OLAVO RODRIGUES DE AGUIAR NETO

Gap Analysis and Information Security Management System proposal for a startup company

SÃO PAULO

2022

OLAVO RODRIGUES DE AGUIAR NETO

Gap Analysis and Information Security Management proposal for a startup

Trabalho de Formatura apresentado à Escola Politécnica da Universidade de São Paulo para obtenção do diploma de Engenheiro de Produção.

Orientador: Fernando Tobal Berssaneti

SÃO PAULO

2022

CATALOG CARD

Neto, Olavo Rodrigues de Aguiar.
Gap Analysis and Information Security Management proposal for a startup / O. R. A. Neto -- São Paulo, 2022
110 p.

Final Paper – Polytechnic School of University of São Paulo. Production Engineering Departament.

1. ISO/IEC 27001 certification 2. Compliance 3. Risk management 4. Information Security Management System I. University of São Paulo. Polytechnic School. Production Engineering Department II.t

To my grandmother, the person I admire
the most, for all the love, support and
care provided. To my parents and sister,
who provided all material and emotional
conditions to thrive and are the reason I
live. To my uncle and godfather, Sérgio
Godoy Rodrigues de Aguiar (*in
memoriam*), with whom I would want to
celebrate this moment

ACKNOWLEDGEMENTS

Firstly, I would like to thank my teacher Fernando Tobal Berssaneti, without whom this final paper would not be delivered, for giving me the required knowledge and support to finish this challenge as well as for all the kindness, patience, comprehension, and friendship throughout this process.

I thank my mother, father, and sister, for all support, dedication and sacrifices made that allowed for a privileged education as well as for all the great moments we had together and are still to have.

I thank my friend, Pedro Mauro, for all support, empathy and kindness given. Without him, this final paper would also not be delivered.

I thank all the teachers I had through my graduation for all the knowledge and experience shared.

I thank my college friends for all the good moments we had together, support provided and for making me better person, especially Lucca Almeida, Bruna Queiroz, Gabriel Monet, Victor Ennes, Renan Barros, Mateus Oioli, Marcos Hirasawa, Paula Daniela, Ana Custódio, Giulia Fujiwara, Giulia Ribeiro, Leonardo Dias, Leonardo Kenji, Lucas Portella, Gabriel Marcos, Barbara Moreira and Helena Guo.

I thank my lifelong friends Alexandre Bestwina, Edgard Rodrigues, Fernanda Pontieri, Guilherme Polho, Luana Martins, Lucas & Matheus Sckaier, Luis Afonso, Mateus Nachef, Otávio Mangini, Pedro Azambuja, Pedro Nascimento, Raquel Pontieri, Richard Petri, Vitória Arruda.

Finally, I also thank all the ones I have forgotten to include but somehow helped along these years.

RESUMO

Privacidade e segurança da informação são tópicos que vêm cada vez mais se tornando relevantes perante a sociedade, o Estado e as empresas com a maior geração, acesso e compartilhamento de dados. Este trabalho propõe implementar um Sistema de Gestão de Segurança da Informação (SGSI) em uma startup com menos de dois anos de existência cuja geração de valor envolve o manuseio e gestão de dados sensíveis. O SGSI a ser implementado possui como referência a norma NBR ISO/IEC 27001:2013. Para tal, mapearam-se os processos da empresa em questão e, em seguida, implementaram-se quatro processos referentes à etapa de Planejamento da norma. Dentre os resultados obtidos, encontram-se 25 oportunidades de melhoria mapeadas, 3 das quais já foram implementadas, a melhora na gestão de riscos da organização além do aumento da conscientização interna a respeito de segurança da informação. Além disso, planeja-se dar prosseguimento ao trabalho para conferir o atendimento a todos os requisitos da norma por parte da empresa.

Palavras-chave: Sistema de Gestão de Segurança da Informação. ISO/IEC 27001. Gerenciamento de riscos.

ABSTRACT

Privacy and information security are topics that are increasingly becoming relevant before society, the State and companies with the increased generation, access and sharing of data. This work proposes to implement an Information Security Management System (ISMS) in a startup with less than two years of existence whose value generation involves the handling and management of sensitive data. The ISMS to be implemented has as reference the NBR ISO/IEC 27001:2013 standard. To this end, the processes of the company in question were mapped, and then four processes referring to the Planning stage of the standard were implemented. Among the results obtained are 25 mapped improvement opportunities, 3 of which have already been implemented, improvement in the organization's risk management, and an increase in internal awareness about information security. In addition, it is planned to continue the work to ensure that the company meets all the requirements of the standard.

Keywords: Information Security Management System. ISO/IEC 27001. Risks management.

FIGURES LIST

TABLES LIST

ABBREVIATIONS LIST

ABNT – *Associação Brasileira de Normas Técnicas*

ISMS – Information Security Management System

ISO – International Organization for Standardization

SUMMARY

1 INTRODUCTION

Environmental, social, and corporate governance (ESG) issues have been increasingly gaining relevance across different segments of society especially among consumers, investors and, thus, companies. Although these issues have been under debate and concern regarding society since the mid-20th century at least in an isolated form, the term was formally introduced in 2005 in a report of the International Finance Corporation (IFC, 2005) and, during the 2006 United Nation’s Principles for Responsible Investment (PRI), ESG was firstly appointed as criteria for financial evaluations of companies (Forbes, 2020). As of March 2021, there were 3404 PRI investors signatories with a composed Assets Under Management (AUM) of over US$ 121 trillion compared to 63 signatories and an AUM of US$6.5 trillion for 2006 (PRI, 2021). Therefore, one can appoint the relevance this subject has for companies in the present especially those aiming for an accelerated and sustained growth like startups.

