 1957). For more complex tasks, Multi-Layer Perceptrons (MLP) trained via the Backpropagation algorithm (Rumelhart et al., 1986) are employed, although other techniques like Support Vector Machines (SVM) have outperformed neural networks in some applications (Cortes & Vapnik, 1995). Deep Neural Networks, with multiple layers and architectures such as convolutional and pooling layers, can automatically extract relevant features from input data, achieving satisfactory solutions in complex problems (LeCun et al., 2015).

The advancement of Artificial Intelligence (AI) has transformed everyday life, bringing benefits such as optimized healthcare services, natural language processing, enhanced education, clean energy, fraud detection, and safer, more efficient transportation. However, it also causes negative impacts, such as job displacement and increased social inequality. Beyond social issues, ethical and legal concerns arise, including the use of automated weapons, privacy invasion, and lack of transparency in AI systems—issues that are being partially addressed by international guidelines and national legislation, such as the LGPD and related bills (Hagendorff, 2020).

The challenges of AI include developing systems that are explainable, fair, robust, and privacy-preserving—a field known as Trustworthy Machine Learning. Clear explanations not only help understand AI decisions but also identify potential errors. Currently, the availability of large datasets and

high computational power are crucial for AI success, although efforts are underway to reduce the need for massive data volumes, bringing machine learning closer to human reasoning. Techniques such as pre-trained systems (e.g., BERT, GPT) and self-supervised learning have advanced in this direction, enabling adaptation to specific tasks with fewer data (Devlin et al., 2019; Ravanelli et al., 2020).

Another critical issue is that many training datasets do not adequately represent the real world, potentially introducing biases. For instance, an algorithm trained only with white cats and black dogs may learn incorrect patterns, requiring human intervention for correction. Moreover, dynamic problems such as real-time monitoring and transportation management demand continuous learning techniques to handle constant data flows (Gama, 2012). To enhance ML applicability, automatic and efficient decisions regarding preprocessing, algorithm selection, hyperparameters, attributes, and post-processing are necessary. Meta-learning represents a promising approach, allowing algorithms to automatically learn which methods and parameters to use for high performance (Hospedales et al., 2020).

In this context, the advancement of AI and ML has significantly transformed the field of cybersecurity, introducing new possibilities for threat detection, prevention, and incident response. These technologies enable systems to learn and adapt automatically to behavioral patterns, becoming capable of identifying anomalies, predicting attacks, and autonomously responding to emerging threats. As LeCun, Bengio, and Hinton (2015) highlight, AI can perform complex inferences from large volumes of data, making it especially useful in digital defense contexts where speed and accuracy are crucial.

The use of AI in cybersecurity represents a paradigm shift, replacing reactive approaches with proactive and predictive postures. According to Mitchell (1997), ML is the field of computer science that studies algorithms capable of improving performance based on experience, without relying on explicit instructions. In cyber environments, this capability is applied to network traffic analysis, intrusion detection, biometric authentication, adaptive encryption, and automated incident response. AI-based tools can process vast amounts of data in real time, recognizing anomalous patterns that might go unnoticed by traditional methods.

According to Taddeo and Floridi (2018), AI has unprecedented potential to strengthen cybersecurity, offering means to anticipate attacks and mitigate vulnerabilities before significant damage occurs. However, they caution that AI use may also generate new risks, especially when deployed autonomously or maliciously. Cybercriminals can use learning algorithms to develop more sophisticated attacks, automate intrusions, and bypass conventional defenses. This duality—combining innovation and threat—underscores the ambivalent nature of AI in digital security.

Recent studies show that deep learning, one of AI's most advanced branches, has been widely used in malware and phishing detection through behavioral and linguistic pattern recognition (Kumar, Singh & Thomas, 2021). This technology can classify events and identify unknown threats based on

historical data and simulations, enhancing the accuracy of cyber defenses. However, Hagendorff (2020) warns that opaque and non-interpretable algorithms may pose ethical and reliability risks, especially when critical security decisions are made without human oversight. Thus, algorithmic transparency and model explainability become essential requirements for responsible AI application in this field.

Moreover, the integration of AI and cybersecurity has driven the development of autonomous response and recovery systems. These systems use neural networks and probabilistic models to predict attack behavior and automatically adjust defense measures. According to Ross (2022), such automation reduces incident response time and minimizes financial and reputational damage to organizations. Nevertheless, ethical and technical limits of this autonomy must be considered, ensuring that human oversight remains central to security decisions, particularly in critical environments such as public infrastructure and financial systems.

AI and ML applications have also contributed to strengthening cyber risk management policies. As Tankard (2011) notes, predictive analysis based on AI helps prioritize threats, assess vulnerabilities, and simulate attack scenarios. This approach enhances organizational resilience by enabling more informed decisions and optimizing resources allocated to security. Furthermore, the combination of AI, blockchain, and IoT has expanded monitoring and protection capabilities in distributed networks, offering additional layers of verification and traceability (Almada & Costa, 2023).

The following table (Table 1) summarizes the main uses, benefits, challenges, and risks of applying Artificial Intelligence and Machine Learning in cybersecurity, based on the analyzed sources.

Table 1 – Main Uses, Description and Examples, Benefits, Challenges, and Risks of Applying Artificial Intelligence and Machine Learning in Cybersecurity

Application / Function	Description and Examples	Benefits	Main Risks and Challenges	References
Threat and intrusion detection	Monitoring of traffic and identification of anomalous patterns using supervised learning	Early attack detection and reduced response time	Possibility of false positives and dependence on training data	LeCun; Bengio; Hinton (2015); Mitchell (1997)
Malware and phishing analysis	Automatic classification of suspicious files and emails using deep neural networks	Greater accuracy in identifying unknown threats	Risk of adversarial attacks that deceive the model	Kumar; Singh; Thomas (2021)
Biometric and behavioral authentication	Facial, voice, and typing pattern recognition based on AI	Enhanced security and personalized access control	Privacy concerns and potential algorithmic biases	Hagendorff (2020); Taddeo; Floridi (2018)
Incident response automation	Systems that apply automatic patches and block attacks in real time	Speed in mitigation and reduction of operational damage	Autonomy failures and loss of human control	Ross (2022); Dhillon (2021)
Predictive analysis and risk management	Scenario modeling and threat prioritization using AI	Strategic planning and anticipation of vulnerabilities	Technological dependency and implementation costs	Tankard (2011); Almada; Costa (2023)

Source: Compiled by the author based on LeCun, Bengio e Hinton (2015); Mitchell (1997); Hagendorff (2020); Ross (2022); Dhillon (2021); Tankard (2011); Kumar, Singh e Thomas (2021); Almada e Costa (2023); Taddeo e Floridi (2018).

