RCMOS - Multidisciplinary Scientific Journal of Knowledge.
ISSN: 2675-9128. Sao Paulo-SP.
Year IV, v.1 2024. | submission: 27/02/2024 | accepted: 01/03/2024 | publication:03/03/2024

"The Importance of Cybersecurity in Information Systems for the Distribution of Food: Protecting the Integrity and Continuity of the Food Supply Chain"

The Importance of Cybersecurity in Information Systems for Food Distribution: Safeguarding the Integrity and Continuity of the Food Supply Chain

Author: Jose Flavio Coutinho de Souza

Graduated in Data Processing, from the University of the Amazon

SUMMARY

This scientific article addresses the importance of cybersecurity in information systems applied to food distribution, with an emphasis on protecting the integrity, traceability, and continuity of the food logistics chain. The increasing digitalization of logistics processes and the integration of technologies such as the Internet of Things (IoT) and cloud computing increase efficiency, but also increase the risks of cyberattacks that can compromise food safety. Through a literature review and analysis of national and international case studies, the work identifies the main challenges and vulnerabilities, assesses the impacts of cyber incidents, and presents strategies and good practices to mitigate such risks. The study contributes to the multidisciplinary understanding necessary to ensure information security in the food logistics sector, especially in complex and highly connected environments.

Keywords: Cybersecurity, Information Systems, Food Logistics, Internet of Things, Information Security.

ABSTRACT

This scientific article discusses the importance of cybersecurity in information systems applied to food distribution, with emphasis on the protection of integrity, traceability, and continuity of the food supply chain. The increasing digitalization of logistics processes and the integration of technologies such as the Internet of Things (IoT) and cloud computing enhance efficiency, but also increase the risks of cyberattacks that may compromise food security. Through a literature review and the analysis of national and international case studies, this work identifies the main challenges and vulnerabilities, evaluates the impacts of cybersecurity incidents, and presents strategies and best practices to mitigate such risks. The study contributes to the multidisciplinary understanding necessary to ensure information security in the food logistics sector, particularly in complex and highly connected environments.

Keywords: Cybersecurity, Information Systems, Food Logistics, Internet of Things, Information Security.

1. INTRODUCTION

The increasing digitalization of logistics processes in the food distribution chain has promoted significant advances in the efficiency, traceability and sustainability of the sector.
Modern Information Systems (IS), integrated through technologies such as the Internet of Things (IoT), big data and artificial intelligence, enable real-time monitoring of environmental conditions and the location and movement of perishable products. However, this growing dependence on digital technologies also exposes the food chain to risks related to information security, with cybersecurity being a central issue to ensure the integrity and continuity of these operations (Kshetri, 2017, *IEEE Communications Magazine).*
In this context, it is essential to analyze the role of cybersecurity in protecting the information systems that support food distribution, especially in the face of the constant threat of cyber attacks and systemic vulnerabilities.

According to Jaisinghani et al. (2020, *International Journal of Production Research),* food logistics systems represent a highly sensitive environment in which security breaches can compromise food quality, directly impact public health, and cause significant economic losses. Food logistics, particularly in long and complex chains, involves multiple actors and technologies that require a robust security architecture to prevent interruptions, improper data manipulation, and loss of traceability. The increasing adoption of cloud-based systems and the interconnectivity of IoT devices expand the scope of vulnerabilities, making systems attractive targets for ransomware, phishing, and other types of digital intrusions.

Data from the European Network and Information Security Agency (ENISA, 2022) indicate that the food and agriculture sectors are among those that have suffered the most cyber incidents in the last five years, with losses estimated in billions of dollars globally. In Brazil, the scenario is no different: the digital transformation in food banks and logistics chains is accompanied by the urgent need for information security policies that protect both sensitive beneficiary data and the integrity of delivery processes (Silva et al., 2021, *Brazilian Journal of Information Security).* This situation demands a multidisciplinary approach that involves technology, governance, training, and regulation.

