International Journal of Engineering Research and Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 21, Issue 6 (June 2025), PP 62-68

Cybersecurity Guide for Healthcare Telemanagement System: Case Study

Aldo Bernardo Barbosa[1], Virgílio Gustavo da Silva[1], Vagner Rogério dos Santos[1]

[1]*Department of Ophthalmology and Visual Sciences. Universidade Federal de São Paulo, São Paulo, SP, Brazil*
Corresponding Author: Aldo Bernardo Barbosa - aldo@aztlan.es

ABSTRACT
Internet of Things (IoT) technologies are increasing significantly every day. In healthcare, this is no different; with its increase, more sensors are being connected to communication networks, making data security a major concern. This case study presents a real-world application of the IoT Cybersecurity Guide for the Health Sector in an air conditioning system at the Research Building II - Prof. Dr. Nestor Schor (EPII), Campus São Paulo of the Federal University of São Paulo (Unifesp), to mitigate possible data security weaknesses. The results were satisfactory and made it possible to identify and implement mitigation actions in the data communication system.

Keywords: *Internet of Things; Computer Security; Telemedicine; Digital Health.*

Date of Submission: 06-06-2025 Date of acceptance: 16-06-2025

I. INTRODUCTION

The growing range of new technologies incorporated into the professional activities of the health sector as a whole must be treated with due attention and seriousness in terms of risk management, especially during patient care services provided by the institutions responsible [1,2].

With technological advances, Internet of Things (IoT) technologies appear as great allies in the telemanagement of hospital equipment [3].

IoT technologies are already being implemented and used in various institutions in the health sector, especially in areas focused on patient care. Soon, patients' entire histories will be accessible at any time and from anywhere based on information from connected devices [4]. IoT technologies are believed to revolutionize medicine and people's lives, with a proven return on investment in hospitals and laboratories [4].

With the significant increase in IoT devices transmitting data via the World Wide Web, private networks, and other forms of radio communication, data security has been a major concern because hackers can illicitly access the data. Therefore, it is important to analyze recent data security methods in the IoT [5].

Information security in healthcare is crucial to obtaining quality medical care and market recognition. Technological advances driven by digital transformation also increase threats to healthcare institutions, which must seek cybersecurity services, i.e., advanced security systems that guarantee the protection of patient data [6].

II. MITIGATION TECHNIQUES FOR CYBERSECURITY FRAGILITIES

2.1 Technique - (a) Strong Passwords

A password is confidential information; the person who created it is responsible for managing it, and only they should have access. Passwords are important to restrict access and guarantee confidentiality and authenticity; however, poorly designed passwords can compromise privacy [7].

To access systems, social networks, and e-mail, users have passwords and, due to this quantity, they start to use simpler combinations, which may contain personal data, to be remembered more easily. The human brain is incapable of inventing new random passwords and memorizing them securely [8]. Faced with this difficulty, people often look for shortcuts. So, they choose easy passwords, such as their children's names or a pattern of keystrokes. Even if they have trouble producing a more complex password, they use it everywhere because they only have to memorize one instead of dozens.

Data leaks related to passwords for accessing systems and e-mail have become very common in recent years. For example, in 2017, 1.4 billion credentials were generated. This list revealed the password profile of Brazilians, in which 60% use only numbers and 20% first names, with very low complexity [9].

Basic passwords, such as a wife's, child's name, and birthday, are easy to remember but also simple for cybercriminals to crack [10].

Most studies indicate that the ideal format for composing a reasonably secure password is at least 12 characters, including numbers, symbols, uppercase and lowercase letters. This composition is expected to take approximately three thousand years to be discovered. Figure 1 shows password discovery times versus the number and type of characters used [7, 11-13].

Number of Characters	Numbers ONLY	Lowercase letters	Upper and lowercase letters	Numbers, upper and lowercase letters	Numbers, upper and lowercase letters, symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 second	5 seconds
7	Instantly	Instantly	25 seconds	1 minute	6 minutes
8	Instantly	5 seconds	22 minutes	1 hour	8 hours
9	Instantly	2 minutes	19 hours	3 days	3 weeks
10	Instantly	58 minutes	1 month	7 months	5 years
11	2 seconds	1 day	5 years	41 years	400 years
12	25 seconds	3 weeks	300 years	2k years	34k years
13	4 minutes	1 year	16k years	100k years	2m years
14	41 minutes	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

Figure 1: Password discovery time (SPECITTC, 2022) [11]

2.2 Technique - (b) Encryption and Guaranteed Data Delivery

One of the main attacks on IoT devices is the interception of messages when they are transmitted wirelessly. One of the most common techniques to hinder this attack is encryption, which guarantees confidentiality and ensures that messages are not delivered to unauthorized entities [14].