From the analysis presented, it is possible to affirm that the integration of Artificial Intelligence and cybersecurity represents both an opportunity and a challenge. AI enables the creation of adaptive and autonomous systems capable of protecting networks and data in real time, but it also introduces new risks, such as lack of transparency, algorithm manipulation, and malicious use by criminal agents. The literature converges on the understanding that the future of cybersecurity depends on the ability to develop ethical, auditable, and human-centered technological solutions. In line with Hagendorff (2020) and Taddeo and Floridi (2018), it is advocated that AI should be applied as a tool for collective protection, not as an instrument of surveillance or control. Thus, building ethical, explainable, and inclusive AI becomes one of the greatest challenges—and simultaneously one of the most promising prospects—for global cybersecurity.

CHALLENGES AND FUTURE PERSPECTIVES

The field of cybersecurity currently faces significant challenges that demand urgent attention, strategic planning, and continuous investment in research and innovation. One of the most pressing issues is the shortage of qualified professionals. With the exponential growth of digital services, cloud

computing, the Internet of Things (IoT), and the adoption of emerging technologies such as artificial intelligence and blockchain, the demand for information security specialists far exceeds the available supply in the market. Recent reports indicate that millions of cybersecurity positions remain unfilled worldwide, and this gap represents not only an operational challenge but also a strategic risk for companies and governments, as the absence of skilled professionals increases vulnerability to cyberattacks (ENISA, 2023).

This shortage is directly related to the growing complexity of digital threats. Sophisticated attacks such as ransomware, targeted phishing, large-scale data breaches, and exploitation of vulnerabilities in critical systems require deep technical expertise, behavioral analysis capabilities, and constant updates on the new tactics employed by cybercriminals. Furthermore, cybersecurity has evolved beyond a purely technological issue to encompass legal, ethical, and social dimensions, including personal data protection, regulatory compliance, and the preservation of citizens' privacy (Hagendorff, 2020; Fernandes et al., 2013).

Another significant challenge is the emergence of new technologies and the risks associated with them. Innovations such as artificial intelligence, quantum computing, 5G, and IoT devices expand the possibilities for innovation but also create new attack surfaces. For example, AI systems can be targeted by data manipulation, adversarial attacks, or the malicious use of algorithms; meanwhile, quantum computing threatens traditional encryption methods, necessitating the development of new protocols resistant to advanced processing capabilities (Shor, 1994; Bada et al., 2019). Global interconnectivity and increasing dependence on digital networks mean that any vulnerability can be potentially catastrophic, affecting essential sectors such as energy, healthcare, finance, and transportation.

In light of these challenges, research and innovation in cybersecurity emerge as strategic tools to mitigate risks and build more resilient digital systems. Promising research areas include the development of automatic threat detection algorithms, proactive defense techniques based on artificial intelligence, cyberattack simulations (red teaming), and security approaches centered on data and users.

Additionally, the creation of more robust educational programs, ongoing training, and specialized certifications are crucial to reducing the gap in qualified professionals (Sommer & Paxson, 2010; ENISA, 2023). Research also highlights the importance of collaboration among public, private, and academic sectors, with information sharing on threats and best practices to enhance collective resilience against cyberattacks.

The future of cybersecurity also depends on the strengthening of public policies and international regulations that promote high security standards, encourage data protection, and foster investment in innovative security technologies. Digital security must be viewed not merely as a set of tools and protocols but as a culture integrated into the operations of businesses, government institutions, and

society at large. Investing in prevention, continuous monitoring, rapid incident response, and digital security education represents not only risk mitigation but also the assurance of trust in increasingly interconnected systems (Kshetri, 2021; Fernandes et al., 2013).

In summary, contemporary cybersecurity faces complex challenges, including the shortage of skilled professionals, the continuous evolution of technologies and threats, and the need for ongoing research and innovation. Future perspectives depend on coordinated actions that unite technology, human expertise, and strategic policies. The training of highly qualified professionals, combined with the development of advanced technologies and global collaboration, will be essential to build a secure, trustworthy, and resilient digital ecosystem, capable of keeping pace with the rapid transformation of the digital world and protecting individuals, businesses, and societies from the cyber risks of the 21st century.

The methodology adopted in this study was designed to enable a broad, critical, and interdisciplinary understanding of cybersecurity in the contemporary context. Given the complexity and constant evolution of the subject, a qualitative and exploratory approach was chosen, allowing for an in-depth analysis of social and technological phenomena, with an emphasis on interpreting the meanings, contexts, and relationships involved. The choice of this approach is based on the need to understand information security not merely as a set of technical practices, but as a dynamic field encompassing human, legal, ethical, and organizational dimensions. According to Minayo (2016), qualitative research seeks to capture reality in its entirety, considering the interaction between subjects and the contexts in which they are embedded, which is well-suited to the nature of this work.

The research is exploratory in nature, as it aims to investigate and discuss a topic in constant transformation and with multiple theoretical and practical facets. As Gil (2019) explains, this type of study is appropriate when the objective is to broaden understanding of a given phenomenon and identify variables, relationships, and trends that are still not well established. Thus, the study sought to explore the challenges and strategies of cybersecurity in different contexts, analyzing their implications for organizations, legislation, and society.

The method used was bibliographic and documentary research, with the purpose of gathering, analyzing, and comparing information from theoretical and normative sources that address cybersecurity and data protection. According to Lakatos and Marconi (2018), bibliographic research consists of analyzing previously published materials—such as books, scientific articles, dissertations, legislation, and technical reports—that contribute to the conceptual development of the studied topic. This methodological choice is justified by the relevance of examining the contributions of recognized authors in the field, such as Stallings (2019), Dhillon (2021), Whitman and Mattord (2022), as well as national sources like Silveira, Lunardi, and Cerqueira (2023), and Almeida and Soares (2022). Official documents were also consulted, including the General Data Protection Law (Law No. 13.709/2018), reports from ENISA (2023) and (ISC)² (2022), and international technical standards such as ISO/IEC 27001, the NIST Cybersecurity Framework, and COBIT 2019, which are widely recognized in both academic literature and professional practice.