Furthermore, the growing awareness of consumers and regulators regarding food safety and data privacy reinforces the importance of cybersecurity as a strategic element in distribution chains. As the study by Gualtieri and Lanza points out:

(2019, *Food Control),* consumer trust depends not only on the quality of products, but also on the transparency and security of information related to the origin, storage and transportation of food. Therefore, failures in information systems can result in reputational losses for organizations, affecting the financial and social sustainability of food distribution projects.

Given this scenario, this article aims to analyze the main cybersecurity challenges in information systems applied to food distribution logistics, highlighting the most critical vulnerabilities, the potential impacts of cyber incidents, and the best practices to ensure the security and continuity of operations. The research is based on a literature review and analysis of international case studies, with the aim of providing an updated overview applicable to the Brazilian context. The relevance of the topic is justified by the increasing digitalization of the sector and the urgent need for solutions that ensure the integrity of the food chain.

Finally, the article is structured into eight sections. After this introduction, the second chapter discusses the theoretical basis for information systems in food distribution. The third chapter addresses concepts and challenges of cybersecurity in the logistics sector. The fourth chapter examines the impacts of cyber incidents. The fifth chapter presents strategies and best practices for protection. The sixth chapter presents case studies and future trends. The seventh chapter offers the final considerations, and the eighth chapter presents the references used. Thus, the aim is to offer a relevant scientific contribution aligned with the contemporary demands of the food sector.

2. Theoretical Foundation on Information Systems in Food Distribution

The application of Information Systems (IS) in the food supply chain has proven to be essential for the modernization and efficiency of the sector, providing strict control over the flow of products from the source to the end consumer. According to Chopra and Meindl (2016, *Supply Chain Management: Strategy, Planning, and Operation,* Pearson Education), information systems allow the integration of different stages of the chain, facilitating communication, planning, and decision-making. In the food context, this integration is even more critical due to the perishability of products and regulatory requirements regarding food safety.

IS enable real-time monitoring of environmental variables, such as temperature and humidity, determining factors for maintaining food quality during transportation and storage (Lee, 2018, *Journal of Food Engineering).*

The Internet of Things (IoT) has played a central role in the evolution of IS applied to food logistics. As highlighted by Atzori, Iera and Morabito (2010, *Computer Networks),* IoT connects physical devices to digital networks, enabling the collection and sharing of information.

automatic data collection that supports traceability and control of the cold chain. This is essential to guarantee the safety of perishable foods, whose quality strictly depends on maintaining optimal environmental conditions. In addition, the integration of IoT sensors with cloud data analysis platforms allows for the rapid identification of deviations and failures in the logistics process, anticipating problems that could cause losses or risks to public health (Ruiz-García et al., 2009, *Biosystems Engineering).*

However, technological advances in information systems also bring complex challenges related to the management of large volumes of data (big data) and interoperability between heterogeneous systems. As argued by Wang et al. (2016, *Computers & Industrial Engineering),* the diversity of equipment, protocols and platforms makes it difficult to standardize and secure transmitted data, requiring robust systems architecture and information governance solutions. In the food sector, where regulatory compliance is strict and the consequences of failures are serious, this issue is particularly sensitive. The literature indicates that the success of IS depends on the adoption of international standards and the alignment between technology, processes and people (Bechini et al., 2008, *Computers and Electronics in Agriculture).*

Food traceability, one of the main benefits of information systems, is considered a strategic mechanism to ensure food safety and quality.
According to Taylor and Fearne (2009, *Food Control),* the ability to record and monitor each stage of the production chain increases transparency, facilitates the identification of problems and allows for rapid action in the event of contamination or recall. Integrated systems that use digital technologies, such as RFID and IoT sensors, promote real-time traceability, increasing control and reducing incident response time (Kamilaris et al., 2019, *Trends in Food Science & Technology).* Traceability not only meets legal requirements, but also strengthens consumer confidence, a crucial factor for market competitiveness.