The word cryptography derives from Greek words kryptos (hidden) and graphein (to write) meaning secret writing [15]. Cryptography is a technique that scrambles messages sent over the network, using one or more passwords, to guarantee confidentiality and ensure that external agents are unable to gain access to the content of exchanged messages; in some cases, it can guarantee the authenticity of information with a digital signature [16].

There are two main types of cryptography: symmetric and asymmetric. Symmetric cryptography, also known as private key cryptography, is so called because of the number of keys used by the sender and the recipient since the same key is used to encrypt and decrypt a message. This type of encryption is shown in Figure 2 [14, 17, 18].

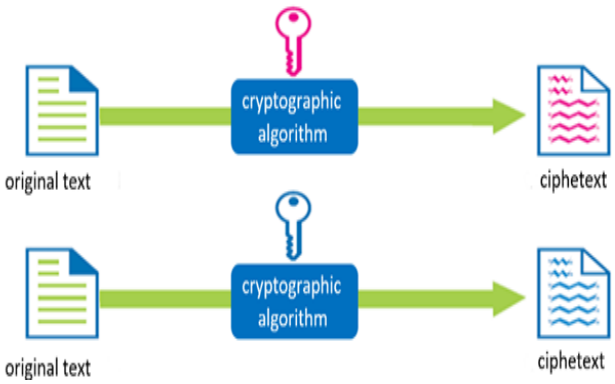

Figure 2: Symmetric cryptography (Oliveira, 2020) [17]

Asymmetric cryptography is based on algorithms that require two keys, one secret, and the other public. For example, the public key encrypts the message or verifies a digital signature, while the private key is used for the opposite operation. This type is shown in Figure 3 [14, 17, 18].

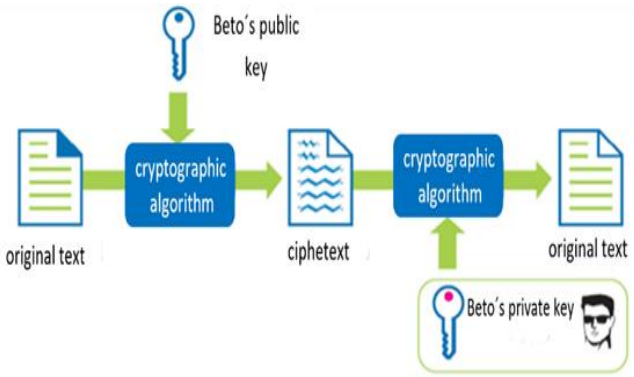

Figure 3: Asymmetric cryptography (Oliveira, 2020) [17]

When cryptography requires authentication, the keys are applied opposite to confidentiality. A document's author uses the private key to encrypt it in order to guarantee authorship or identification in a transaction. This result is only achieved because exclusively its owner, as shown in Figure 4, knows the private key [17, 18].

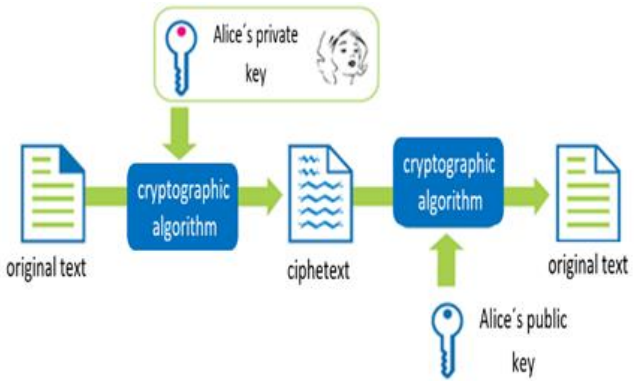

Figure 4: Cryptography with authentication (Oliveira, 2020) [17]

Still, in wireless data transmission, one of the major data security problems that affects integrity and availability is data loss, whether due to interception by cybercriminals, lack of power, or unstable communication. In other words, there is no point in the message being encrypted if there is no guarantee that it will be delivered to the client. To this end, the Message Queuing Telemetry Transport (MQTT) protocol uses three levels of quality of service (QoS) [18, 19].