The data collection process consisted of a systematic search for updated and relevant materials published between 2015 and 2024, available in academic databases such as SciELO, Scopus, Google Scholar, and IEEE Xplore, as well as institutional websites and official reports from government agencies and international organizations. The keywords used in the searches included “cybersecurity,” “data protection,” “information governance,” “organizational culture,” and “emerging technologies.” The selection of materials followed criteria of thematic relevance, scientific credibility, and contemporaneity, ensuring a solid and current foundation for discussion.

After collection, the materials were subjected to a qualitative analysis process, based on the content analysis technique as proposed by Bardin (2016). This technique enabled the organization and interpretation of information, identifying thematic categories such as “information security management,” “legal and normative frameworks,” “technological risks,” “education and organizational culture,” and “future perspectives.” The central ideas extracted from the sources were compared and synthesized to allow for a critical and integrated reading of the phenomenon under study. This stage was essential for relating theoretical content to real-world practices and the challenges faced by organizations and society today.

The methodology was structured to ensure coherence between the objectives and the procedures adopted, guaranteeing that the analyses and discussions presented were grounded in solid theoretical foundations and recognized empirical evidence. The study was developed in five main stages: (1) Preliminary survey of theoretical and documentary references; (2) Definition of analytical categories and organization of materials; (3) Critical reading and interpretation of selected texts; (4) Elaboration of results and discussion, relating theory and practice; (5) Construction of conclusions and proposals for future research. This methodological sequence enabled both a panoramic and in-depth view of cybersecurity, highlighting its interconnections with technological innovation, legislation, and organizational culture.

Finally, it is important to emphasize that the qualitative and bibliographic nature of this research did not aim to quantify data, but rather to understand meanings, relationships, and impacts. The study sought, above all, to reflect on possible paths toward the consolidation of a sustainable and ethical information security culture. The adopted methodology allowed for the construction of a critical and interpretative analysis, aligned with the complexity of the topic and the ongoing transformations in digital society. In this way, the methodological path taken in this work provided the necessary foundation for the development of the following chapters, which present the theoretical framework, discussion of results, and final considerations, reaffirming this study’s commitment to producing knowledge that is both relevant and applicable to the reality of contemporary cybersecurity.

The results obtained in this study demonstrate that cybersecurity has been consolidated as a strategic dimension of organizational governance and digital sovereignty. The integrated analysis of bibliographic sources and technical documents revealed that the current landscape is marked by complex and dynamic challenges, ranging from the advancement of digital threats to the need for consolidating a global culture of information protection.

The investigation showed that the evolution of threats parallels the growth of connectivity and technological dependence. According to Stallings (2019), the increase in digitalization expands the exposure surface of institutions, making them more susceptible to sophisticated attacks. This vulnerability is exacerbated by human error and the lack of awareness policies—an aspect highlighted by Silveira, Lunardi, and Cerqueira (2023), who emphasize the influence of organizational behavior and cultural values on the effectiveness of security standards. Thus, building a solid information culture proves to be as necessary as investing in protection technologies.

The results also indicated that Brazil has made consistent progress in the legal domain, particularly with the enactment of the General Data Protection Law (Law No. 13.709/2018) and the creation of regulatory instruments such as the National Cybersecurity Strategy (Brazil, 2020). These measures represent milestones in the institutionalization of information governance, but still face challenges regarding practical implementation and the technical training of professionals responsible for executing these policies (Almeida & Soares, 2022).

To understand the relationship between the various technical and legal frameworks applicable to cybersecurity, Table 2 presents a synthesis of the main characteristics and purposes of the normative frameworks analyzed in this research.

Table 2 – Main Characteristics and Purposes of Normative Frameworks

Framework / Standard	Origin / Institution	Main Focus	Methodological Approach	Practical Applicability
ISO/IEC 27001	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)	Information security management	PDCA cycle (Plan, Do, Check, Act)	Creation and maintenance of Information Security Management Systems (ISMS) in public and private organizations
NIST Cybersecurit y Framework	National Institute of Standards and Technology (EUA)	Identification and mitigation of cyber risks	Structure based on five functions: Identify, Protect, Detect, Respond, and Recover	Applicable to organizations across various sectors; flexible and adaptable to national contexts
COBIT (v.5 and 2019)	ISACA – Information Systems Audit and Control Association	IT governance and control	Integrates corporate goals with security management practices	Focused on governance and auditing of technological processes
LGPD (Law No. 13.709/2018)	Federal Government of Brazil	Personal data protection and privacy	Legal and regulatory principles	Applicable to all data processing agents within national territory
GDPR (General Data Protection Regulation)	European Union	Privacy and international data transfers	Extraterritorial regulation focused on consent and accountability	Serves as a model for privacy legislation in various countries

Source: Adapted from Whitman e Mattord (2022); Dhillon (2021); Haes e Van Grembergen (2020); Almeida e Soares (2022); Kuner (2020).

The comparison presented in Table 2 reveals that technical standards (such as ISO and NIST) provide an operational and methodological foundation, while legislation such as the LGPD and GDPR constitute the legal framework necessary to guarantee fundamental rights and institutional accountability. The integration of these references is essential for strengthening digital resilience and consolidating a culture of data protection. According to Dhillon (2021), security maturity depends on a balanced combination of governance, technology, and human behavior.

Another significant finding concerns the adoption of new technologies and their impact on cybersecurity. The research showed that although tools such as cloud computing, the Internet of Things (IoT), and blockchain offer gains in efficiency and connectivity, they also introduce new vulnerabilities. Cândido and Araújo Júnior (2022) emphasize that cloud data storage requires strict access control policies and clear contractual clauses regarding responsibility. João, Souza, and Serralvo (2019) warn that IoT expands the attack surface, demanding specific security measures such as distributed authentication and continuous monitoring.

To illustrate the impact of these technologies, Table 3 summarizes the main risks and mitigation strategies.

Table 3 – Main Risks and Mitigation Strategies

Technology	Main Risks	Mitigation Measures	References
Cloud Computing	Data leakage, DDoS attacks, account hijacking	Encryption, multi-factor authentication, backup policies, clear SLA contracts	Cândido; Araújo Júnior (2022); Castro; Alves (2021)
Internet of Things (IoT)	Vulnerable devices, lack of standardization, sensor attacks	Automatic updates, distributed authentication, decentralized architecture	João; Souza; Serralvo (2019); Rosa; Souza; Silva (2020)
Blockchain	Risks of tracking and excessive control	Ethical governance, decentralized auditing, privacy-preserving encryption	Almada; Costa (2023)
Artificial Intelligence and Machine Learning	Algorithmic bias, data manipulation, misuse	Algorithmic transparency, ethical and explainable learning, human oversight	Mitchell (1997); Hagendorff (2020); LeCun et al. (2015)

Source: own elaboration based on the references analyzed.