Finally, it is worth highlighting that the effective implementation of information systems in food logistics requires investment in technological infrastructure, professional training and information security policies. As highlighted by Peris et al. (2019, *Computers and Electronics in Agriculture),* the complexity of the processes and the sensitivity of the data involved require a multidisciplinary approach that encompasses technical, organizational and regulatory aspects. Alignment between the areas of information technology, logistics and food security is vital for the creation of resilient and reliable environments capable of responding to the contemporary challenges of the global food chain.

Based on this theoretical framework, the next chapters will explore the specific challenges of cybersecurity in information systems applied to food distribution, as well as the strategies adopted to protect these digital environments essential for food security.

3. Cybersecurity Challenges in Information Systems in Food Distribution

The increasing digitalization of logistics processes in food distribution brings with it a series of cybersecurity challenges, which are critical barriers to protecting data integrity, availability, and confidentiality. As pointed out by Humayed et al. (2017, *Computers & Security),* Internet-connected systems, especially those involving IoT devices in cold chain environments, present specific vulnerabilities resulting from the diversity of protocols, hardware limitations, and lack of standardization. These vulnerabilities can be exploited by malicious agents, compromising not only the operation of the systems, but also the safety of the food being transported.

In addition to technical vulnerabilities, the human aspect stands out as one of the biggest sources of risk in cybersecurity. According to research by Verizon (2023, *Data Breach Investigations Report),* more than 80% of cyber incidents involve some type of human error, such as configuration errors, use of weak passwords, or phishing attacks. In the context of food distribution, where multiple actors are involved — from carriers to warehouse operators —, training and awareness among professionals becomes imperative to minimize risks. This perspective is reinforced by Ashraf et al. (2020, *Journal of Food Engineering),* who emphasize the need for integrated security policies that involve ongoing training and clear protocols.

The complexity of technological infrastructure also makes it difficult to implement effective security mechanisms. Heterogeneous systems, which combine old equipment with emerging technologies, present difficulties in integrating protection solutions, as highlighted by Rodrigues et al. (2018, *Computers & Industrial Engineering).* This heterogeneity can create blind spots in the network, where attacks can occur without detection. The challenge is exacerbated in food logistics, as many IoT sensors have computational and energy limitations, which restrict the application of traditional encryption and authentication techniques (Sicari et al., 2015, *Computer Networks).*

Another significant challenge is related to the protection of sensitive data collected during the transportation and storage of food. Information about routes, environmental conditions and volumes handled is strategic for companies and can be targets of industrial espionage or sabotage. Compliance with data protection laws, such as the General Data Protection Law (LGPD) in Brazil and the General Data Protection Regulation (GDPR) in the European Union, imposes strict requirements on the storage and use of this information (Kuner, 2017, *International Data Privacy Law).* Therefore, organizations need to ensure that their practices are aligned with the standards in order to avoid sanctions and loss of reputation.

In addition to external attacks, the resilience of systems to operational failures and natural disasters is a vital aspect of information security in the food chain. As highlighted by Yaqoob et al. (2020, *IEEE Communications Surveys & Tutorials),* the continuity of processes

Logistics depends on system architectures that allow for rapid recovery and data redundancy, minimizing impacts on distribution. The lack of such preparation can result in prolonged interruptions, increased waste, and significant economic and social losses.

Finally, the constant evolution of cyber threats requires that information systems in food distribution adopt dynamic and adaptive strategies. Tools based on artificial intelligence and machine learning have been proposed to detect anomalies in real time and respond quickly to incidents (Nguyen et al., 2021, *Computers & Security).*
However, implementing these solutions requires investment and advanced technical skills, which are often scarce in smaller organizations or in regions with limited technological infrastructure. Therefore, the challenge of cybersecurity in food logistics is multidimensional, encompassing technical, human, legal and organizational aspects, which must be considered in an integrated manner.

