The ISO 27000 Family and its Applicability in LGPD Adaptation Projects for Small and Medium- Sized Enterprises

How the ISO 27000 family standards can help with the challenge of complying with the General Data Protection law for small and medium-sized businesses

André de Freitas Fernandes, Fabiano Camilo Santiago de Brito, Fátima Fernandes Periard, Grazielle A. Viana Matias, Mariana Sbaite Gonçalves, Reinaldo Gomes Baldoino Filho

IESB University Center

andre.fernandes@serpro.gov.br, fabianocamilos@gmail.com, fatima.periard@crmbrasil.com.br, grazielle@m2cloud.com.br, marianasbaite@gmail.com, reinaldo.baldoino@iesb.edu.br

Abstract - This article describes the relationship between the Brazilian Data Protection Law (LGPD) - nº 13.709 / 2018 - with the information security through ISO Standards. The theme is extremely relevant, as it shows the difficulty for small and medium-sized companies to comply with current and applicable legislation on privacy and protection of personal data, as well as the need for security and investment, to protect the privacy of the holders of personal data and not suffer future damage, whether property or reputation. Some companies have already received fines for the irregular processing of personal data. Being adequate is the immediate answer for the evolution of their businesses and the protection of personal data. This article demonstrates the importance of complying with the LGPD and using security frameworks and investment in information security, improving data management and governance of associations.

Keywords- LGPD; Adequacy; ISO; Security; Technology; SMEs.

I. INTRODUCTION

We live in a challenging environment when it comes to protecting personal data. On the one hand, personal data protection and privacy laws take shape, bringing changes in society. On the other hand, there is an epidemic of data exposures and breaches affecting businesses of all sizes and market segments globally. Companies are at the heart of this situation, which depends on technology and data to maintain their business continuity.

A survey conducted by Microsoft between September and October 2020 [1] indicated that for small and medium-sized companies, technology was the best answer to get around the crisis. The study shows that, during the pandemic, 42% of SMEs accelerated the adoption of new technologies, mainly medium-sized companies and, for 83% of respondents, these technologies lead the way towards economic recovery.

While these businesses need to use technology for their reinvention, they must comply with a series of regulations related to their performance, and now, they need to adjust to comply with current and applicable privacy and data protection laws. The matter would be simple if all companies had a vision of processes and budgets defined for the security and compliance areas. However, for most small and medium-sized Brazilian companies, the reality is quite different.

In a survival market, SMEs are focused on producing and delivering, in the famous so-called "turning the wheel." With leaner structures and tight cash, the SME entrepreneur has not defined business processes, and many do not even consider information security necessary. Their concerns are precisely on product or service.

This article aims to demonstrate that one of the ways to achieve compliance with the LGPD – General Data Protection Law is the use of the frameworks of the ISO 27000 standards as well as making room for small and medium businesses to evolve in their management, with information security as one of the pillars of this process.

Some questions that guided the article:

- *What is the need to adapt SMEs to the LGPD?*
- *What difficulties do SMEs face on a day-to-day basis?*
- *How to invest in Technology, Information Security and Compliance?*
- *Are these companies aware of the risks that non-compliance with the Law brings to the continuity of their business?*

In the following sections, we will see the purpose of the article and the questions that guided the work. In section II, we will talk about SMEs and citing examples from Brazil. In section III, we will talk about the General Data Protection Law and its impacts. In section IV, we will talk about the DPO career. In section V, we will talk about the LGPD and ABNT standards. In section VI, we will talk about ISO 27000 standards. In section VII, we explain privacy management. In Section IV, we present our final remarks.

II. WHAT IS SMALL AND MEDIUM SIZE COMPANIES

SME is an acronym for Small and Medium Enterprise. It is an acronym often used to classify the size of a company as a function of the number of workers employed and the annual income earned. This type of company occupies an important place in the economy of countries through the generation of jobs.

