Proposal of an information security policy aimed at protecting sensitive data in a health clinic.

Abstract
This article addresses information security and data protection in the health sector, focusing on the elaboration of a policy aligned with ISO/IEC 27002 standards and the General Data Protection Law (LGPD). The research was conducted based on qualitative and quantitative methods, using data from sources such as the CERT.br and the MITRE CVE database. The results show the vulnerability of hospital systems to cyber attacks, with emphasis on phishing attempts, malware and ransomware, in addition to the identification of critical flaws in electronic medical record systems and IoT devices. The analysis points to the urgent need to implement robust security policies, combined with auditing processes, technological updating and training of professionals. It is concluded that the protection of sensitive patient data should be treated as a strategic priority, and not just a technical one, within health institutions.

Keywords: *Information security; Data protection; Digital health; ISO/IEC 27002; LGPD; Hospital cybersecurity; Electronic medical records; Vulnerabilities (CVEs).*

Date of Submission: 07-06-2025 Date of Acceptance: 18-06-2025

I. Introduction

Data protection consists of a set of security practices and strategies to ensure the privacy of an organization's sensitive data against breaches and unauthorized access, involving the use of privacy policies that respond to compliance regulations and hinder damage to the organization's reputation and leakage of its customers' information. In the current scenario, RÊGO (2013) highlights that there is a general consensus in companies that data is their most important asset. Following this analysis, an information security policy, as stated by STALLINGS (2018), plays a crucial role in protecting data as organizational assets, establishing guidelines to prevent, detect, and respond to security incidents.

The security policy is a set of regulations necessary for an organization to have an effective information security and data protection process. According to FONTES (2015), the organizational process of information security needs to guarantee its information as follows: Confidentiality (Where it should be accessed only by the previously authorized user who needs it to carry out their professional activities related to the organization), Integrity (The guarantee that there has been no tampering with the information and that it is kept in its original state without being corrupted over time), Availability (Must be accessible to authorized access at any time required), Authenticity (Consists of ensuring the identification of the source of the information through authentication), Auditability (Ensuring that the information is audited) and Legality (Be in accordance with current legislation, corporate rules and other regulations and regulations). In Brazil, the healthcare industry has faced increasing challenges related to data protection. In 2023 there was a significant growth in incidents involving hospitals, clinics and other institutions in the area, compared to the previous year.

The adoption of technology has ensured advances in several sectors, including healthcare. Consequently, there is a need to integrate different resources in order to improve the efficiency and quality of services. Taking into account issues of improvement, in the midst of so many demands, there is a deficit in the effort aimed at creating direct guidelines. In the absence of relevance, business risks are translated into information technology risks.

This proposal was prepared with the aim of enabling information security, applying specific rules aimed at an institution in the health sector with adherence to risk management and incident response. The main purpose of the proposal is to ensure the availability, integrity, confidentiality and authenticity according to the NBR ISO/IEC 27002 standard of interconnected systems within the conformities of operational processes, considering the obligations and responsibilities in relation to security, which must be balanced in depth. In addition, in accordance with the NBR ISO/IEC 27006:2007 standard, the document declares periodic compliance checks, highlighting another important process that considers support from external entities.

DOI: 10.9790/0661-2703040812

II. Theoretical Reference

The concepts of information security and data protection must be essentially scored at the organizational level, as stated by Whitman and Mattord (2018), information security is built on a tripod of pillars (Confidentiality, integrity and validability) that guide the protection of data against internal and external threats.

2.1 Information security

According to Parker (1998) proposes a broad and holistic view, involving not only technology, but also people, processes and policies for the concept of information security, where the author goes beyond the traditional pillars of confidentiality, integrity and availability, introducing the *Parkerian Hexad*, which expands the understanding of information security to six dimensions: confidentiality, integrity, availability, possession, authenticity, and usefulness. Parker's approach reinforces the idea that the protection of informational assets is not limited to technical controls, but also encompasses human, organizational, and legal aspects. This perspective elevates information security from purely technical concepts, reinforced and argued by Anderson (2001). According to the author, organizations need to balance costs, benefits and risks when implementing protective measures, with the way they deal with the limitations and failures inherent to human behavior.