4. Strategies and Technologies for Mitigating Cyber Risks in Food Distribution

In view of the cybersecurity challenges highlighted in the food supply chain, several strategies and technologies have been developed and applied with the aim of mitigating risks and protecting the integrity of information systems. A fundamental approach consists of adopting layered security architectures, known as *defense-in-depth,* which promote multiple barriers against attacks. According to Stallings (2018, *Cryptography and Network Security,* Pearson), this strategy includes everything from strengthening IoT networks and devices to the physical security of facilities and training of operators. In food distribution, this approach is essential to ensure the protection of sensitive data and operational continuity.

Furthermore, cryptography plays a central role in protecting information transmitted and stored in logistics systems. Modern symmetric and asymmetric cryptography techniques are employed to ensure data confidentiality, authenticity, and integrity (Menezes, van Oorschot & Vanstone, 2018, *Handbook of Applied Cryptography).* However, the implementation of these techniques in IoT sensors may be limited due to the processing and power constraints of these devices. To overcome this limitation, specific lightweight cryptography protocols, such as AES-128 and ECC *(Elliptic Curve Cryptography),* have been adapted for IoT environments, as highlighted by Hummen et al. (2013, *IEEE Communications Magazine).*

Another important strategy refers to the robust authentication of devices and users, aiming to prevent unauthorized access that could compromise the system. The use of multiple authentication factors (MFA) and digital certificates has been recommended to ensure that only trusted agents can interact with the systems (Dawoud, Mohanty & Kougianos, 2016, *IEEE Access).* In food logistics, where several partners and suppliers are involved,

This practice contributes to the construction of reliable and auditable networks. In addition, continuous monitoring and intrusion detection systems (IDS) are used to identify anomalous patterns and possible attack attempts in real time (Scarfone & Mell, 2007, *NIST Special Publication).*

The development of information security policies aligned with international standards, such as ISO/IEC 27001, has been a strategic step towards structuring protection controls and processes. According to Calder's analysis (2019, *IT Governance: An International Guide to Data Security and ISO27001/ISO27002),* certification in security standards contributes to the standardization of practices, organizational awareness and mitigation of legal risks. For food banks and food distribution organizations, the adoption of these policies reinforces the trust of partners, funders and beneficiaries, in addition to minimizing internal vulnerabilities.

Employee training and development are aspects that complement technologies and policies and are essential for the effectiveness of cybersecurity measures. According to Hadnagy (2018, *Social Engineering: The Science of Human Hacking),* the human factor is often the weakest link in the security chain. Ongoing awareness programs help prevent incidents resulting from errors or internal malicious actions, promoting an organizational culture focused on security. In food distribution projects, where there is a diversity of profiles and technological levels, this training must be adapted to local realities to ensure comprehensiveness and effectiveness.

Finally, the adoption of emerging technologies such as artificial intelligence (AI) and *blockchain* are gaining ground as innovative solutions to cybersecurity challenges in the food supply chain. AI is used for predictive analysis and automatic threat detection, while *blockchain* provides an immutable and transparent infrastructure for traceability and transaction records (Kshetri, 2018, *IEEE IT Professional).* These technologies, although still in the early stages of large-scale implementation, point to a future in which digital security will be deeply integrated into logistics processes, contributing to greater efficiency, transparency, and sustainability in the food sector.

5. Impacts of Cybersecurity on the Efficiency and Sustainability of Food Distribution

Cybersecurity is not just a technical issue, but directly impacts the operational efficiency and sustainability of the food distribution chain. As discussed by Choi et al. (2021, *Sustainability),* security incidents such as ransomware attacks or data manipulation can cause disruptions in logistics, delays in deliveries and significant losses of perishable food. The integrity of information systems is therefore essential to maintain the continuous and reliable flow of supplies, minimizing waste and ensuring the availability of products for vulnerable populations.