The results presented demonstrate that although technology is part of the solution, it can also be a vector of vulnerability when not accompanied by appropriate ethical and regulatory policies. Almada and Costa (2023) emphasize that blockchain, for example, should not be adopted solely for its technical potential, but also based on critical reflection about its social and political impacts. This finding reinforces the notion that cybersecurity is a multidimensional construct, involving science, law, ethics, and culture.

In the field of Artificial Intelligence, the research highlighted the growing role of Machine Learning in threat detection and incident response automation. According to LeCun et al. (2015) and Mitchell (1997), AI-based systems can identify anomalous patterns in real time and significantly reduce response times to attacks. However, risks related to algorithmic bias and misuse of technology remain ethical and technical obstacles that must be addressed through transparency policies and continuous auditing (Hagendorff, 2020).

The discussion of results leads to the conclusion that the effectiveness of cybersecurity depends on three interdependent dimensions:

1. Institutional governance, represented by standards and laws (ISO, NIST, LGPD, GDPR);
2. Technological innovation, supported by research in AI, blockchain, and IoT;
3. Organizational culture, which integrates awareness and ethical responsibility.

This triad constitutes the core of a sustainable digital security policy, capable of ensuring protection, privacy, and trust in the information age. According to Tankard (2011) and Silveira, Lunardi,

and Cerqueira (2023), the success of cybersecurity lies not only in the tools themselves, but in the human capacity to understand, apply, and improve them in favor of a safer and more just society.

Cybersecurity has emerged as one of the major challenges of the 21st century, reflecting the direct impact of digital transformation on human life, organizations, and states. This study sought to understand this phenomenon from a broad perspective, analyzing the main challenges, strategies, and future prospects for data protection in digital environments. Throughout the research, it became evident that technological advancement, while promoting efficiency and connectivity, also intensifies vulnerabilities and expands the reach of cyber threats, requiring increasingly sophisticated and integrated responses. Thus, cybersecurity reveals itself not merely as a technical issue, but as an interdisciplinary field that interweaves technology, law, ethics, and organizational culture.

The objectives proposed were achieved throughout the development of the study. The analysis of bibliographic and documentary sources demonstrated that the effectiveness of security policies depends directly on the integration of normative frameworks, technological innovation, and a culture of awareness. From the literature review, it was found that standards such as ISO/IEC 27001, the NIST Cybersecurity Framework, and COBIT play a fundamental role in structuring internal policies and managing risks, offering methodological foundations for implementing information security systems. At the same time, legislation such as Brazil's General Data Protection Law (LGPD) and the European Union's General Data Protection Regulation (GDPR) reinforce the commitment to transparency, privacy, and social responsibility, establishing essential legal standards for digital governance.

The research also confirmed the hypothesis that effective protection of data and information depends on a balance between technology, regulation, and education. Technology alone is not sufficient to prevent cyber threats if it is not accompanied by ethical policies and a consolidated security culture. In this regard, authors such as Dhillon (2021) and Silveira, Lunardi, and Cerqueira (2023) emphasize that the human factor remains the most vulnerable—and at the same time, the most decisive—element for the effectiveness of information security. Awareness, continuous training, and digital education therefore emerge as indispensable pillars for strengthening organizational resilience.

Another relevant point identified was the need to rethink the role of emerging technologies, such as cloud computing, the Internet of Things (IoT), blockchain, and artificial intelligence, which, although they offer significant advancements, also introduce unprecedented risks. The analysis revealed that the use of these tools must be accompanied by auditing practices, ethics, and digital governance, ensuring that innovation does not become a new source of vulnerability. Artificial intelligence, for example, has proven essential for attack detection and incident response automation, but raises concerns about algorithmic bias and misuse of data, which require specific regulation and transparency in the development of intelligent systems.

The study also highlighted the global shortage of qualified cybersecurity professionals, as reported by (ISC)² (2022) and ENISA (2023). This deficit represents one of the greatest bottlenecks to the

advancement of digital security and reinforces the need for investment in technical education, continuous training, and public policies aimed at developing specialists. In this regard, cooperation among universities, companies, and governments is essential for building a more robust and sustainable culture of protection.

Overall, the results obtained allow us to conclude that cybersecurity must be understood as a continuous and multidimensional process, requiring coordinated efforts among various social actors. Building a secure digital environment demands ethical commitment, technological innovation, and collective responsibility. The triad formed by technology, legislation, and education constitutes the foundation of an effective security strategy, capable of promoting not only the protection of systems and data but also the preservation of trust and fundamental rights in the information age.

Finally, this study contributes to the academic debate by reaffirming that cybersecurity is a strategic dimension of contemporary society, directly linked to democracy, privacy, and digital sovereignty. More than a set of technical practices, it presents itself as a social and ethical project, essential to maintaining freedom and the integrity of human relationships in an increasingly connected world. For future research, it is recommended to deepen empirical studies that analyze concrete cases of security policy implementation, as well as to investigate the impact of artificial intelligence and new international regulations on the Brazilian landscape. In doing so, it will be possible to advance the construction of a cybersecurity model that unites innovation, ethics, and sustainability, contributing to a safer, more conscious, and equitable digital society.

1. Alkhalil, Z.; Hewage, C.; Nawaf, L.; Khan, I. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science, v. 3, 2021. Available at: https://doi.org/10.3389/fcomp.2021.563060 . Accessed on: 15 Sept. 2025.

2. Almeida, S. do C. D. de; Soares, T. A. Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital [The Impacts of the General Data Protection Law – LGPD in the Digital Scenario]. Perspectivas em Ciência da Informação, v. 27, n. 3, p. 26–45, July 2022. Available at: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/ . Accessed on: 09 Sept. 2025.

3. Almada, P. E. R.; Costa, E. S. Controle e vigilância no capitalismo digital: uma análise da tecnologia blockchain e sua implementação empresarial [Control and Surveillance in Digital Capitalism: An Analysis of Blockchain Technology and Its Business Implementation]. Cadernos EBAPE.BR, v. 21, n. 1, p. e2022–0020, 2023. Available at: https://www.scielo.br/j/cebape/a/Z3PQHS9JcsQq9wCVPC5c4kH/. Accessed on: 09 Sept. 2025.