Although the three aspects of ESG have their respective relevance among the market and society, this final paper will be concerned only with the G (governance) criterion of it regarding data and information security. In this sense, governance is understood as processes and structures that provide control, accountability, and transparency for the respective stakeholders of an organization such as customers and investors. This has been an issue among companies managing sensitive information considering recent data leakages such as the one that involved the leakage of over 223 million Brazilians – including deceased ones – resulting in the bureau Operation Deepwater (*Operação Deepwater* in Portuguese) in March 2021 as well as another in December 2020 deriving from the leakage of over 243 million Brazilians – also including deceased ones – from Brazil’s Ministry of Health. One outcome of such kind of events was the pressure on legislators among different countries to provide a more robust regulation of data and information management followed by the adoption of the European General Data Protection Regulation and its Brazilian’s counterpart LGDP legislations.

Therefore, to satisfy these governance demands, some companies have been targeting the adoption or improvement of their information security management systems not only to guarantee legislation compliance but also as an assurance of transparency and commitment to its stakeholders towards the market. A common and effective way to assure this is by obtaining a certification from a globally recognized institute among which the International Organization for Standardization (ISO) is part of. The ISO/IEC 27001: 2013 is one set of standards that specifies the requirements for a data and information security management system and it is part of the broader 27000 series.

1.1 THE COMPANY

Salars Softwares e Soluções Ltd. is a B2B startup company that operates in the city of São Paulo, Brazil and provides solutions aiming at improving the efficiency of organizations regarding remuneration as well as Human Recourses (HR) processes. Officially founded in September 2021, its existence dates to the beginning of the same year when one of the two co-founders started studying HR issues among companies in Brazil and other countries such as difficulties in determining the appropriate salary for their workforce to prevent an overpaying scenario especially within startups. This research ultimately led to his final paper to graduate as a Production Engineer of the Polytechnic School of the University of São Paulo. As of the present day, having three external investors, Salars Softwares e Soluções Ltd.'s vision is to become the tool that attends to each remuneration needs for a company.

Currently, Salars Softwares e Soluções Ltd.'s portfolio consists of two solutions sold together. In the first one, the client can consult for its respective industry how much the market is paying on average for each position from a database of Salars Softwares e Soluções Ltd.'s, thus assuring a more assertive decision regarding hiring and preventing an overpriced workforce. As a counterpart, the client provides access to its payroll. In this sense, the reliability of the solution is based on the fact the output salary is calculated directly from the original source.

The second solution is a virtual environment with the purpose to centralize HR processes of promotions and salary increase requests. By setting different constraints such as the employee performance, average market payment for the specific position, department budget and others, the decision regarding the request becomes more efficient and transparent. According to one of the partners, during an interview, working on these requests represents up to one fourth of the useful time from an HR employee. Also, it is worth mentioning that this solution only makes sense for a startup with a workforce of over 100 employees, when the inefficiencies start arising according to the company's top management.

In terms of revenue generation, the service is sold as a subscription model signed annually and paid monthly. The amount each company pays is correlated with its workforce size.

As of the present day, Salars Softwares e Soluções Ltd. has a total workforce of 6 people:

a) 2 partners and co-founders;

b) 2 software developers focused on improving the system operation as well as programming new features; and

c) 2 web designers (both of which are part-time employees) focused on improving user interface and experience.

The roles performed by each of the partners are as follows:

a) Partner A: Customers and Sales Management; Finance and Office Management; Investors Relationship; and Legal Matters.

b) Partner B: Developers Team management.

The roles both partners take part on are:

a) Product Management;

b) Business Intelligence;

c) Clients Interviews; and

d) Recruiting.

In the future, the two partners have plans to distribute stocks among the two developers.

Salars Softwares e Soluções Ltd.'s current sales strategy is to make partnerships with venture capital funds aiming to attend at once all (or most of) the startups under each fund's management instead of reaching potential clients in an individual way. By doing so, the company has managed to obtain its ongoing 40 clients on a 90-days free trial resulted from the partnership with two funds.

According to Partner A, Salars Softwares e Soluções Ltd. faces three main challenges currently:

a) The bad economic scenario for small startups operating in Brazil;

b) The uncertainty if the companies will extend their free trial to paid subscription;

c) The lack of an information security management system.

1.2 PAPER STRUCTURE

In chapter 1, it is presented the context this paper is involved with, which is the governance aspect of the ESG criteria regarding information security and management, as well as the company this study is based on.

In chapter 2, the problem concerning the company and the consequences justifying its relevance are defined. Chapter 3 determines the objectives this paper targets to solve along with the scope of the study. In chapter 4, the theorical basis for this paper is exposed with a literature review. Chapter 5 specifies the methodology used to develop and conduct the study and, in chapter 6, the results are presented and analyzed. Finally, in chapter 7, the conclusion is exposed and next steps are discussed.

2 PROBLEM DEFINITION

Considering its less than one year of existence, its recent customers and contribution of capital as well as a limited number of only 6 employees, Salars Softwares e Soluções Ltd. neither has a system nor processes regarding information security management and privacy of data yet. However, in spite of these governance gaps, the two partners are aware of the problem since obstacles concerning this issue have already manifested themselves, which represent risks to Salars Softwares e Soluções Ltd. and its potential growth.

In terms of revenue generation, it has been reported that five potential customers, although finding relevant value on Salars Softwares e Soluções Ltd.’s solution, have declined the service in the end because of a lack of an information security management system in the startup. In one of these occasions, the partners saw themselves alongside a potential customer’s supplier assessment team, part of which consisted of lawyers, evaluating Salars Softwares e Soluções Ltd.’s information security processes. In another one, it was explicitly asked if they were certificated on the NBR ISO/IEC 27001: 2013. It is interesting to notice that all these five lost customers are significantly bigger and more structured companies than Salars Softwares e Soluções Ltd.’s current average customers are which might indicate that postponing the adoption of a robust information security management system could impose a barrier for obtaining bigger (thus, more profitable) customers and ultimately limiting the startup growth perspective. Numerically, as the current date of this project, even though these declines represent 12.5% of the total amount of Salars Softwares e Soluções Ltd.’s number of customers (40), the percentage in terms of potential revenue loss would be significantly higher because of the revenue model since these companies have a greater workforce.