- QoS 0 (at most once): This is the fastest data transfer mode; the device sends the data without more worries. However, information delivery is not guaranteed in this case.
- QoS 1 (at least once): The device sends the data and waits for a confirmation from the server; if the server does not send it, it forwards again until it receives the confirmation. In this case, delivery is guaranteed, but the server may receive duplicate data.
- QoS 2 (exactly once): The device sends the data and waits for a confirmation from the server. In this case, it only sends once; there is mutual confirmation, guaranteeing delivery without repetition, which makes this mode slower.

2.3 Technique - (c) Cybersecurity Best Practices

There is great concern about cyber threats, which take advantage of system vulnerabilities to break into networks and steal user data. However, not only can virtual flaws cause problems for the institution, but human errors can also happen and compromise information, and this is what social engineering tries to cause [20].

Most of the time, the attackers are internal employees, customers, or disguised suppliers with access to useful information in various ways and can provide information to cybercriminals. For this reason, a list of 11 good practices was created that can help protect against social engineering attacks, based on the Guide to Protecting Sensitive Knowledge, drawn up by the Brazilian Intelligence Agency [21-23]:

a) Avoid easily accessible Universal Serial Bus (USB) ports on the device.
b) Do not connect unknown USB sticks, or those given by suppliers or clients, before formatting them.
c) Conduct training focused on clarifying social engineering attacks.

d) Do not provide technical information about the device to family, friends, or teachers.
e) Develop a hiring strategy with the Human Resources Department, avoiding hiring employees linked to competing companies.
f) Control the firmware version centrally on one computer, preferably not connected to the internet.
g) Control the employees who record the firmware; only trusted staff are allowed.
h) Control employee access to the firmware-recording environment.
i) Avoid discussing technical details at celebrations, get-togethers, and technical fairs.
j) Do not buy gifts from suppliers or clients intended to connect to computers.
k) Implement rules for disposing of information stored on any medium (paper, magnetic media).

Thus, if IoT devices are not properly designed, specified, and installed, they can be affected or hacked in cyberattacks. Therefore, this study aims to demonstrate the impact of mitigation and errors in using IoT in healthcare, following the IoT Cybersecurity Guide for the Health Sector (GCIS).

III. METHODS

This work took place from January to December 2021, during the installation of the IoT device for telemanagement of the air conditioning system of the Research Building II – Prof. Dr. Nestor Schor (EPII), at Pedro de Toledo Street, 669 – Vila Clementino, São Paulo – SP, ZIP code 04039-032.

To assess the effectiveness of the GCIS, a pre- and post-application analysis was conducted on the data transmission history sent to the EPII air conditioning manager between June and November 2021. The AL2 Tecnologia platform (website: www.al2.com.br) was used to access this data.

To identify the vulnerabilities in EPII's IoT system, the Cybersecurity Checklist was used, where the answers to the data security questions are recorded, the information from which will be used to implement corrective actions, enabling auditors to assess whether the solutions are compliant. The "Fragilities mitigation techniques" field can help clarify the non-compliance described in the Cybersecurity Corrective Action Form and assist in a possible solution.

Figure 5 shows the flowchart of the entire GCIS application process.