4. Anderson, R. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras [Countermeasures in Information Security and Cyber Vulnerability: Empirical Evidence from Brazilian Companies]. Revista de Administração (São Paulo), v. 48, n. 4, p. 757–769, 2001. Available at: https://www.scielo.br/j/rausp/a/tH7hv6Jh3YcdjBNgsgzfXSM/#. Accessed on: 28 Sept. 2025.

5. Anderson, Ross; Böhme, Rainer; Clayton, Richard; Moore, Tyler. Security Economics and the Internal Market. European Network and Information Security Agency – ENISA, 2008. Available at: https://www.enisa.europa.eu/sites/default/files/publications/report_sec_econ_%26_int_mark_20080131.pdf. Accessed on: 28 Sept. 2025.

6. Araujo, Márcio T.; Ferreira, Fernando Nicolau Freitas. Política de Segurança da Informação [Information Security Policy]. 2. ed. Rio de Janeiro: Ciência Moderna, 2009.

7. Bada, A.; Sasse, M. A.; Nurse, J. R. C. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672, 2019. Available at: https://arxiv.org/pdf/1901.02672. Accessed on: 28 Sept. 2025.

8. Bauman, Zygmunt. Vigilância líquida [Liquid Surveillance]. Rio de Janeiro: Zahar, 2017.

9. Boer, M.; Vazquez, J. Cyber Security & Financial Stability: how cyber-attacks could materially impact the global financial system. Institute of International Finance, Sept. 2017. Available at: https://www.iif.com/Publications/ID/228/Cyber-Security-Financial-Stability-How-Cyber-attacks-Could-Materially-Impact-the-Global-Financial-System. Accessed on: 28 Sept. 2025.

10. Bosworth, S.; Kabay, M. E.; Whitman, M. E. Computer Security Handbook. 6. ed. Hoboken: Wiley, 2014.

11. Brasil. Constituição da República Federativa do Brasil de 1988 [Constitution of the Federative Republic of Brazil of 1988]. Brasília, DF: Senado Federal, 1988. Available at: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Accessed on: 28 Sept. 2025.

12. Brasil. Decreto nº 12.573, de 4 de agosto de 2025 [Decree No. 12.573 of August 4, 2025]. Institui a Estratégia Nacional de Cibersegurança – E-Ciber e dispõe sobre a sua governança [Establishes the National Cybersecurity Strategy – E-Ciber and Provides for Its Governance]. Diário Oficial da União: seção 1,

Brasília, DF, 5 Aug. 2025. Available at: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm. Accessed on: 6 Nov. 2025.

13. Brasil. Decreto Legislativo nº 37, de 2021 [Legislative Decree No. 37 of 2021]. Aprova o texto da Convenção de Budapeste sobre Crimes Cibernéticos [Approves the Text of the Budapest Convention on Cybercrime]. Diário Oficial da União: Brasília, DF, 2023. Available at: https://legislacao.presidencia.gov.br/atos/?tipo=DLG&numero=37&ano=2021&data=16/12/2021&ato=e95QTRU9UMZpWT48a. Accessed on: 17 Sept. 2025.

14. Brasil. Discurso da Presidenta da República Federativa do Brasil, Dilma Rousseff, na 68ª Assembleia-Geral da ONU [Speech by the President of the Federative Republic of Brazil, Dilma Rousseff, at the 68th UN General Assembly]. Nova York, 24 Sept. 2013. Available at: https://www.gov.br/mre/pt-br/centrais-de-conteudo/publicacoes/discursos-artigos-e-entrevistas/presidente-da-republica/presidente-da-republica-federativa-do-brasil-discursos/dilma-vana-rousseff-2011-2016/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68-assembleia-geral-das-nacoes-unidas. Accessed on: 25 Sept. 2025.

15. Brasil. Lei Geral de Proteção de Dados (LGPD) [General Data Protection Law]. 2018. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed on: 17 Sept. 2025.

16. Brasil. Lei nº 12.737, de 30 de novembro de 2012 [Law No. 12.737 of November 30, 2012]. Dispõe sobre a tipificação criminal de delitos informáticos [Provides for the Criminal Typification of Computer Crimes]. Diário Oficial da União: Brasília, DF, 2012. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Accessed on: 17 Sept. 2025.

17. Brasil. Lei nº 12.965, de 23 de abril de 2014 [Law No. 12.965 of April 23, 2014]. Marco Civil da Internet [Brazilian Civil Rights Framework for the Internet]. Diário Oficial da União: Brasília, DF, 2014. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Accessed on: 17 Sept. 2025.

18. Brasil. Lei nº 14.155, de 27 de maio de 2021 [Law No. 14.155 of May 27, 2021]. Altera o Código Penal para dispor sobre crimes cibernéticos [Amends the Penal Code to Provide for Cybercrimes]. Diário Oficial da União: Brasília, DF, 2021. Available at: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=14155&ano=2021&ato=3a4cXUU5UMZpWT48d. Accessed on: 09 Sept. 2025.

19. Brasil. Escola Superior de Defesa. Exercício Guardião Cibernético é realizado na ESD com participação recorde [Cyber Guardian Exercise Held at ESD with Record Participation]. Brasília: ESD, 16 Sept. 2025. Available at: https://www.gov.br/esd/pt-br/central-de-conteudo/noticias/exercicio-guardiao-cibernetico-e-realizado-na-esd-com-participacao-recorde. Accessed on: 23 Oct. 2025.

20. Biden White House. National Cybersecurity Strategy. Washington, DC: The White House, 2023. Available at: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. Accessed on: 24 Oct. 2025.

21. Cândido, A. C.; Araújo Júnior, R. H. de. Potencialidades do desenvolvimento de cloud computing no âmbito da gestão da informação [Potentialities of Cloud Computing Development in the Context of Information Management]. Perspectivas em Ciência da Informação, v. 27, n. 1, p. 57–80, Jan. 2022. Available at: https://www.scielo.br/j/pci/a/rXjTqsQByRGZp6NQxSr8Wyw/. Accessed on: 09 Sept. 2025.