Another aspect to consider is the legislation and the company’s reputation among the market concerning governance issues. By not having a proper information security management system, Salars Softwares e Soluções Ltd. might become vulnerable to lawsuits especially in terms of the recent Brazilian LGDP. The company also becomes more vulnerable in case of data leakage or hacker attack without any preventive or remedial pre-established security measures and procedures since sensitive data such as employee name, identification number, wages, city of residence and others are being managed.

All these factors and others not mentioned reveal the importance for a company (especially one in an early development phase) to have a robust and proven information security management system to achieve a sustainable growth and return value to the society. Hence, Salars Softwares e Soluções Ltd.'s goal to implement such a system.

3 OBJECTIVE

With the problem this paper addresses being the absence of a data and information security management system in Salars Softwares e Soluções Ltd., the objective of the project consists of implementing one based on the following clauses of the NBR ISO/IEC 27001: 2013:

a) 4 – Context of the organization;
b) 5 – Leadership;
c) 6 – Planning;
d) 7 – Support;
e) 8 – Operation; and
f) 9 – Performance assessment.

Therefore, this paper will not comprehend the implementation of the 10th clause (*Continuous improvement*) of the NBR ISO 27001: 2013 - nor other certifications concerning the analyzed issue – since it has been understood and aligned that clauses 4 – 9 of the referred certification will provide the required basis for Salars Softwares e Soluções Ltd. to further improve the robustness of its data and information security management system as well as other governance features. Also, the environmental and social aspects of the ESG set of standards will not be considered, with the governance pillar being the unique concern.

4 LITERATURE REVIEW

This chapter will present the concepts used as theorical basis for the development and result analysis of this paper.

4.1 QUALITY CONCEPTS

4.1.1 Client Definition

The most common definition concerning client is of an addressee of a product or service provided by a supplier which is often regarded as the final user only. However, clients can also be interpreted as shareholders, employees, internal clients, the government and society. In this sense, the concept should be expanded towards a stakeholder focus as a driver for one business to thrive (BERSSANETI; BOUER, 2018).

This raises the question on who should always be contemplated or at least remembered besides the final client. These are the key stakeholders, the ones who could compromise the delivery to the final client if their needs are not satisfied. There are also other non-critical stakeholders depending on the context of the business that would not cause interference having their boundary conditions respected (BERSSANETI; BOUER, 2018).

4.1.2 Quality Definition

As of the present day, there is no consensus in respect of the definition of Quality, being an extensive and complex concept. The definitions derived from quality gurus are the most frequent ones with each reflecting the context of its time in history (BERSSANETI; BOUER, 2018).

During World War 2, the concept was understood as pattern adequacy considering the necessity of sharing ammunition among Allied Forces. For the post-war, Joseph M. Juran defined it as usage adequacy focusing on the client needs. This mindset reflected, for example, in the automobile industry with vehicle assemblers providing different models for each usage. During the 1970s, known for the two oil crises, the concept saw a shift towards costs adequacy alongside the increasingly relevance of the term productivity and the ascension of Japanese companies on the international scenario. Following this period, Quality move towards client's needs, from adequacy of latent needs during the 1980s and 1990s to client fidelity in the 2000s (BERSSANETI; BOUER, 2018).

Therefore, it can be concluded that definition of Quality is fluid and has changed based on the main challenges of their time. Various of these concepts can be encountered in the same context with companies having the task to interpret its business to prioritize the definition that provides more value.

4.2 QUALITY MANAGEMENT TOOLS

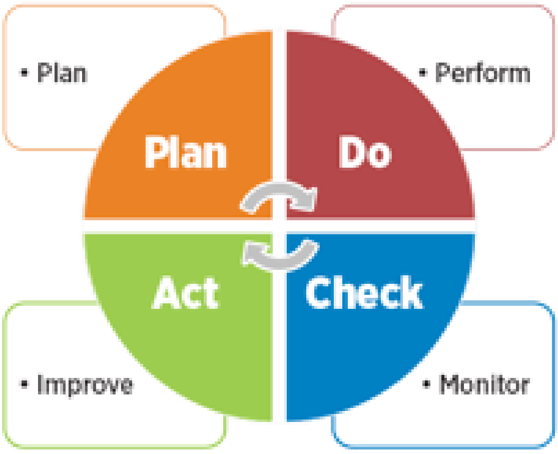
4.2.1 PDCA and SDCA Cycles

The PDCA Cycle (also known as Deming Cycle or Shewhart Cycle), illustrated by **Figure 1** was firstly introduce in Japan with the goal of providing clearness and agility to processes within management. It is, therefore, a management tool, focused on enabling the survival and sustained growth of an organization by yielding guidance the decision-making process for the establishment of goals as well as the means and required actions to execute and monitor them (BERSSANETI; BOUER, 2018).

The cycle should be executed continuously and is composed of four sequential steps:

a) Plan;
b) Do;
c) Check; and
d) Act.

Figure 1 - Illustration of a generic PDCA Cycle



Source: American Society for Quality.

During the Plan step, the goals, plans and projects as well as the methods (processes) to achieve these goals are designed. For the Do step, the established methods are executed with trainings being provided if necessary. The Check consists of verifying the results as well as comparing them with what was planned, and, according to these results during the Act step, the organization acts upon the process (BERSSANETI; BOUER, 2018).

In respect of the scope of this final paper, it can be noticed that the clauses 4 – *Context of the organization*; 5 – *Leadership*; and 6 – *Planning* – of the ISO/IEC 27001: 2013 correspond to the Plan step of the PDCA cycle. Clauses 7 – *Support* – and 8 – *Operations* – correspond to the Do step and clause 9 – *Performance evaluation* correlated with the Check step. Finally, the 10th clause – *Continuous improvement* –, which is not part of this paper's scope, fits in the Act step.