2.2 Data protection from the perspective of the General Data Protection Law (LGPD)

In Brazil, the General Data Protection Law No. 13,709, sanctioned on August 14, 2018, with the objective of regulating rules for the protection of personal data, states that non-compliance results in 2% of the company's gross revenue. (General Data Protection Law, 2018). The LGPD represents a milestone in privacy regulation in Brazil, aligning with international standards such as the European Union's General Data Protection Regulation (GDPR). Doneda (2019) points out that the law not only imposes obligations on organizations, but also strengthens the autonomy of individuals over their data, requiring transparency and clear consent for the processing of personal information. The implementation of an information policy aligned with the LGPD becomes essential to ensure legal compliance, avoid sanctions and, above all, protect patients' rights.

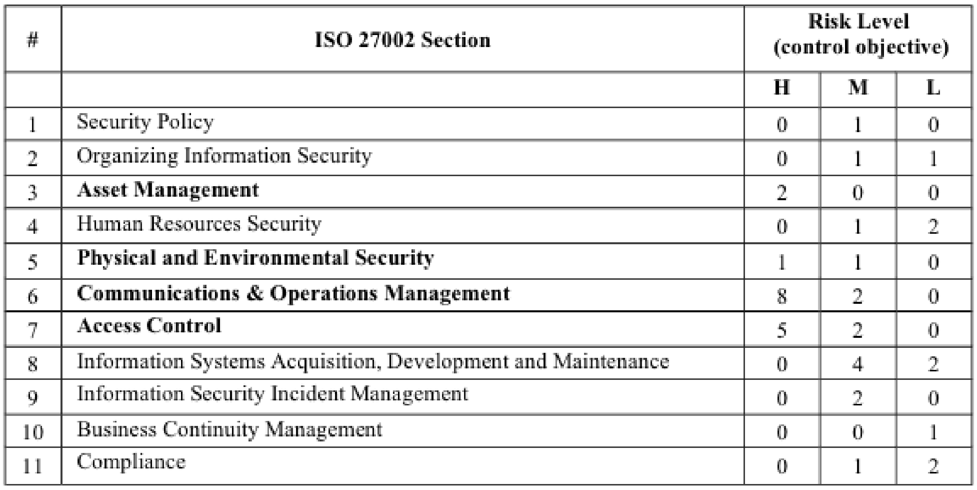
2.3 Information Technology security standards in the healthcare environment

Information security in the healthcare environment represents one of the greatest challenges of the digital age, especially due to the sensitive nature of clinical data and the stringent legal requirements that govern the sector. According to Gomes and Lapão (2008), this complexity stems from the need to protect confidential patient information — such as electronic medical records, diagnoses and medical histories — which, if improperly exposed or manipulated, can cause serious damage to individuals' privacy and institutional integrity. In addition, the authors point out that, in order to face these challenges, it is essential to adopt internationally recognized security standards and frameworks, such as ISO/IEC 27002, which provides guidelines and best practices for information security management. This standard proposes specific controls aimed at ensuring the confidentiality, integrity, and availability of information, which are essential requirements in health institutions. In the Brazilian context, compliance with legislation such as the General Data Protection Law (LGPD) further reinforces the need for a structured and robust approach to ensure the ethical and secure treatment of patient information. Therefore, implementing safety standards based on international regulations and in line with local legal requirements is essential for the trust, continuous functioning and credibility of health services today.

2.3.1 Relevance of ISO 27002 in healthcare

According to Gomes and Lapão (2008) they point out that ISO 27002, being an international standard, offers guidelines for information security management, covering 11 control areas, such as access security policies and incident management. The adoption of this standard was made at Hospital S. Sebastião (HSS) and allowed the concise visualization of the risk levels for each control area, helping the Chief Information Officer (CIO) to have an overview and at a glance of the risk classification and the prioritization of corrective actions, especially in datacenter infrastructure. As shown in table 1.