22. Candido, J. W.; Florian, F.; Borges, J. H. G. Segurança da informação com foco na propagação iminente de ransomware nas corporações [Information Security Focused on the Imminent Spread of Ransomware in Corporations]. Revista Foco, v. 16, n. 5, e1766, 2023. Available at: https://doi.org/10.54751/revistafoco.v16n5-024. Accessed on: 20 Sept. 2025.

23. Castells, Manuel. A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade [The Internet Galaxy: Reflections on the Internet, Business, and Society]. Rio de Janeiro: Zahar, 2003.

24. Castro, F. F. de; Alves, R. C. V. Cloud Services e o padrão PREMIS rumos para a preservação digital [Cloud Services and the PREMIS Standard: Directions for Digital Preservation]. RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação, v. 19, p. e021001, 2021. Available at: https://www.scielo.br/j/rdbci/a/X3xQTJ49mGpMcH7rzscDYtz/. Accessed on: 09 Sept. 2025.

25. Cepik, M. A. C. Espionagem e democracia: agências de inteligência e política externa no Brasil [Espionage and Democracy: Intelligence Agencies and Foreign Policy in Brazil]. Belo Horizonte: Editora UFMG, 2018.

26. China. China Military Power – Modernizing a Force to Fight and Win, 2019. Available at: https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/China_Military_Power.pdf. Accessed on: 16 Sept. 2025.

27. Clarke, R.; Knake, R. Cyber War: The Next Threat to National Security and What to Do About It. Rio de Janeiro: Brasport, 2015.

28. Clearsale. Engenharia social: o que é, tipos de ataque, técnicas e como se proteger [Social Engineering: What It Is, Types of Attacks, Techniques, and How to Protect Yourself]. 2022. Available at: https://br.clear.sale/blog/engenharia-social-o-que-e-e-como-se-proteger. Accessed on: 17 Sept. 2025.

29. Cloudflare. O que é um ataque de negação de serviço (DoS)? [What Is a Denial-of-Service (DoS) Attack?]. [s.d.]. Available at: https://www.cloudflare.com/pt-br/learning/ddos/glossary/denial-of-service/. Accessed on: 16 Sept. 2025.

30. Clough, Jonathan. Principles of Cybercrime. New York: Cambridge University Press, 2010.

31. Compugraf. Quem é quem em um ataque de Engenharia Social [Who's Who in a Social Engineering Attack]. 2020. Available at: https://www.compugraf.com.br/blog/engenharia-social-quem-e-quem/. Accessed on: 16 Sept. 2025.

32. Cortez, I. S.; Kubota, L. C. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras [Countermeasures in Information Security and Cyber Vulnerability: Empirical Evidence from Brazilian Companies]. Revista de Administração (São Paulo), v. 48, n. 4, p. 757–769, 2013. Available at: https://www.scielo.br/j/rausp/a/tH7hv6Jh3YcdjBNgsgzfXSM/. Accessed on: 10 Sept. 2025.

33. Cortes, C.; Vapnik, V. Support-vector networks. Machine Learning, v. 20, p. 273–297, 1995. Available at: https://doi.org/10.1007/BF00994018. Accessed on: 10 Sept. 2025.

34. Council of Europe. Budapest Convention on Cybercrime. Strasbourg: Council of Europe, 2022. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed on: 10 Sept. 2025.

35. Creemers, R. Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century. Journal of Contemporary China, v. 25, n. 101, p. 85–100, 2016. Available at: https://www.tandfonline.com/doi/full/10.1080/10670564.2016.1206281. Accessed on: 10 Sept. 2025.

36. Cremonini, M.; Nizovtsev, D. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras [Countermeasures in Information Security and Cyber Vulnerability: Empirical Evidence from Brazilian Companies]. Revista de Administração (São Paulo), v. 48, n. 4, p. 757–769, 2006. Available at: https://www.scielo.br/j/rausp/a/tH7hv6Jh3YcdjBNgsgzfXSM/#. Accessed on: 10 Sept. 2025.

37. Devlin, J. et al. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. arXiv:1810.04805, 2019. Available at: https://arxiv.org/abs/1810.04805. Accessed on: 10 Sept. 2025.

38. Doneda, Danilo. Da privacidade à proteção de dados pessoais [From Privacy to Personal Data Protection]. São Paulo: Thomson Reuters Brasil, 2019.

39. Doneda, D. A Lei Geral de Proteção de Dados Pessoais (LGPD) e a proteção da privacidade no Brasil [The General Data Protection Law (LGPD) and Privacy Protection in Brazil]. 2. ed. São Paulo: Revista de Direito Privado, 2020.

40. Enisa – European Union Agency for Cybersecurity. Annual Report - Trust Services Security Incidents 2023. 2023. Available at: https://www.enisa.europa.eu/publications/annual-report-trust-services-security-incidents-2023. Accessed on: 10 Sept. 2025.

41. Fernandes, D. A. B.; Soares, L. F. B.; Gomes, J. V.; Freire, M. M.; Inácio, P. R. M. Security issues in cloud environments: a survey. International Journal of Information Security, v. 20, n. 2, p. 123–158, 2013. Available at: https://link.springer.com/article/10.1007/s10207-013-0208-7. Accessed on: 10 Sept. 2025.

42. Feng, S. et al. Intelligent driving intelligence test for autonomous vehicles with naturalistic and adversarial environment. Nature Communications, v. 12, p. 748, 2021. Available at: https://www.nature.com/articles/s41467-021-21007-8. Accessed on: 10 Sept. 2025.

43. Fonte, Edison Luiz Gonçalves. Segurança da informação: o usuário faz a diferença [Information Security: The User Makes the Difference]. Rio de Janeiro: Saraiva, 2007.

44. Gama, J. A survey on learning from data streams: current and future trends. Progress in Artificial Intelligence, v. 1, n. 1, p. 45–55, 2012. Available at: https://link.springer.com/article/10.1007/s13748-011-0002-6. Accessed on: 10 Sept. 2025.

45. Gartzke, E. The Myth of Cyberwar: bringing war in cyberspace back down to Earth. International Security, Cambridge, v. 38, n. 2, p. 41–73, Oct. 2013. Available at: https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136. Accessed on: 28 Sept. 2025.

46. Gragido, Will; Molina, Daniel; Pirc, John; Selby, Nick; Hay, Andrew. Blackhatonomics: An Inside Look at the Economics of Cybercrime. Waltham: Elsevier, 2013.