The improvement an appropriate application of the PDCA cycle methodology provides will not have significant effect, however, if it does not become consistent within the organization's routine. This is achieved by standardizing the solutions encountered into the processes of the organization with the SDCA cycle being one appropriate tool for the issue. In it, the Plan step of the PDCA cycle is substituted with the Standardize (S) step, thus assuring a continuous and consistent improvement among the organization (BERSSANETI; BOUER, 2018).

4.2.2 Deming's 14 Points

Deming's 14 Points on Quality Management is a set of management practices to help companies increase their quality and productivity, being a core aspect for implementing Total Quality Management (TQM). Among the advantages of these practices are their versatility to fit into various business and organizational contexts (American Society for Quality).

The 14 points are:

a) 1: Create constancy of purpose toward improvement of product and service, with the aim to become competitive and to stay in business, and to provide jobs;
b) 2: Adopt a new philosophy. We are in a new economic age. Western management must awaken to the challenge, must learn their responsibilities, and take on leadership for change;
c) 3: Cease dependence on inspection to achieve quality. Eliminate the need for inspection on a mass basis by building quality into the product in the first place;

d) 4: End the practice of awarding business on the basis of price tag. Instead, minimize total cost. Move toward a single supplier for any one item, on a long-term relationship of loyalty and trust;

e) 5: Improve constantly and forever the system of production and service, to improve quality and productivity, and thus constantly decrease cost;

f) 6: Institute training on the job;

g) 7: Institute leadership (see point 12). The aim of leadership should be to help people and machines and gadgets to do a better job. Leadership of management in need of overhaul, as well as leadership of production workers;

h) 8: Drive out fear, so that everyone may work effectively for the company;

i) 9: Break down barriers between departments. People in research, design, sales, and production must work as a team, to foresee problems of production and in use that may be encountered with the product or service;

j) 10: Eliminate slogans, exhortations, and targets for the work force;

k) 11: Eliminate work standards (quotas) on the factory floor;

l) 12: Remove barriers that rob the hourly worker of his right to pride of workmanship. The responsibility of supervisors must be changed from sheer numbers to quality;

m) 13: Institute a vigorous program of education and self-improvement; and

n) 14: Put everybody in the company to work to accomplish the transformation. The transformation is everybody’s job (ASQ).

By setting theses points, it can be noticed Deming’s emphasize on the importance of everybody’s participation alongside the pride for accomplishments achieved. Also, the necessity of learning and knowledge with a consistent purpose of continuous improvement are highlighted (BERSSANETI; BOUER, 2018).

Among the points, 2; 6; 7; 13; and 14 are the ones with greater synergy in respect of the nature of this study.

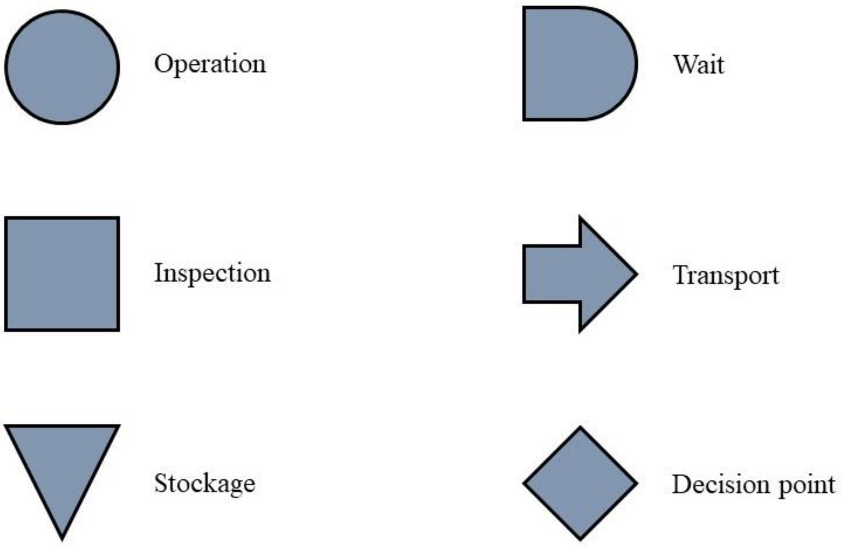
4.2.3 Flowchart

Flowchart is a commonly used tool for quality programs as well as products and services quality improvement process. By being visual, didactic and easy to interpret, it is useful to register the production flow of a product or a service provision for learning, communication and opportunities mapping purposes (BERSSANETI; BOUER, 2018).

The flowchart exhibits the current way a process is being executed, including the responsibility for each activity allowing to compare with how it was designed. Additionally, the tool enables critical analysis alongside audits of process adequacy targeting opportunities for improvement by providing concrete evidences of vulnerabilities and deficiencies sources of the process (BERSSANETI; BOUER, 2018).

Being a support or core business process, each entrepreneurial process can be registered using a flowchart. The adopted symbology does not represent a global pattern, thus normally being the quality function of a company responsible to define the best way the processes are portrait according to the culture (BERSSANETI; BOUER, 2018). This paper, however, uses the classical symbology to represent a flowchart illustrated below.

Figure 2- Classical symbology of a flowchart



Source: author.

When planning the design of a flowchart, it is fundamental to consider the following aspects (BERSSANETI; BOUER, 2018):

a) The participation of all involved parts of the process;
b) Mapping key specifics of the process with questions that enable knowing:
    i) What happens firsts;

ii) What is the source of the material or information;

iii) How does the material reaches processing;

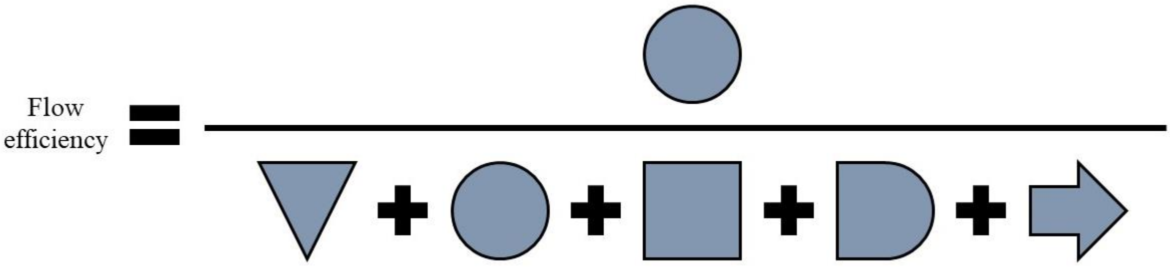
iv) Where are the decisions being made;

v) What is the destiny of the product/service of this operation; and

vi) What controls are made during the production or service provision.