Table 1: HSS ISO 27002 Risk Level



#	ISO 27002 Section	Risk Level (control objective)		
		H	M	L
1	Security Policy	0	1	0
2	Organizing Information Security	0	1	1
3	**Asset Management**	2	0	0
4	Human Resources Security	0	1	2
5	**Physical and Environmental Security**	1	1	0
6	**Communications & Operations Management**	8	2	0
7	**Access Control**	5	2	0
8	Information Systems Acquisition, Development and Maintenance	0	4	2
9	Information Security Incident Management	0	2	0
10	Business Continuity Management	0	0	1
11	Compliance	0	1	2

Fonte: Adoption of IT Security, 2024

III. Methodology

The purpose of this research was to carry out a study relating qualitative and quantitative approaches with the objective of understanding the needs of an information security policy for data protection in the health sector. First, the study used the qualitative method in the meantime, seeking to interpret the technological context of a fictitious company in the health sector, as well as to perform an analysis of data on threats in institutions in the field, making it possible to inductively map risks and incidents. As a consequence of the understanding of descriptive analyses, the result of the information acquired ratified the importance of the development of this policy.

3.1 Context of the research

As a starting point in this methodology, it is necessary to contextualize the company addressed in this study, where it is a fictitious company in which it will be created to simulate real data protection challenges in the hospital environment, based on statistics from institutions in the same field. The institution has the following characteristics.

- Size: Medium complexity (60 employees, average of 140 patients/day);
- Critical infrastructure: Uses the virtualization of documents such as electronic medical records, radiological and oncological information systems and the use of IoT technologies.

Guidelines involving important topics related to information security policy were analyzed, which integrate technical and organizational security controls, aligned with critical requirements for the health sector. Considering the assumption of the inductive method, from open collection sources such as the Center for the Study, Response and Treatment of Security Incidents of Brazil (CERT.br), Through the statistics menu in the search parameter, through the word "health" analyzing the graph, it was possible to observe a growing interest in insurance and health information determined from January to March 2025. Data specified through the phishing attack vector, launched to obtain personal and financial data. As it is the development of an information policy, it is possible to consider data related to communication and file-sharing tools such as the widely used corporate webmail, reaching 230 attempts from the beginning of 2025 to March of the same year.

3.2 Mapping Common Exposures

Through a survey with the objective of understanding in depth the frequency of disclosure of the so-called Common Vulnerabilities and Exposures, which are unique identifiers managed by MITRE to classify vulnerabilities according to the critical level of impact. The qualitative analysis of CVEs revealed that information security in health systems does not depend only on technology, but also on the internal collaboration of employees and users of the systems. This process served to organize systems commonly used in the infrastructure. In this way, the development of a security policy has become more specific.

IV. Results

This chapter presents the results obtained from the qualitative and quantitative analysis regarding information security in hospital environments. Data were collected from national statistics (such as CERT.br), case studies and simulations, with the aim of assessing the maturity of the information security policy and the main vulnerabilities in the health sector. The results were organized on two main fronts: analysis of cyberattack attempts and the mapping of the most common vulnerabilities (CVEs) identified.

4.1 Cyber Attack Attempts on Hospital Systems (2025)

To understand the reality of the hospital environment in the face of the growing cyber threat, a simulation was carried out based on data from the CERT.br between January and March 2025. The survey analyzed phishing attempts, malware, ransomware, and external intrusions into health systems, with a special focus on institutions that use electronic medical records and IoT-based solutions. As shown in Table 1.

Table 1. Cyberattack Attempts by Type

Type of Attack	Recorded occurrences	Percentage (%)
Phishing	230	46%
Malware	110	22%
Ransomware	95	19%
External invasions	65	13%
Total	**500**	**100%**

Source: CERT.br (2025)

Phishing accounted for the majority of attack attempts (46%), showing that social engineering continues to be the most exploited vector for compromising data in hospital environments. This reveals flaws in the processes of awareness and training of internal users. The significant presence of malware (22%) and ransomware (19%) also indicates the vulnerability of systems, especially those that do not have segmented access control and updated policies. This reality reinforces the urgency of robust safety policies and continued training for all health professionals.

4.2 Vulnerability Mapping (CVEs) in Health Systems

In order to identify critical flaws in the systems commonly used by healthcare institutions, an analysis of the most recurrent Common Vulnerabilities and Exposures (CVEs) between 2023 and 2025 was carried out in electronic medical record software, PACS (medical imaging systems), and IoT devices.