 ISBN: 978-1-61208-894-5

The classifications according to the number of workers employed are as follows:

Industry:

- Microenterprise - up to 19 employees
- Small Business - from 20 to 99 employees
- Medium Company - from 100 to 499 employees
- Large Company - 500 or more employees

Trade and Services:

- Microenterprise - up to 9 employees
- Small Business - 10 to 49 employees
- Medium Company - 50 to 99 employees
- Large Company - more than 100 employees

According to Sebrae (Brazilian entrepreneur support service) [2], they can also be divided into four segments by revenue range, except for small rural producers. Briefly, small businesses are divided as follows:

- Individual Microentrepreneur – Annual turnover up to R$ 81 thousand.
- Microenterprise – Annual turnover up to R$360 thousand.
- Small Business - Annual turnover between R$360 thousand and R$4.8 million.
- Small Farmer - Property with up to 4 fiscal modules or annual sales of up to R$ 4.8million

Segmentation by billing follows the criteria of Complementary Law 123/2006, also known as the General Law for Micro and Small Companies.

According to Data Sebrae [2], there are approximately 19 million companies in Brazil, and of this total, about 7.5 million are into the SME categories. In 2020, these companies corresponded to around 29% of GDP. Regarding the volume of jobs, the same Data Sebrae indicates that in 2018 SMEs generated about 17.79 million jobs with a salary volume of around R$ 34.27 billion. Data from the PNAD (National survey by the sample of households) carried out by the IBGE show that between 2003 and 2013, there was a 10% growth in the number of business owners in the country, from 21.4 million to 23.5 million people. In this same period, the number of highly computerized business owners almost quadrupled, from 3.9 million to 14.3 million people (an increase of 10.4 million individuals).

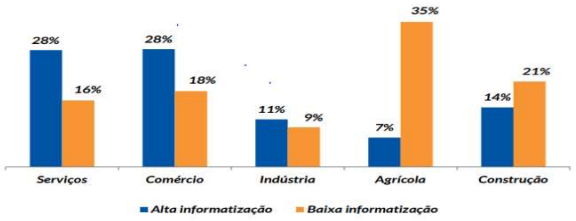

Figure 1. Distribution by sector of activity [3]

This data leads us to a potential market of millions of SMEs seeking to adapt to new data protection legislation and needing support for this task, mainly in the Commerce and Services sectors.

According to consulting firm Price Waterhouse Coopers: "The power of SMEs is evident in their 30% share in the Gross Domestic Product (GDP) of R$4.4 trillion in Brazil. The segment employs more people than any other: 10.1 million employees in small companies and 5.5 million in medium ones"

According to Disterer [20], a 2008 survey of ISO27001 - certificated companies found that 50 percent of the certificated organizations which responded had fewer than 200 employees and were therefore in the SME category. Perhaps more surprisingly, around half of these had fewer than 50 employees. The framework has used the ISO27002 code of practice to define the elements considered within the ISMS. Each component is then developed through a maturity model life cycle to establish an ISO 27001-compliant ISMS process.

III. The General Personal data Protection Law and Small and midsize Enterprises

The Brazilian Law No. 13.709/2018 – General Law for the Protection of Personal Data (LGPD) [4] provides for companies' processing of personal data throughout Brazil, without mentioning differences in the dealings of the small, medium large companies or self-employed professionals. It is clear to establish equal guidelines for all figures.

The administrative sanctions provided for in the Law are effective from August 2021, and with less than two months to go before the scheduled date, few companies are complying.

The purpose of the Law is to organize and structure organizations about privacy, preserve the dignity of the human person and allow holders to be able to exercise their rights.

In addition to bringing principles and new rights to the holders of personal data, it needs to adopt technical and administrative measures to maintain the security and confidentiality of information. Furthermore, it requires a governance plan and the application of good practices to protect and preserve the safety of all personal data involved in business flows and processes. The problem is: it is neither easy nor cheap to adapt to the LGPD. Therefore, companies need to structure themselves to have the budget and human resources to practice everything the law requires. In the case of SMEs, it turns out to be arduous, not only for lack of investment but also for lack of information.

The General Law for the Protection of Personal Data requires internal organization, the definition of roles and responsibilities, and increased budget to invest in training and tools, among other activities that most companies do not have in Brazil. It is essential to point out that the administrative sanctions of the Law started in August 2021, and few companies are in compliance, which can lead to financial and reputational losses. According to Almeida [20], "...we consider it fundamental to think of ways to make the application of the law by small businesses viable so that they can successfully fulfill their obligations." To believe that the

 ISBN: 978-1-61208-894-5

LGPD, to be applied, must treat all companies equally, respecting their characteristics and enabling the actual applicability of its rules.