The symbology presented earlier enables the usage of one key indicator for industrial operations: the flow efficiency indicator, illustrated by **Figure 3**. It highlights an efficient process as one with the highest proportion of operation activities, in other words, activities that aggregate value to the inputs, alongside with the least number of other symbols (BERSSANETI; BOUER, 2018).

Figure 3- Flow efficiency indicator



Source: adapted from BERSSANETI; BOUER (2018).

4.2.4 Process Decision Program Chart diagram

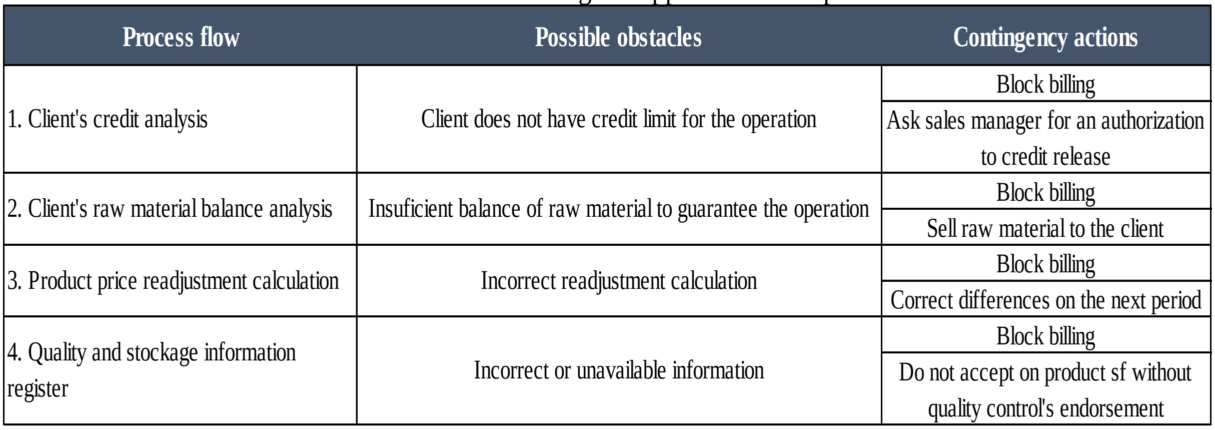
The Process Decision Program Chart Diagram (PDPC) exhibits probable events as well as its contingencies that might occur during the implementing of a project. It is used to plan each possible sequence of events that must happen when the problem or targeted objective is not fully known (BERSSANETI; BOUER, 2018).

The tool’s purpose is to identify all variations and uncertainties inherited to the environment that may affect the accomplishment of one organization’s goals. The PDPC Diagram not only anticipates possible route deviations, but can also develop contingencies plan and alternative flows to treat and prevent them respectively. Besides this, since the alternative actions are already planned, the speed of response is increased (BERSSANETI; BOUER, 2018).

Being a versatile tool, the PDPC Diagram can be adopted in projects in general. It significantly contributes with any formed team involved with activities in which the mapping of critical events and a pre-established response policy must be considered to guarantee success. Additionally, it is recommended to explore as much as possible previous experiences from people and past projects (BERSSANETI; BOUER, 2018).

An exemplified application of the PDPC Diagram is presented below by **Table 1**.

Table 1 - PDPC Diagram application example



Process flow	Possible obstacles	Contingency actions
1. Client's credit analysis	Client does not have credit limit for the operation	Block billing Ask sales manager for an authorization to credit release
2. Client's raw material balance analysis	Insuficient balance of raw material to guarantee the operation	Block billing Sell raw material to the client
3. Product price readjustment calculation	Incorrect readjustment calculation	Block billing Correct differences on the next period
4. Quality and stockage information register	Incorrect or unavailable information	Block billing Do not accept on product sf without quality control's endorsement

Adapted from BERSSANETI; BOUER (2018).

4.3 MANAGEMENT BY GUIDELINES

Strategy is an Action Plan targeted to achieve an established objective. Strategy management comprehends processes of developing, evaluating and making decisions in order for an organization to achieve its mid and long-term objectives. By establishing its strategic plan, one organization should be aware of the questions (BERSSANETI; BOUER, 2018):

a) Are the mission, vision and strategy well interpreted and defunded among everyone involved?
b) Are the values and beliefs clearly defined and deeply known by everybody involved? And
c) Are these values and beliefs specific enough as well as recognized as relevant?

The process of strategic planning can be broken on the following parts:

a) Evaluation: an analysis of the current performance;

b) Mission: what is done, the existence purpose;
c) Vision: what it aims to become;
d) Strategic Plan: how to achieve the proposed vision based on the current performance;
e) One Action Plan: how to establish short-term action plans to achieve the mid and long-term objectives.

The strategic unfolding provides guidance for planning and actions among the whole value flow within an organization, establishing the connections between its needs and daily activities. Being a top-down analytical approach, this break-down should be done by methodic procedures of introducing activities, processes, projects, programs or systems for all areas among an organization (BERSSANETI; BOUER, 2018).

Strategic objectives correspond to what has been agreed between high management translating one organization's vision. For each aspect of the vision, one objective and target level should be defined (in some cases, it may be interesting to define two levels for each objective, with the first one being the bottom acceptable level and the second one being the desired optimum level).