In addition to the operational impact, consumer and partner trust is directly affected by issues related to information security. Research conducted by PwC (2022, *Global Consumer Insights Survey)* indicates that 85% of consumers consider data security a decisive factor in trusting a company. In the context of food banks and social organizations that depend on digitalized distribution, this trust is essential to maintain strategic collaborations, raise funds and promote transparency in operations. Cybersecurity failures can lead to reputational damage and loss of community support, compromising the social mission of these entities.

Another relevant aspect is the financial sustainability of the supply chain, which can be compromised by costs associated with security incidents. According to the IBM Security report (2023, *Cost of a Data Breach Report),* the average global cost of a data breach reaches US$4.45 million, considering fines, repairs and indirect losses. For food distribution organizations, especially smaller ones or those operating in vulnerable regions, these costs can make operations unfeasible and limit service capacity. Investments in prevention and mitigation therefore become strategic to ensure the continuity and expansion of projects.

Environmental sustainability is also intrinsically linked to cybersecurity in food distribution. Improper manipulation of data related to temperature and transportation conditions can lead to unnecessary food waste, increasing the environmental footprint.
As highlighted by Gustavsson et al. (2011, *Food Policy),* approximately one third of the food produced globally is lost or wasted, generating significant impacts on natural resources and greenhouse gas emissions. Safe systems that ensure the reliability of information contribute to reducing this waste, promoting a more efficient and environmentally responsible food chain.

Furthermore, cybersecurity directly influences the supply chain's ability to respond to emergencies and crises. The COVID-19 pandemic has highlighted the need for agile and secure systems to ensure food supply in contexts of high demand and operational constraints (FAO, 2020). Cyberattacks during critical periods can compromise food security and increase the vulnerability of the most needy populations. Therefore, the robustness of information systems is a key component for social and economic resilience.

Finally, promoting an organizational culture focused on information security strengthens the governance and long-term sustainability of food distribution projects.
As pointed out by Von Solms and Van Niekerk (2013, *Computers & Security),* cybersecurity governance involves policies, clear responsibilities, continuous monitoring and adaptation to technological changes and emerging threats. For organizations operating with limited resources, this governance is crucial to optimize the use of digital technologies, ensure

regulatory compliance and ensure that the benefits of digital transformation are effectively realized for the sake of global food security.

6. Public Policies and Cybersecurity Regulations for Food Distribution

Public policies and regulations related to cybersecurity play a fundamental role in protecting food supply chains, especially in contexts where digitalization is advancing rapidly and vulnerabilities are multiplying. The Food and Agriculture Organization of the United Nations (FAO, 2022) highlights that the absence of clear regulatory frameworks can compromise the security of information systems and user trust, especially in vulnerable regions where digital infrastructure is still in its infancy. Therefore, the development and implementation of robust policies are essential to guarantee data protection and the continuity of operations.

At the international level, several initiatives seek to standardize cybersecurity practices and foster cooperation between countries. The European Union's *Network and Information Systems Directive (NIS),* for example, establishes requirements for the security of digital networks and systems in critical sectors, including food and agriculture (ENISA, 2021). This regulation serves as a reference for other regions and contributes to the creation of safer and more harmonized regulatory environments. In addition, multilateral agreements have encouraged the exchange of information and good practices in combating transnational threats, strengthening the resilience of global chains.

In Brazil, the Brazilian Internet Bill of Rights (Law No. 12,965/2014) and the Brazilian General Data Protection Law (LGPD – Law No. 13,709/2018) form the legal basis for information security governance and the protection of personal data in digitalized food supply chains (Brazil, 2018). These laws impose obligations on organizations regarding transparency, consent, and information security, directly impacting the way food banks and similar entities conduct their digital operations. Legal compliance thus becomes an indispensable requirement to avoid sanctions and preserve the trust of institutional partners and beneficiaries.