One of the most important novelties is the need for the person in charge of Data Processing, corresponding to the Data Protection Officer of the General Data Protection Regulation and about which we will discuss below.

IV. DATA PROTECTION OFFICER FIGURE ENTRY

The General Data Protection Law introduced the figure of Data Protection Officer, the person responsible for the processing of personal data, who, in a simplified way, has the function of conducting the organization's compliance process, in addition to being the point of communication between the holders of personal data, the processing agents and the regulatory body National Data Protection Authority. To perform its role well, the Data Protection Officer needs to know much more than the Law. It must understand compliance, processes, technology, people management, and being familiar with security frameworks. The Data Protection Officer must be involved in all techniques or flows involving personal data to verify gaps and the best security controls to be applied to mitigate or eliminate the risks.

The LGPD [4], in its article 46, brings to treatment agents the need to adopt technical and administrative security measures. However, the Data Protection Officer is responsible for making things happen and developing a culture of privacy within companies. And it is precisely at this point that the need to know and apply the requirements of the ISO 27000 family of standards comes into play. These standards, which address cybersecurity, bring clarity and structure to business processes that need to be revised but are not even known by small and medium companies. These businesses do not have process management and compliance budgets and cannot see value in their adoption. The standard brought by the ISO family adds both in the sense of assisting in information security, as it allows companies to improve their way of managing assets, flows, processes, and people.

The requirement of compliance with the LGPD will bring these companies greater visibility into their processes, previously in the dark, leading to new approaches for all areas and more excellent organization in terms of management, improving the trust relationship with customers and business partners.

V. LGPD, ABNT AND THE ISO STANDARDS

Chapter VII of the LGPD [4], addresses Security and Good Practices: Section I - Security and Data Secrecy; and Section II: Good Practices and Governance. In this sense, it determines the adoption of security measures and good practices to maintain confidentiality, when necessary, and for better governance; however, it does not clarify how companies can comply with these requirements. Then, the ISO 27000 family standards come into play to help businesses of all sizes to structure their compliance and governance processes, helping to adapt to the LGPD and allowing for a more comprehensive governance performance.

The Brazilian Association of Technical Standards (ABNT) [19] is the National Forum for Standardization. The Brazilian Standards, whose content is the responsibility of the Brazilian Committees (ABNT/CB), Sectoral Standardization Bodies (ABNT/ONS), and Special Study Commissions (ABNT/CEE), are prepared by Study Commissions (CE), formed by the interested parties in the subject-object of the standardization. ABNT Technical Documents and International Standards (ISO and IEC) are voluntary and do not include contractual, legal, or statutory requirements.

These ABNT Technical Documents do not replace Laws, Decrees, or Regulations, which users must comply with, taking precedence over any ABNT Technical Document. Therefore, the ISO standards and the technical documents developed by ABNT serve as a support tool for companies of different sizes to follow best practices and follow the guidelines and guidelines provided in the documentation.

VI. A TURN THROUGH THE ISO 27000 FAMILY STANDARDS

The ISO 27000 set of standards constitutes complete security and privacy framework. Compliance takes place in continuous improvement, which, in addition to promoting improvement in internal processes, brings noticeable results to the end customer. Next, we will talk about each standard.

According to Gillies [21], when companies use the ISO 27000 standard, they can significantly improve information security management.

A. ISO 27001 – Information Security and Management System

This standard covers the concept of information security in an integral way, dealing with various topics, such as protection of the physical environment, telecommunications, application security, human resources, business continuity, licensing, and other items that may vary according to the model business.

As a general principle, it addresses the adoption of a set of requirements, processes, and controls, which aim to correctly identify and manage the Information Security risks present in organizations, helping to adopt an adequate model of establishment, implementation, operation, monitoring, review, and management of an Information Security Management System.

The Information Security Management System (ISMS) is, following the principles of the ISO 27001 standard, a holistic model of approach to Security and independent of technological brands and manufacturers, as it is intended to establish processes and procedures that can be materialized

 ISBN: 978-1-61208-894-5

in each organization differently, according to the specificity of each technological and organizational environment [5].