Table 2. Major Vulnerabilities (CVEs) in Healthcare Systems

CVE Code	Failure Type	Affected System	Gravity (CVSS)
CVE-2024-10234	Remote Code Execution	Electronic Medical Record (EHR)	9.8 (Critical Review)
CVE-2023-55421	Authentication failure	PACS (Imaging System)	8.6 (High)
CVE-2025-11011	API vulnerability	Cardiac IoT Device	7.9 (High)
CVE-2023-88945	Exposure of unencrypted data	Administrative System	6.2 (Moderate)
CVE-2024-45007	Command injection	Patient Portal	9.2 (Critical Review)

Fonte: Adapted from MITRE CVE Database, 2023–2025.

The most critical vulnerabilities (with a CVSS score above 9.0) are concentrated in systems directly linked to the patient, such as electronic medical records and access portals. The existence of remote execution and command injection failures highlights severe risks to the integrity and confidentiality of data. The lack of proper encryption and the fragility of authentication suggest that many institutions still operate with outdated systems or without a strict security policy. These data justify the immediate adoption of standards such as ISO/IEC 27002, recurring auditing processes and vulnerability correction.

V. Final Considerations

Information security in the health sector is a field that requires constant vigilance, updating, and institutional commitment. The increasing digitalization of processes and the integration of technologies such as electronic medical records and IoT devices have brought numerous benefits to the efficiency of services, however, they have also increased the attack surface and exposure to cyber risks. The results of this study highlight a worrying scenario, especially with regard to the increase in cyberattacks with emphasis on phishing attempts — and the existence of critical vulnerabilities in sensitive systems, such as those aimed at storing and accessing clinical patient data. The analyses carried out reinforce the importance of well-defined information security policies aligned with international standards, such as the NBR ISO/IEC 27002 standard, the need for compliance with current legislation, such as the General Data Protection Law (LGPD). The survey revealed that while there is a growing awareness of the relevance of data protection, many institutions still operate without clear guidelines and effective incident prevention, monitoring, and response practices.

In this context, the urgency of adopting a holistic approach to information security is highlighted, which includes not only appropriate technologies, but also training of professionals, periodic review of internal policies, regular audits, and active participation of senior management in data governance. The development of a structured policy, as proposed in this study, is essential to ensure the confidentiality, integrity, availability and authenticity of information, ensuring the continuity of services and patient confidence. Finally, it is concluded that information security in the hospital environment cannot be treated as an isolated technical aspect, but rather as a strategic part of organizational management, being indispensable for the sustainability and credibility of health institutions in the digital age.

References

[1]. ANDERSON, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2. ed. Indianapolis: Wiley, 2001.

[2]. BRAZIL. *General Law for the Protection of Personal Data (LGPD) – Law No. 13,709, of August 14, 2018*. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed on: May 15, 2025.

[3]. DONEDA, Danilo. *From privacy to the protection of personal data: elements of the formation of the General Data Protection Law*. Journal of Contemporary Civil Law, São Paulo, n. 19, p. 13-41, Jan./Apr. 2019.

[4]. FONTES, R. A. *Information Security: a practical approach*. São Paulo: Novatec, 2015.

[5]. GOMES, C.; LAPÃO, L. V. Adoption of IT Security in Health Sector: The Portuguese Case. *International Journal of Medical Informatics*, v. 77, n. 5, p. 291–299, 2008.

[6]. ISO/IEC. *NBR ISO/IEC 27002:2022 - Information Technology — Security Techniques — Code of Practice for Information Security Controls*. Brazilian Association of Technical Standards (ABNT), 2022.

[7]. ISO/IEC. *ISO/IEC 27006:2007 - Information Technology — Requirements for bodies that provide auditing and certification of information security management systems*. ABNT, 2007.

[8]. PARKER, Donn B. *Fighting Computer Crime: A New Framework for Protecting Information*. New York: Wiley, 1998.

[9]. RÊGO, M. A. C. *Strategic Management of Information and Knowledge in Organizations*. João Pessoa: Editora Universitária UFPB, 2013.

[10]. STALLINGS, William. *Network Security: Principles and Practice*. 6. ed. São Paulo: Pearson, 2018.

[11]. WHITMAN, Michael E.; MATTORD, Herbert J. *Principles of Information Security*. 6. ed. Boston: Cengage Learning, 2018.