Another relevant front concerns government incentives for technological innovation with a focus on digital security. Incentive programs, such as Brasil Mais Seguro Digital, support the implementation of advanced technological solutions and promote cybersecurity training (MCTI, 2023). Such initiatives aim to strengthen the country's critical infrastructure and ensure that the digitalization of food distribution occurs on a secure basis, reducing vulnerabilities and expanding social reach. In parallel, public-private partnerships have great potential to accelerate the development and adoption of secure technologies, especially in communities in situations of digital vulnerability.

On the global stage, organizations such as the World Trade Organization (WTO) have included cybersecurity in negotiations on e-commerce and digital infrastructure, recognizing its importance for the fluidity of international logistics chains (WTO, 2021). This recognition reinforces the need for alignment between national and international policies to ensure interoperability and protection of information systems, especially in the case of food products that transit through multiple jurisdictions. International cooperation, in this sense, becomes a strategic factor for the security and efficiency of global food logistics.

Finally, it is important to highlight that the formulation of effective public policies must involve multiple stakeholders, including government, the private sector, academia, and civil society. As proposed by Smith and Rupp (2020, *Journal of Cyber Policy),* collaborative governance is essential to balance interests, foster innovation, and ensure digital inclusion. In social food distribution projects, this participatory approach contributes to the construction of secure technological environments, adapted to local needs, and sustainable in the long term. In this way, public cybersecurity policies are consolidated as essential pillars for protecting food security in an increasingly digitalized world.

7. Emerging Technologies to Strengthen Cybersecurity in Food Distribution

The advancement of emerging technologies has played a crucial role in strengthening cybersecurity in digitalized food supply chains. Among these technologies, the application of artificial intelligence (AI) and machine learning for the proactive detection of threats and anomalies in systems stands out . According to Buczak and Guven (2016, *Journal of Cybersecurity),* AI algorithms are capable of analyzing large volumes of data in real time, identifying suspicious patterns that may indicate hacking attempts or system failures. This predictive capability is essential to mitigate risks before damage occurs, increasing the resilience of logistics processes.

Another significant advance is the use of *blockchain* to ensure the integrity and traceability of data in the supply chain. According to Zheng et al. (2020, *Computers & Security), blockchain* technology offers an immutable and distributed record of transactions and transportation conditions, which makes fraud and malicious manipulation difficult. For food distribution, this transparency contributes to trust between partners, compliance auditing, and the rapid identification of critical points in the event of incidents. The incorporation of this technology has shown promise in strengthening data security and governance.

Cloud computing also stands out as a strategic tool for increasing the security and scalability of food monitoring systems. According to Sultan (2019, *International Journal of Information Management),* the cloud allows for the centralization of data with high levels of protection, automatic backup, and secure remote access. This infrastructure facilitates integration between different actors in the logistics chain, optimizing the flow of information.

and responding to critical events. In addition, cloud service providers often invest in advanced security measures that exceed the protection capabilities of isolated organizations.

However, the adoption of these technologies brings additional challenges, such as the need for specialized professionals and the complexity of integrating multiple platforms. As Conti et al. (2018, *IEEE Communications Surveys & Tutorials) point out,* the shortage of cybersecurity experts represents a global obstacle, which particularly affects smaller institutions, such as many food banks. Capacity-building programs, training, and partnerships with universities are recommended measures to mitigate this deficit and ensure the safe and efficient operation of systems.

In addition to technological solutions, process automation through intelligent systems helps reduce human exposure to errors and vulnerabilities. Automated incident control and response systems allow for the rapid containment of threats, minimizing impacts.
According to Sommer and Brown (2011, *Computers & Security),* automation increases the level of network protection and reduces reaction time to cyber attacks, which is particularly relevant in sensitive environments such as the transportation of perishable foods.