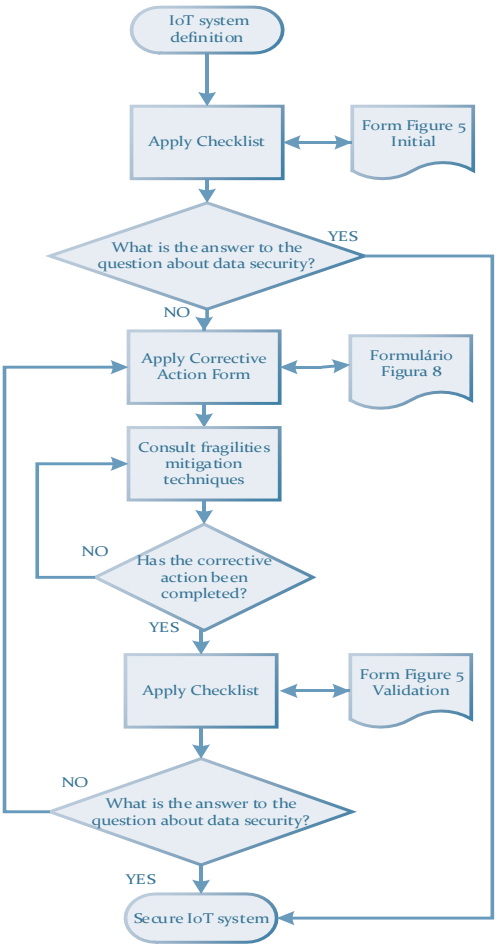

Figure 5: Flowchart of the entire GCIS Application Process

To apply the GCIS, we used the Cybersecurity Checklist in Figure 6 and the Cybersecurity Corrective Action Form in Figure 7.

UNIFESP	Cybersecurity Checklist			
Company:			Checklist:	
Responsible:			Initial	
Address:			Validation	
Application area:			Date:	
Fragilities mitigation techniques	Item	Data security questions	Status	Notes
			Yes / No	
A	1	Are passwords for accessing the device composed of at least 12 characters, including numbers, symbols, uppercase and lowercase letters?		
B	2	Is the communication between the device and the server encrypted?		
	3	Is the communication between the device and the server authenticated?		
	4	Does the device and server communication have a QoS level?		
	5	Does the device receive constant firmware updates?		
C	6	Is the device protected from physical attacks, with no open USB ports and easy access to the microprocessor?		
	7	Is the physical recording environment for the microprocessor firmware controlled?		
	8	Is the computing environment for recording the microprocessor firmware access controlled?		
	9	Is the computer or firmware recorder disconnected from the internet?		
	10	Do employees working with the device receive training on social engineering attacks?		
	11	Are the electronic components used to manufacture the device of legitimate origin?		
Checklist auditor		Checklist approval		
Creation: Aldo Bernardo Barbosa	Approval: Aldo Bernardo Barbosa	Review 1	Date: 07/15/2022	

Figure 6: Cybersecurity checklist

The Cybersecurity Corrective Action Form assessed non-conformities in the EPII's air conditioning system. It guides the indication and recording of occurrences, identifies solutions, indicates those responsible, and controls deadlines (Figure 7).

UNIFESP	Cybersecurity Corrective Action Form			
Responsible:		Application area:		
Company:		Date:		
Item	Non-compliance (vulnerabilities)	Data security corrective action	Conclusion date	Responsible
1				
2				
3				
4				
5				
6				
7				
Responsible		Approval		
Creation: Aldo Bernardo Barbosa	Approval: Aldo Bernardo Barbosa	Review 1	Date: 07/15/2022	

Figure 7: Cybersecurity corrective action form

IV. RESULTS

Graph 1 (Figure 8) shows the historical data received by the hospital manager between June and September 2021, before the GCIS was used.

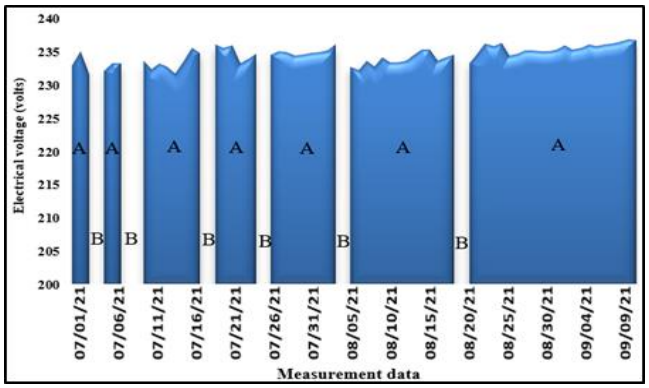

Figure 8: Data Received before the Checklist Application

Graph 2 (Figure 9) shows the historical data received by the hospital manager between September and December 2021, after the corrective actions implemented using GCIS. In Graph 2, no gaps are highlighted with the letter B, only with the letter A, i.e., no information was lost.

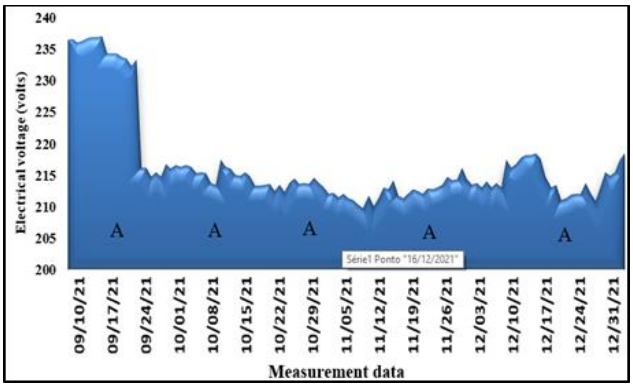

Figure 9: Data Received after the Checklist Application

After the actions were implemented, the monitoring graphic kept the data transmission stable.