The number of objectives to be defined should follow the conciseness principle since the mere addition of new objectives does not automatically increase the quality of the strategic plan. Therefore, in general, five to ten strategic objectives can be considered enough. To be qualified for its introduction on the company's strategic plan, these objectives must follow five criteria (BERSSANETI; BOUER, 2018):

a) A strategic objective should be achievable;
b) It must be relevant throughout all the levels of an organization;
c) The objective and its associated metric must be clear among everyone involved;
d) It must be measurable and its associated metric calculated with minimum effort. If a given objective cannot be measured, it has no value, thus should not be included in the strategic plan;
e) A strategic objective should only be included if it represents something that is controllable, that is, the ones involved with it must be able to exert control over the factors determining and affecting the objective.

The management by guidelines, which can also be understood as an application of the PDCA cycle to the management process, identifies change initiatives, selects objectives for the modifications identifies the critical measures of performance, define projects to reach these objectives and allocates resources for its execution. The means to achieve such goals define a group of specific actions to reach the established strategic objectives.

Via management by guidelines, conditions are created for the management of the daily organization’s priorities. It is a systematic way of breaking and aligning the organization regarding its strategic objectives, highlighting the contribution of each area or sector with their own specific objectives. By breaking the guidelines, it is possible to provide autonomy for each area among the organization enabling what actions each one of them should take (BERSSANETI; BOUER, 2018).

The management by guidelines contemplates five elements:

a) Declaring a desired objective: defining the direction the organization should follow;
b) Results and goals to achieve organized in a timeline;
c) A deadline for the achievement of each goal;
d) Boundary conditions;
e) Guidance to establish the means and processes.

Table 2 below exemplifies the five principles.

Table 2 - Five elements of management by guidelines

Direction	Quantitative result	Deadline	Boundary conditions	Means and processes to achieve
Market share increase	From: 40% To: 70%	2 years	Do not decrease product quality	Map and meet clients needs Develop new products Reduce the time to market

Adapted from BERSSANETI; BOUER (2018).

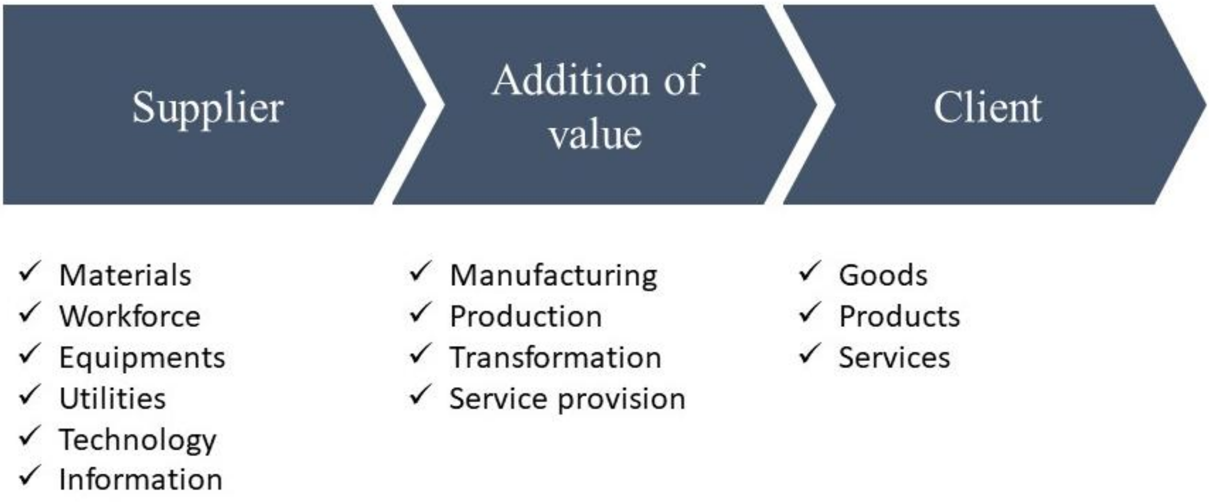
4.4 CROSS-FUNCTIONAL MANAGEMENT

Cross-Functional Management (CFM) is a methodology for continuous evaluation, analysis and improvement of processes performance for a given company in relation to the satisfaction among its customers and shareholders. In this case, process is understood as a set of rationally linked activities adding value to the inputs and generating an output that meets a client need. A system of quality is made by a set of processes properly organized and provides the operational organizational context to the project teams.

Within the CFM, there is incentive for a broad involvement of all the members of one organization. This generates more satisfaction with the job given a clearer activities description, better skills development as well as an increase of individual autonomy and authority for the individuals.

A set of activities is characterized as a process when three basic elements are identified: the process supplier; addition of value; and the client (BERSSANETI; BOUER, 2018). **Figure 4** below illustrates the flow of these basic elements:

Figure 4- Elements of a process



Adapted from BERSSANETI; BOUER (2018).

A process can be interpreted as one supplier-client chain with each link contributing for the desired end achievement – the client satisfaction. A lack of systemic view, however, might incur relevant interface kind problems between the steps of the process generating obstacles for a smooth and efficient flow especially regarding different areas/departments, where these issues become more highlighted (BERSSANETI; BOUER, 2018).

Generally, a process performance is evaluated by indicators related to three aspects:

a) Efficacy;

b) Efficiency; and

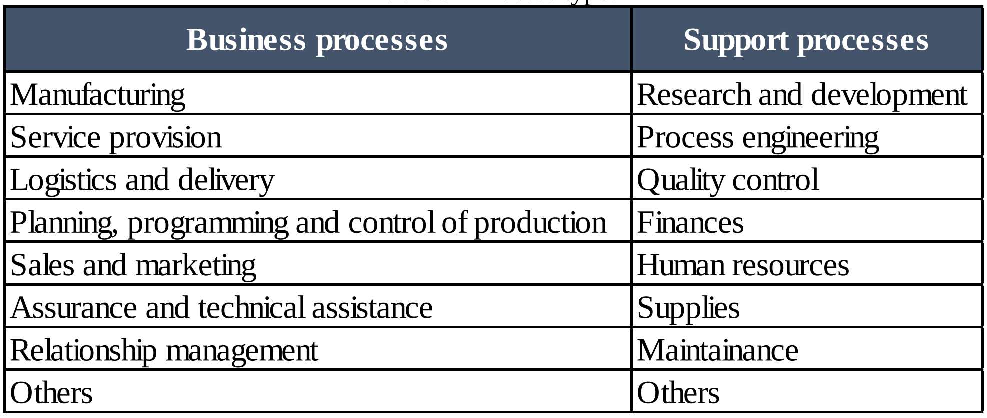
c) Adaptability.