47. Hagendorff, T. The Ethics of AI Ethics: An Evaluation of Guidelines. Minds & Machines, v. 30, p. 99–120, 2020. Available at: https://link.springer.com/article/10.1007/s11023-020-09517-8. Accessed on: 10 Sept. 2025.

48. Hurel, Louise Marie; Lobato, Luisa Cruz. Uma estratégia para a governança da segurança cibernética no Brasil [A Strategy for Cybersecurity Governance in Brazil]. Instituto Igarapé, Nota Estratégica n. 30, Sept. 2018. Available at: https://igarape.org.br/wp-content/uploads/2018/09/Uma-estrate%CC%81gia-para-a-governanc%CC%A7a-da-seguranc%CC%A7a-ciberne%CC%81tica-no-Brasil.pdf. Accessed on: 15 Oct. 2025.

49. IBM Security. Cost of a Data Breach Report 2024. Armonk, NY: IBM Corporation, 2024. Available at: https://www.ibm.com/security/data-breach. Accessed on: 28 Sept. 2025.

50. Interpol. 2022 INTERPOL Global Crime Trend Summary Report. Lyon: Interpol, 2022. Available at: https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf. Accessed on: 10 Sept. 2025.

51. International Institute for Strategic Studies (IISS). Strategic Survey 2018: The Annual Assessment of Geopolitics. London: IISS, 2018. Available at: https://www.iiss.org/publications/strategic-survey/strategic-survey-2018-the-annual-assessment-of-geopolitics/. Accessed on: 10 Sept. 2025.

52. International Organization for Standardization. ISO/IEC 27005:2018: Information technology — Security techniques — Information security risk management. Geneva: ISO, 2018.

53. João, B. D. N.; Souza, C. L. D.; Serralvo, F. A. A systematic review of smart cities and the internet of things as a research topic. Cadernos EBAPE.BR, v. 17, n. 4, p. 1115–1130, Oct. 2019. Available at: https://www.scielo.br/j/cebape/a/mBqjGxPSbRKPsXcS99z8LrD/. Accessed on: 09 Sept. 2025.

54. Juncker, Jean-Claude. Discurso sobre o estado da União [State of the Union Address]. 2017. Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165. Accessed on: 09 Sept. 2025.

55. Kaspersky. Ransomware attacks in 2023: Evolution and trends. Moscow: Kaspersky Lab, 2023. Available at: https://www.kaspersky.com/blog/ransowmare-attacks-in-2023/50634/. Accessed on: 09 Sept. 2025.

56. Kshetri, N. Cybersecurity Management: An Organizational and Strategic Approach. Toronto: University of Toronto Press, 2021. DOI: 10.3138/9781487531249. Available at: https://www.researchgate.net/publication/359034950_Cybersecurity_Management_An_Organizational_and_Strategic_Approach. Accessed on: 23 Oct. 2025.

57. Kuner, C. The General Data Protection Regulation: A Commentary. Oxford: Oxford University Press, 2020.

58. Laudon, Kenneth; Laudon, Jane. Sistemas de informações gerenciais [Management Information Systems]. São Paulo: Pearson Universidades, 2014.

59. LeCun, Y. et al. Deep learning. Nature, v. 521, p. 436–444, 2015. Available at: https://www.nature.com/articles/nature14539. Accessed on: 09 Sept. 2025.

60. Lloyd's of London. Estimativas de perdas financeiras devido a ciberataques [Estimates of Financial Losses Due to Cyberattacks]. July 2017. Available at: https://www.sindsegrs.com.br/2017/07/20/ciberataque-extremo-pode-custar-us-53-bilhoes-revela-estudo-do-lloyds-of-london/. Accessed on: 10 Sept. 2025.

61. Lopes, L. Security Officer. 2014. Available at: https://www.jusbrasil.com.br/artigos/security-officer/153252634. Accessed on: 10 Sept. 2025.

62. Malwarebytes. Phishing. [s.d.]. Available at: https://br.malwarebytes.com/phishing/. Accessed on: 15 Apr. 2025.

63. McCulloch, W. S.; Pitts, W. A logical calculus of the ideas immanent in nervous activity. Bulletin of Mathematical Biophysics, v. 5, p. 115–133, 1943. Available at: https://doi.org/10.1007/BF02478259. Accessed on: 10 Sept. 2025.

64. Microsoft. O que é ransomware? [What Is Ransomware?]. [s.d.]. Available at: https://www.microsoft.com/pt-br/security/business/security-101/what-is-ransomware. Accessed on: 20 Sept. 2025.

65. Mitchell, T. Machine Learning. S. l.: McGraw Hill, 1997.

66. Morgan, S. Cybercrime Damages $6 Trillion By 2021. Menlo Park, Calif.: Cybersecurity Ventures, 16 Oct. 2017. Available at: https://cybersecurityventures.com/annual-cybercrime-report-2017/Cybercrime. Accessed on: 15 Oct. 2025.

67. Netexperts. Conceitos éticos que guiam as decisões de cibersegurança [Ethical Concepts Guiding Cybersecurity Decisions]. 2023. Available at: https://netexperts.com.br/conceitos-eticos-que-guiam-as-decisoes-de-ciberseguranca/. Accessed on: 10 Sept. 2025.

68. Nye, Joseph S. The Future of Power. New York: PublicAffairs, 2011.

69. OCDE. Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. 2012. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2012/11/cybersecurity-policy-making-at-a-turning-point_g17a21e7/5k8zq92vdgtl-en.pdf. Accessed on: 28 Sept. 2025.

70. Otter, D. W. et al. A survey of the usages of deep learning for natural language processing. IEEE Transactions on Neural Networks and Learning Systems, v. 32, n. 2, p. 604–624, 2020. Available at: https://doi.org/10.1109/tnnls.2020.2979670. Accessed on: 10 Sept. 2025.

71. Perallis. Engenharia social, a arte de manipular os sentimentos do ser humano [Social Engineering: The Art of Manipulating Human Emotions]. [s.d.]. Available at: https://www.perallis.com.br/news/tudo-o-que-voce-queria-saber-sobre-engenharia-social. Accessed on: 10 Sept. 2025.

72. Ravanelli, M. et al. Multi-task self-supervised learning for robust speech recognition. In: ICASSP 2020 – IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Barcelona, 2020. p. 6989–6993. Available at: https://ieeexplore.ieee.org/document/9053569. Accessed on: 10 Sept. 2025.