B. ISO 27002 – Information Security - Requirements

ISO 27002 establishes a code of best practices to support implementing the Information Security Management System (ISMS) in organizations, complementing the previous standard. Its main objective is to establish guidelines and general principles to initiate, implement, maintain, and improve information security management in an organization, including selection, implementation, and management of controls, considering the identified risks. The items below make up the standard's approach [5] [6]:

- Information Security Policy
- Information Security Organization
- Asset Management
- Security in human resources
- Physical and environmental security
- Security of operations and communications
- Access control
- Acquisition, development, and maintenance of systems
- Information security incident management
- Business continuity management
- Conformity

The objective of NBR ISO/IEC 27002:2013 is stated as follows [6], “Information security is achieved by implementing an adequate set of controls, including policies, processes, procedures, organizational structure and software and hardware functions. These controls need to be established, implemented, monitored, critically analyzed and improved as necessary to ensure that the organization's business and security objectives are met."

C. ISO 27003 – Guidelines to Implementation the Security Management Information System

While ISO 27001 provides the requirements for implementing the ISMS, ISO 27003 provides guidance on the process and recommendations, possibilities, and possible permissions. According to the standard, there are 5 phases of planning an ISMS project [5] [7]:

1. Obtain approval from senior management (top management) to initiate the ISMS project.
2. Define the scope, limits, and policy of the ISMS.
3. Conduct analysis of information security requirements.
4. Conduct risk analysis/assessment and plan risk treatment.
5. Define the ISMS.

D. ISO27004– Information Security Management

ISO 27004 guides how to assess the performance of ISO 27001, providing a set of standards to guide the development, operation, and measurement of processes to evaluate and report the results of a set of information security metrics [5] [8].

The standard demonstrates how to build an information security measurement program, how to select what to measure and how to operate the necessary measurement processes, it also includes comprehensive examples of different types of measures and how can assess the effectiveness of those measures.

Among the greatest benefits of adopting the law, we highlight:

- Greater responsibility
- Improved performance of information security and ISMS processes
- Evidence of compliance with the requirements of ISO / IEC 27001, as well as applicable laws, rules, and regulations.

E. ISO 27005–Iformation Security Risk Management

To provide guidelines for the management of information security (IS) risks, ISO 27005 supports the concepts specified in ISO 27001, in addition to assisting in the implementation and certification of such management systems[5] [9].

According to the standard, the IS risk management process comprises the following activities:

- Identify and assess risks.
- Decide what to do about risks (how to deal with them)
- Monitor risks, risk treatments etc., identify and respond appropriately to significant changes, problems/concerns, or opportunities for improvement.
- Keeping stakeholders (mainly the organization's management) informed throughout the process.

F. ISO 27007–ISMS Audit Guidelines

The text of ISO 27007 discusses the management of an information security management system (ISMS) audit program, the performance of audits, and the competence of the ISMS auditors. It is an applicable standard for those who need to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit program [10].

According to the standard, they constitute a management and auditing process:

- Audit principles
- Management and audit program
- Conducting an audit
- Competence and assessment of auditors

G. ISO 27014 - Information Security Management

ABNT NBR ISO/IEC 27014 (2013) points out that Information Security Governance should aim to [11]:

- Align business objectives with the Information Security strategy.

 ISBN: 978-1-61208-894-5

- Ensure that information risks are elucidated and forwarded to those responsible.
- Add value to the business, senior management, and stakeholders.

H. ISO 27031 - ICT Preparation (Information and Communication Technology) for business continuity

The ISO 27031 standard guides the concepts and principles behind the role of ICT – Information and Communication Technology in ensuring business continuity [12].

By default, the norm:

- Suggests a structure or structure (a coherent set or set of methods and processes) for any organization - private, governmental, and non-governmental.
- Identifies and specifies all relevant aspects, including performance criteria, design, and implementation details, to improve ICT readiness as part of the organization's ISMS, helping to ensure business continuity.
- Allows an organization to measure its ICT continuity, security and therefore readiness to survive a disaster in a consistent and recognized manner.

I. ISO 27032 – Cyber Security

The ISO 27032 standard addresses basic security practices for stakeholders in cyberspace, providing [13]:

- Cybersecurity overview,
- Relationship between cybersecurity and other types of security,
- Definition of stakeholders and description of their roles in cybersecurity,
- Guidance for addressing common cybersecurity issues, and
- Framework to enable stakeholders to collaborate on solving cybersecurity issues.