V. DISCUSSION

The growing use of IoT devices in the healthcare sector highlights the need to develop solutions that strengthen data security. Issues such as latency, error rate, and instability, which play a key role in the reliability of communications in IoT environments [24]. These factors can directly influence the timely and accurate delivery of data, which is essential for critical applications such as healthcare.

There is a growing concern about data security in healthcare, especially in areas focused on patient care, arising from the application of IoT technologies in institutions. This point has been well addressed at another study [25] that illustrate the main cyberattacks faced by systems and propose a list of good security practices. Those human errors can happen and compromise information [20]. Information security in healthcare has emerged as a crucial factor in guaranteeing the quality of medical care, and initiatives to mitigate risks and ensure data protection, integrity, and privacy are mandatory.

The GCIS developed and presented in this study proved to be a tool of great assistance to specialized professionals, corroborating the data presented [26]. The GCIS proved easy to assimilate, with simple guidelines and a quick learning curve, a requirement confirmed in the case study [27].

After evaluating the data shown in Graph 1, it was found that during the three months of monitoring, the device failed to send messages seven times. After applying the Guide, no additional data was lost, as shown in the three-month simulation in Graph 2.

This case study showed that the GCIS, which consists of two instruments – the Cybersecurity Checklist and the Cybersecurity Corrective Action Form – was easy to apply and quickly assimilated. It increased data security by mitigating flaws and reducing social engineering vulnerabilities.

GCIS has been incorporated into the routine product and maintenance engineering activities at AL2 Tecnologia.

VI. CONCLUSION

The GCIS proposal effectively addressed vulnerabilities, mitigated failures, and demonstrated how quality tools developed and incorporated into companies' day-to-day activities can impact safety and quality. For future studies and practical implementations, we recommend expanding the sample of IoT systems evaluated to cover a wider range of devices, infrastructures, and configurations. This will allow for a more comprehensive and robust analysis of IoT data security strategies, providing a solid basis for recommendations and best practices in protecting healthcare systems and other critical sectors.

ACKNOWLEDGEMENT

To the National Council for Scientific and Technological Development (CNPq). Fundings Projects: 303346/2023-0 and 442222/2016-5.

REFERENCES

[1]. Kuwabara, C. C. T., Evora, Y. D. M., & de Oliveira, M. M. B. (2010). Risk management in technovigilance: construction and validation of a medical-hospital product evaluation instrument. *Revista Latino-Americana de Enfermagem*, 18(5), 943–951. https://doi.org/10.1590/s0104-11692010000500015

[2]. Lorenzetti, J., Lanzoni, G. M. de M., Assuiti, L. F. C., Pires, D. E. P. de, & Ramos, F. R. S. (2014). Health management in Brazil: dialogue with public and private managers. *Texto & contexto enfermagem*, 23(2), 417–425. https://doi.org/10.1590/0104-07072014000290013

[3]. Mishra, P., Puthal, D., Tiwary, M., & Mohanty, S. P. (2019). Software defined IoT systems: properties, state of the art, and future research. *IEEE wireless communications*, 26(6), 64–71. https://doi.org/10.1109/mwc.001.1900083

[4]. Paiva, F. (2019, janeiro 16). *IoT na Saúde: o futuro já começou*. Saúde Business. https://www.saudebusiness.com/ti-e-inovao/iot-na-sade-o-futuro-j-chegou.

[5]. Selvaraj, S., & Sundaravaradhan, S. (2020). Challenges and opportunities in IoT healthcare systems: a systematic review. *SN Applied Sciences*, 2(1), 139. https://doi.org/10.1007/s42452-019-1925-y

[6]. Almeida, F & Sauer, J. (2019, abril 9). *Práticas essenciais para segurança da informação na área da saúde*. Pixeon. https://www.pixeon.com/blog/praticas-essenciais-para-seguranca-da-informacao-na-area-da-saude/.

[7]. Mitnick, K. D & Simon, W. L. (2005). *A arte de invadir*. Pearson.