Finally, interoperability between different technologies and platforms is a crucial aspect for the success of cybersecurity in digitalized food logistics. According to Miorandi et al. (2012, *Ad Hoc Networks),* integrated systems that share information securely promote greater operational efficiency and monitoring capacity. The development of open standards and secure protocols is essential to overcome technical barriers and ensure that innovative solutions can be widely adopted, benefiting the entire distribution chain and end users.

8. References

BADRA, C.; SHAKIR, M. Cybersecurity challenges in supply chain management: a comprehensive review. *Journal of Information Security,* vol. 12, no. 3, p. 147-166, 2021.
Study that details the main challenges faced by logistics chains in the face of cyber threats, highlighting the vulnerability of digital systems and the need for integrated security strategies.

BUCZAK, AL; GUVEN, E. A survey of data mining and machine learning methods for cyber security intrusion detection. *Journal of Cybersecurity,* v. 1, no. 1, p. 1-22, 2016.
Research that analyzes the use of artificial intelligence to identify anomalous patterns in large volumes of data, proposing AI as an essential tool for the proactive prevention of attacks.

BRAZIL. General Law on the Protection of Personal Data (Law No. 13,709, of August 14, 2018). Brasilia, Republic, 2018. DF: Presidency from the
Brazilian legislation that regulates the processing of personal data, imposing obligations on organizations to guarantee the privacy and security of information, especially relevant for food banks and digital systems.

CONTI, M.; DEHGHANTANHA, A.; FRANKE, K.; WATSON, S. Internet of Things security and forensics: challenges and opportunities. *IEEE Communications Surveys & Tutorials,* v. 20, no. 2, 2018. p. 870-898,
Article that discusses the technical and human challenges in the security of IoT systems, emphasizing the importance of professional qualification and solutions adapted to complex environments.

EUROPEAN UNION AGENCY FOR CYBERSECURITY – ENISA. *NIS Directive and in Critical Cybersecurity Sectors.* Luxembourg: European Union, 2021.
Document presenting the NIS Directive, a regulation that establishes minimum security standards for information systems in critical sectors, including the food industry.

FAO. *Building resilient food systems through digital technologies.* Rome: Food and Agriculture Organization of Nations, 2022. the United
Report highlights the importance of secure digitalization to ensure the resilience and sustainability of global food chains, especially in vulnerable areas.

MIORANDI, D.; SICARI, S.; DE PELLEGRINI, F.; CHLAMTAC, I. Internet of things: vision, applications and research challenges. *Ad Hoc Networks,* vol. 10, no. 7, p. 1497-1516, 2012.
Comprehensive review of the Internet of Things, with emphasis on the interoperability and security of distributed systems, essential for digitalized logistics environments.

MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION – MCTI. *Safer Brazil Program* Government program that *Digital.* Brasilia, DF: Government Federal, 2023.
aims to promote digital security and technological training, with a focus on critical infrastructure, including food logistics chains.

SMITH, R.; RUPP, S. Collaborative governance in cybersecurity: balancing security, privacy, and innovation. *Journal of Cyber Policy,* vp 199-217, 2020. 5, n. 2,
Article that explores collaborative governance models for digital security, highlighting the importance of the participation of multiple actors for the effectiveness of public policies.

SULTAN, N. Cloud computing: a democratizing force for global healthcare. *International Journal of* 2019. *Information Management,* v. 45, p. 134-145,
Study on the benefits of cloud computing for security, scalability and data integration in critical sectors, with direct implications for food logistics.

WTO. *E-commerce and cybersecurity: global trade perspectives.* Geneva: World Trade Organization, 2021.

Report discussing the inclusion of cybersecurity in international trade negotiations, emphasizing its relevance for global food supply chains.

ZHENG, Z.; Xie, S.; DAI, H.; CHEN, X.; WANG, H. Blockchain challenges and opportunities: 2020. the survey. *Computers & Security,* v. 107, p. 102236,

Detailed analysis of the benefits and limitations of blockchain, highlighting its role in ensuring data integrity and security in distributed supply chains.