J. ISO 27037 – Preservation of Digital Evidence

The content of ISO 27031 [14] makes up a relevant set of information for forensic professionals. It makes up an international standard for identifying, collecting, acquiring, and preserving digital forensic evidence at all stages of the investigation process.

The standard standardizes the specific activities in the treatment of digital evidence, ranging from identifying, collecting, acquiring, and preserving digital evidence that may have evidential value. It assists organizations in their disciplinary procedures in facilitating the exchange of digital evidence between jurisdictions.

ISO 27031 generally considers the following devices or functions that are used in various circumstances [14]:
Digital storage media used in computers, such as HD, floppy disks, CD/DVD, pen-drive, smartphones, tablets, Personal Digital Assistants (PDA), Personal Electronic Devices (PED), Memory Cards, and Mobile navigation systems (GPS).

- Embedded systems.
- Digital video and photo cameras (including CCTV).
- Desktops, Notebooks.
- Networks based on TCP/IP and other digital protocols, and
- Devices with functions like those described above.

K. ISO 27701 – Privacy Management

As mentioned at the beginning of this article, almost all organizations handle personal data, whether employees or customers. In addition, the amount and types of personal data processed is increasing, as is the number of situations in which an organization needs to cooperate with other organizations regarding the processing of personal data. The protection of privacy in the context of the processing of personal data is a societal need and a topic of dedicated legislation and/or regulation around the world.

ISO 27701 is an extension of ISO 27001 and 27002 [5] [6] [15] that specifies the requirements and provides guidance to establish, implement, maintain, and continuously improve an Information Privacy Management System (IPMS), the document specifies in detail the requirements related to the IPMS and the guidelines that must implement in companies that are responsible for the processing of personal data.

The table below presents the mapping of the extension of the term information security for application and use of this document, it is possible to see how both are similar just adding the aspect of privacy in their content.

TABLE I. SECURITY AND PRIVACY APPROACH IN ISO 27001 AND ISO 27701 STANDARDS

ABNT NBR ISO/IEC 27001	ABNT NBR ISO/IEC 27701
Information Security	Information Security and Privacy
Information Security Policies	Privacy and Information Security Policies
Information Security Management	Information Security Management and Information Privacy
Information Security Management System (ISMS)	Privacy Management System
Information Security Objectives	Information Security and Privacy Objectives
Information Security Performance	Information Security and Privacy Performance
Security Information Requirements	Security Information and Privacy Requirements
Information Security Risks	Information Security and Privacy Risks
Information Security Assessment	Security Risk Assessment of Information and Privacy
Treatment of Security Risks of Information	Treatment of Security Risks of the Information and Privacy

 ISBN: 978-1-61208-894-5

VII. Conclusion And Future Work

From risk definition to business continuity and response plan, the ISO 27001 family provides a robust framework that allows understanding and applying the concepts of security and privacy. The standards guide how to identify risks related to the processing of personal data, in addition to reinforcing the need for policies, internal and external contractual agreements, items that are unknown to most small and medium-sized companies. When guided by the requirements of this set of standards, an organization tends to develop secure processes to manage the security of the information it handles. Therefore, privacy tends to be included in the process, becoming part of the business culture.

Considering the recent arrival of the General Data Protection Law in Brazil, small and medium-sized companies should pay attention to information security and the protection of personal data collected and held in custody to comply with regulations and ensure the image and reputation of their businesses. Understanding that small businesses run the same risks as large corporations can be the starting point for a strategic vision regarding privacy and data protection. Small businesses in this regard are even more vulnerable, as the lack of investments in cyber security makes them an easy target for cybercrime.

The biggest cost is the non-investment in information security. According to a recent survey carried out by First Data Corporation, about 90% of intrusions are directed to the systems of small and medium-sized companies. The average cost of vulnerabilities was enough to increase these companies' expenses by around U$D 36,000 annually. In that same survey, identified that the biggest impact is not the financial one. Still, the reputational one and in the scope of public relations, 31% of the clients and consumers said that upon discovering that the company was the target of data leakage due to malicious attacks, they would not return to doing business with the institution.

In another article in the Brazilian magazine Gestão&Negócios PME (Management and Business SME), 128 Edition/ 2019, November, was reiterated that despite investments in security systems, having a partner with vast expertise in the field of information security and data protection to help with this transition coupled with a mapping of personal data throughout the data lifecycle is a key part of greater protection in companies.