The efficacy can be defined as the extension in which the objectives are successfully achieved raising the question on how well conditioned the process is to satisfy the clients' needs continually and consistently. Efficiency relates to how well are the resources applied and used to generate the results bringing the challenge to optimize the employment of resources. Finally, adaptability relates to how well and fast does the process respond to changes. In this sense, it should be able to rapidly adjust itself to satisfy new requirements (BERSSANETI; BOUER, 2018).

Within companies, processes are normally split into two group: business processes and support processes.

Business processes are the ones related to the generation of value among a company with the final output being internalized monetary resources for it. On the other side, support processes are responsible for sustaining the existing business processes by providing conditions for their execution, thus generating value to internal clients. **Table 3** below presents a list of exemplified processes segmented by business and support ones for a given manufacturing or service company.

Table 3 - Process types



Business processes	Support processes
Manufacturing	Research and development
Service provision	Process engineering
Logistics and delivery	Quality control
Planning, programming and control of production	Finances
Sales and marketing	Human resources
Assurance and technical assistance	Supplies
Relationship management	Maintainance
Others	Others

Adapted from BERSSANETI; BOUER (2018).

4.5 RISK MANAGEMENT

4.5.1 Failure Mode and Effects Analysis

The Failure Mode and Effects Analysis (FMEA) is an approach aiming to identify ahead potential problems, its effects and causes to establish mechanisms of detection, control and intervention assuring quality and reliability required by the client. Its first appearance occurred during the 1960s at the National Aeronautics and Space Administration (NASA) being currently used mostly on the automotive industry.

FMEA's finality is to prevent the occurrence of problems being a resource that should be applied in a team scenario. In this sense, the tool uses a systematic analysis to reveal and orientate potential failures of products and processes in development, thus helping with the proposal of preventive actions (BERSSANETI; BOUER, 2018).

Eight major contributions of this methodology could be appointed:

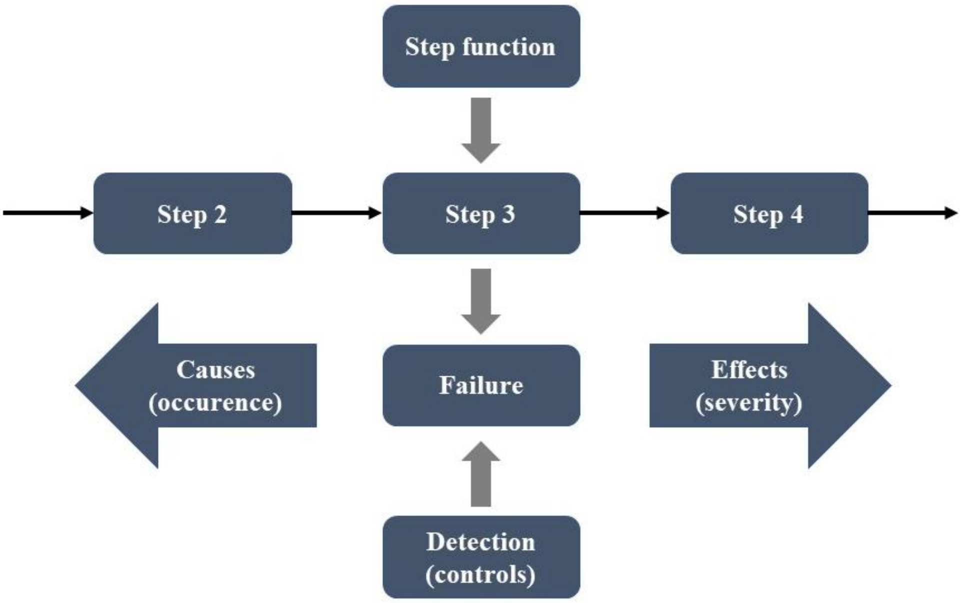
a) Reduce the development time of processes and products;
b) Review underperforming processes;
c) Reduce the volume of reworks;
d) Increase the productivity of the development of new processes by reducing the workforce needed to do so;
e) Reduce operations problems;
f) Promote integration as well as multifunctional work;
g) Document and disseminate the risks from the development of products and processes; and
h) Avoid project and processes failures reaching the client.

By applying the tool, one can obtain the Risk Priority Number (RPN), which consists of the product of three key elements of the FMEA:

a) Severity of the failure;
b) Occurrence (causes of the failure); and
c) Detection (controls).

These three elements of the RPN are given partial scores with each one ranging from zero to ten. The failures with the highest overall score are prioritized. **Figure 5** illustrates the relationship between the RPN elements.

Figure 5- RPN's three elements



Adapted from BERSSANETI; BOUER (2018).

The step function of the process expresses the demand the step attends to. It should be described in a concise way with the information regarding the environmental conditions as well specifications the process is to operate. It is also recommended formatting the step function on the format: verb on infinitive with a noun (BERSSANETI; BOUER, 2018).

A Failure is described as the way a system/component and/or an operation/activity can fail and not attend to its pre-established function. It is, thus, the way the failure manifests itself by not accomplishing the expectations from the client and requirements from the project/process.