73. Renato Costa, R. B. A Lei Geral de Proteção de Dados Pessoais aplicada à Internet das Coisas: uma revisão sistemática [The General Data Protection Law Applied to the Internet of Things: A Systematic Review]. 2022. Available at: https://repositorio.ufc.br/bitstream/riufc/66631/1/2022_tcc_rbcosta.pdf. Accessed on: 09 Sept. 2025.

74. Rezende, Denis Alcides. Governança de tecnologia da informação e comunicação: fundamentos, modelos e aplicação nas organizações [Governance of Information and Communication Technology: Fundamentals, Models, and Application in Organizations]. 3. ed. São Paulo: Atlas, 2020.

75. Rid, Thomas. Cyber War Will Not Take Place. London: Oxford University Press, 2020.

76. Rosa, C. M.; Souza, P. A. R. de; Silva, J. M. da. Inovação em saúde e internet das coisas (IoT): Um panorama do desenvolvimento científico e tecnológico [Innovation in Health and Internet of Things (IoT): An Overview of Scientific and Technological Development]. Perspectivas em Ciência da Informação, v. 25, n. 3, p. 164–181, July 2020. Available at: https://www.scielo.br/j/pci/a/hsKV8qkqbCztFscHPPXBxRc/. Accessed on: 09 Sept. 2025.

77. Rosenblatt, F. The Perceptron – A perceiving and recognizing automaton. Report 85-460-1. Cornell Aeronautical Laboratory, Nov. 1957.

78. Rumelhart, D. E. et al. Learning representations by back-propagating errors. Nature, v. 323, p. 533–536, 1986. Available at: https://www.nature.com/articles/323533a0. Accessed on: 09 Sept. 2025.

79. Santos, C. S. A. dos et al. Proposta de avaliação da Política Nacional de Segurança da Informação por Processo de Análise Hierárquica [Proposal for Evaluating the National Information Security Policy Using Hierarchical Analysis Process]. Perspectivas em Ciência da Informação, v. 27, n. 4, p. 108–145, Oct. 2022. Available at: https://www.scielo.br/j/pci/a/ks9gSpJbgRNJP9vZxbfHJqL/. Accessed on: 09 Sept. 2025.

80. Saracco, R. Congrats Xiaoyi. You are now a medical doctor. IEEE Future Directions, 2017. Available at: https://cmte.ieee.org/futuredirections/2017/12/02/congrats-xiaoyi-you-are-now-a-medical-doctor/. Accessed on: 10 Sept. 2025.

81. Schmidt, Guilherme. Crimes cibernéticos [Cybercrimes]. 2014. Available at: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Accessed on: 28 Sept. 2025.

82. Schneier, B. Security Officer. [s.d.]. Available at: https://www.jusbrasil.com.br/artigos/security-officer/153252634. Accessed on: 10 Sept. 2025.

83. Shor, P. W. Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, p. 124–134, 1994.

84. Silveira, J. R.; Lunardi, G. L.; Cerqueira, L. S. Relação entre cultura e segurança da informação: como evitar falhas decorrentes do “jeitinho brasileiro” [Relationship Between Culture and Information Security: How to Avoid Failures Due to the “Brazilian Way”]. REAd. Revista Eletrônica de Administração, v. 29, n. 1, p. 143–170, Jan. 2023. Available at: https://www.scielo.br/j/read/a/mXzJBPHSXLkxTFPBVGMhkqs/?format=html&lang=pt. Accessed on: 09 Sept. 2025.

85. Spyman. Hacking: manual completo do hacker [Hacking: Complete Hacker Manual]. 3. ed. São Paulo: Book Express, 2000.

86. Stallings, W. Cryptography and Network Security: Principles and Practice. 8. ed. Boston: Pearson, 2019.

87. Stallings, W. Fundamentals of Information Systems Security. 2. ed. Upper Saddle River: Pearson, 2017.

88. Stallings, William. Computer Security: Principles and Practice. 4. ed. New Jersey: Pearson, 2019.

89. Tanenbaum, A. S.; Wetherall, D. J. Computer Networks. 5. ed. Upper Saddle River: Pearson, 2011.

90. Tanenbaum, A. S.; Wetherall, D. J. Redes de Computadores [Computer Networks]. 5. ed. São Paulo: Pearson, 2011.

91. Tankard, Colin. Advanced Persistent Threats and how to monitor and deter them. Network Security, v. 2011, n. 8, p. 16–19, 2011. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1353485811700861. Accessed on: 10 Sept. 2025.

92. Torfi, A. et al. Natural language processing advancements by deep learning: A survey. arXiv preprint arXiv:2003.01200, 2020. Accessed on: 10 Sept. 2025.

93. Turing, A. M. Computing Machinery and Intelligence. Mind, LIX, v. 236, p. 433–460, 1950.

94. United States. National Cyber Strategy of the United States of America. Washington, DC: The White House, 2018. Available at: https://www.hsdl.org/?view&did=810563. Accessed on: 10 Sept. 2025.

95. Varian, H. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras [Countermeasures in Information Security and Cyber Vulnerability: Empirical Evidence from Brazilian Companies]. Revista de Administração (São Paulo), v. 48, n. 4, p. 757–769, 2004. Available at: https://www.scielo.br/j/rausp/a/tH7hv6Jh3YcdjBNgsgzfXSM/#. Accessed on: 10 Sept. 2025.

96. Vetis-Zaganelli, M.; Binda Filho, D. L. A Lei Geral de Proteção de Dados e suas implicações na saúde: as avaliações de impacto no tratamento de dados no âmbito clínico-hospitalar [The General Data Protection Law and Its Implications in Health: Impact Assessments in Clinical-Hospital Data Processing]. Rev. Bioética y Derecho, n. 54, p. 215–232, 2022. Available at: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872022000100013. Accessed on: 09 Sept. 2025.

97. Whitman, M. E.; Mattord, H. J. Principles of Information Security. 7. ed. Boston: Cengage Learning, 2022.

98. World Economic Forum. Global Risks Report 2018. Geneva: WEF, 2018. Available at: https://www.weforum.org/reports/the-global-risks-report-2018. Accessed on: 28 Sept. 2025.

99. Zúquete, André. Segurança em redes e sistemas computacionais [Security in Networks and Computer Systems]. Lisbon: FCA, 2022.

REALIZATION:

CNPJ: 589029480001-12
contato@aurumeditora.com
(41) 98792-9544
Curitiba - Paraná
www.aurumeditora.com