[8]. Kissell, J. (2017). *Aprendendo a proteger suas senhas.* Novatec.

[9]. Almeida, F. (2018, julho 6). Infográfico: perfil da senha do brasileiro. *Blog.axur*. https://blog.axur.com/pt/infografico-perfil-da-senha-do-brasileiro/.

[10]. Santos, N. (2020, fevereiro 28). *Segurança de senhas: longa ou mais complexa?* Vaultone. https://vaultone.com/pt-br/blog/seguranca-de-senhas-longa-ou-mais-complexa/.

[11]. Specittc. (2022, agosto 22). *Quanto tempo leva para um hacker descobrir sua senha?* Specit. https://specit.com.br/tempo-para-hacker-descobrir-senha/.

[12]. Rossini, M. C. (2022, maio 18). *Quanto tempo um hacker demoraria para descobrir minhas senhas?* Super Interessante. https://super.abril.com.br/coluna/oraculo/quanto-tempo-um-hacker-demoraria-para-descobrir-minhas-senhas/.

[13]. Palmeira, C. (2021, fevereiro 6). *Quanto tempo leva para um hacker descobrir a sua senha?* Tecmundo. https://www.tecmundo.com.br/seguranca/210443-tempo-leva-hacker-descobrir-senha.htm/.

[14]. Silva, R. L. S. (2017). *Um estudo sobre ambiente IoT e seus aspectos de segurança* [Trabalho de Conclusão de Curso, Universidade Federal do Pará].

[15]. Tanenbaum, A. S., & WetheralL, D. (2011). *Redes de computadores* (D. Vieira, Trad.; 5a ed.). Pearson Prentice-Hall.

[16]. Stallings, W., Bressan, G., & Barbosa, A. (2008). *Criptografia e segurança de redes*. Pearson Educacion.

[17]. Oliveira, L. [2020, maio 20]. Criptografia simétrica e assimétrica: saiba a diferença. *Itecnologia.* https://ltecnologia.com.br/blog/criptografia-simetrica-e-assimetrica-saiba-a-diferenca/.

[18]. Andrade, E. R, Lunardi, R. C., Ramos, N. U. (2021). Conceitos básicos de criptografia. In E. M. F. Amaral, D. Kreutz, E. R. Andrade, R. Lunardi (Orgs.). *UniHacker: Fundamentos de segurança I* (pp. 91-111). EDIURCAMP.

[19]. Kegenbekov, Z., & Saparova, A. (2022). Using the MQTT protocol to transmit vehicle telemetry data. *Transportation Research Procedia*, *61*, 410–417. https://doi.org/10.1016/j.trpro.2022.01.067

[20]. Branco, C. D. (2021, setembro 15). *O que é engenharia social? Veja como evitar problemas de segurança*. Canaltech. https://canaltech.com.br/seguranca/o-que-e-engenharia-social-195773/.

[21]. Descompliq. (2022, setembro 28). Saiba como se proteger da engenharia social! *Descompliq*. https://blog.liqi.com.br/engenharia-social/.

[22]. Marcondes, S. J. (2017, fevereiro 6). Engenharia social: o que é? Conceitos, técnicas e como se proteger. *Blog Gestão de Segurança Privada*. https://gestaodesegurancaprivada.com.br/engenharia-social-o-que-e-conceitos/.

[23]. Agência Brasileira de Inteligência. (2021). *Engenharia social: guia para proteção de conhecimentos censíveis*. ABIN.

[24]. Saavedra, E., Mascaraque, L., Calderon, G., Del Campo, G., & Santamaria, A. (2022). A Universal Testbed for IoT wireless technologies: abstracting latency, error rate and stability from the IoT protocol and hardware platform. *Sensors (Basel, Switzerland)*, *22*(11), 4159. https://doi.org/10.3390/s22114159

[25]. Bortoli, K. U., & Baltazar, N. C. (2023). *Segurança em IoT* [Trabalho de Conclusão de Curso, Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"].

[26]. Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the internet of medical things. *Health Policy and Technology*, *10*(3), p. 100549.

[27]. Silveira, E. F. da, & Werner, L. (2011). Proposta de método de priorização de processos a serem monitorados no controle estatístico de processo: uma aplicação em trocador de calor. *Revista Produção Online*, *11*(1), 116–135. https://doi.org/10.14488/1676-1901.v11i1.517