As a practical guide on improving the maturity of information security and data protection in companies, the ISO 27000 Family Standards provides a series of tools that help implement Information Security policies, whatever the size and budget of the company. With the recent arrival of the General Data Protection Law (LGPD - Law 13.709) [4], the need for adaptation was even greater as sanctions related to the protection of personal data also need greater attention from now on, where before the arrival of the Law only corporate data had a relevant adequacy need due to trade and trade secrets.

It is also important to highlight that the Law should not be seen as a hindrance or an obstacle in front of the commercial and technological evolution of companies, as many claim to be, as well stated by Leonardo Gondim, executive director of IT2S, in Gestão&Negócios PME Magazine, 128 Ed.: "The Law does not prevent the data from being used for one purpose or another, it only requires the user to be informed of this use and authorize it. It ends up giving back to the user the control of something that has always been his, allowing him to decide whether or not to provide the data and, also, knowing exactly what it will be used for".

In conclusion, the best thing to do going forward, both for the preservation of holders' privacy and for the business, is to have a security mindset in the first place. As explored in this article, not even small and medium-sized companies can assume risk-free, especially when much of the information is in an online environment. Changing the mindset is essential to avoid future losses and maintain the trust of customers and business partners.

For future work, a study will be carried out in companies called SMEs. Still, this study will verify the applicability of the general data protection law and its impact in the information technology sector.

References

[1] Microsof News, "Como as PMEs brasileiras enfrentaram a pandemia de COVID-19" - https://news.microsoft.com/pt-br/82-das-pmes-brasileiras-pretendem-continuar-o-processo-de-adocao-de-novas-tecnologias-apos-a-pandemia-segundo-estudo/- Aug. 17, 2021.

[2] Data Sebrae, https://datasebrae.com.br/ – Aug, 29, 2021

[3] B. A. Marcos, "Os donos de negócio no Brasil: análise por faixa de renda (2003-2013)": Sebrae, 2015.

[4] Presidência da República, Lei Geral de Proteção de Dados - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm - Aug, 25, 2021

[5] International Organization for Standardization, ISO/IEC 27001: 2013, Information Technology--Security Techniques--Information Security Management Systems, 2013.

[6] International Organization for Standardization, ISO/IEC 27002:2013, Information technology-Code of practice for information security management, 2013.

[7] International Organization for Standardization, ISO/IEC 27003:2017 - Information technology — Security techniques — Information security management systems — Guidance, 2017.

[8] International Organization for Standardization, ISO/IEC 27004:2016 - Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation, 2016.

[9] International Organization for Standardization, ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management, 2018.

 ISBN: 978-1-61208-894-5

[10] International Organization for Standardization, ISO/IEC 27007:2020 - Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing, 2020.

[11] International Organization for Standardization, ISO/IEC 27014:2020 - Information security, cybersecurity and privacy protection — Governance of information security, 2020.

[12] International Organization for Standardization, ISO/IEC 27031:2011 - Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity, 2011.

[13] International Organization for Standardization, ISO/IEC 27032:2012 - Information technology — Security techniques — Guidelines for cybersecurity, 2012.

[14] International Organization for Standardization, ISO/IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence, 2012.

[15] International Organization for Standardization, ISO/IEC 27701:2019 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, 2019.

[17] Ministério da Economia, “Especificação de Requisitos de Segurança da Informação em Contratações de Tecnologia da Informação”, Secretaria de Governo Digital, 2020.

[16] PriceWaterHouseCoopers, “O poder das PMEs no Brasil”, 2013.

[17] Gestão & Negócios PME, “De olho na segurança do seu cliente”, Edição 128, 2019.

[18] D. Almeida, Mirante contábil, “Proteção de dados e o papel dos pequenos negócios”, 2021.

[19] A. A. Bertini, J. C. Martins and E. Thomaz, "Desempenho de edificações habitacionais: guia orientativo para atendimento à norma ABNT NBR 15575/2013.", 2013.

[20] D. Georg, "ISO/IEC 27000, 27001 and 27002 for information security management.", (2013).

[21] G. Alan, "Improving the quality of information security management systems with ISO27000.", 2011.

 ISBN: 978-1-61208-894-5