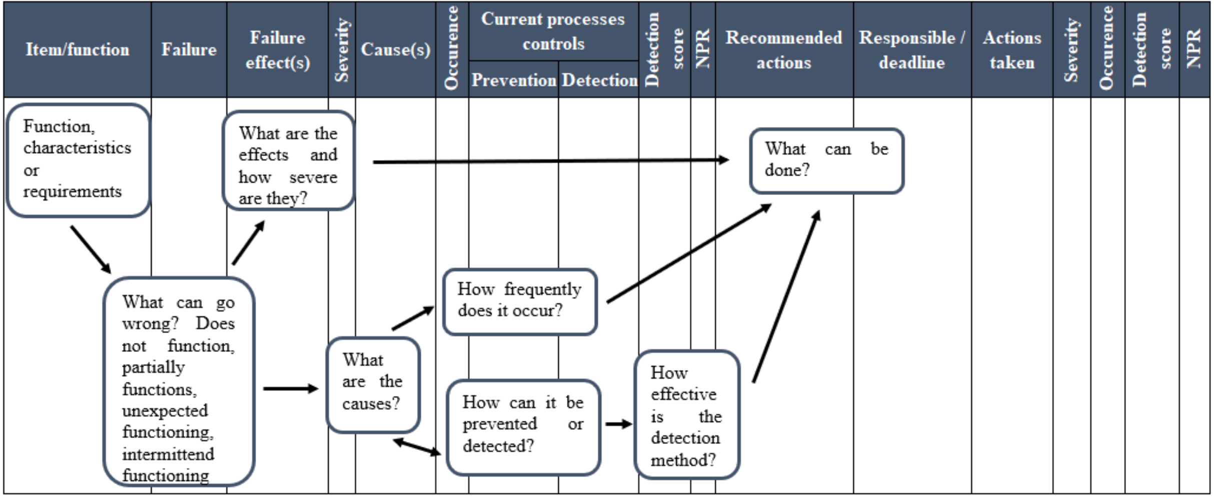
The Failure Effect on the FMEA corresponds to the consequences of the failures from a point of view of what internal and external clients can experience in term of usage requisites, function or product situation. The more severe the effect is, the higher the attributed score.

A cause of a Failure can be defined as the reason why the failure will be manifested, being an indication of a process or project flaw. It is also possible that the same failure is a consequence of multiples causes and vice-versa. Aiming at orienting preventive measures, the causes should be described in the most specific way. Additionally, the more frequent the cause is, the higher its score.

Finally, the Detection as a probability estimative of detecting the failure where it occurs and with the demanded precision. With a low amount of control and detection mechanisms, the lower becomes the probability of properly detecting the failure and the higher its evaluation score is (BERSSANETI; BOUER, 2018).

Figure 6 exemplifies the application of the FMEA using a sheet.

Figure 6 - Logical sequence for applying the FMEA


Item/function
Failure
Failure effect(s)
Severity
Cause(s)
Occurence
Current processes controls
Prevention
Detection
Detection score
NPR
Recommended actions
Responsible / deadline
Actions taken
Severity
Occurence
Detection score
NPR
Function, characteristics or requirements
What are the effects and how severe are they?
What can be done?
What can go wrong? Does not function, partially functions, unexpected functioning, intermittend functioning
What are the causes?
How frequently does it occur?
How can it be prevented or detected?
How effective is the detection method?

Adapted from BERSSANETI; BOUER (2018).

4.6 INDICATORS MANAGEMENT

In recent decades, the concept of productivity has been widely discussed among the business and academic communities. However, its meaning has been frequently misunderstood with the concepts of efficacy and efficiency, which also have separate meanings (BERSSANETI; BOUER, 2018). In this sense, a clarification of such terms is required in this final paper.

Thus, the definition of productivity for this paper is the following:

$$Productivity = \frac{Outputs}{Inputs}$$

Some possible inputs are human resources; technology; information; capital; energy; utilities; and materials (BERSSANETI; BOUER, 2018).

In respect of efficacy and efficiency terms, there is no consensus for their definition among literatures. Therefore, the International Organization for Standardization (ISO) convention is used.

In this sense, efficacy is understood as an output or execution indicator measuring the performance of an organizational system focusing on its results, in other words, calculating how much the objectives have been accomplished. For efficiency, it is a measure of how economically the resources are used to promote a given satisfaction level of clients and other stakeholders, being defined as follows:

$$Efficiency = \frac{Real\ obtained\ output}{Expected\ output}$$

Another indicator concept is availability. This can be defined as the relation between the effective available time and the total expected time of operation for a given resource. One way to measure this is by using the Mean Time Between Failures (MTBF), which corresponds to the average time it takes between two consecutive failures (BERSSANETI; BOUER, 2018). Thus, the availability indicator can be calculated as:

$$Availability = \frac{MTBF}{MTBF + MTTR}$$

With MTTR being the Mean Time to Repair, corresponding to the average to repair the resource.

An analysis of the Availability expression can provide some oriented actions for management. The MTBF, being a reliability indicator, can be defined as the probability for the given resource to execute its function in pre-define conditions and during a pre-determined time range. The MTTR is a maintainability indicator corresponding to the probability of reestablishing a resource operating specified condition for a given time interval and with the usage of pre-established resources.

Such kind of indicators become especially relevant for cases of companies using a highly integrated network infrastructure which is the case for Salars Softwares e Soluções Ltd. In this sense, it is not the availability of the system itself being valued, but the guarantee of executing the service. Thus, the lack of availability compromises the assurance to the clients of properly providing the service (BERSSANETI; BOUER, 2018).

4.7 SERVICE LEVEL AGREEMENT

4.7.1 Introduction

Although there is not a consensus among literature regarding the definition of Service Level Agreement (SLA), it can be understood as a contract formalizing a business relationship between two parts, being of valuable usage since it determines measurement standards for the provided service. In spite of a current widespread application for this contract approach, SLAs have arisen during the 1990s as a way of Technology Information departments measure and manage the quality of service they were providing among the company (BERSSANETI, 2006).

According to Lee and Ben-Natan (2002), SLAs frequently have a form of a contract negotiated between a service provider and a consumer defining the price for the possession right of the service under specific terms, conditions and financial assurances. Additionally, SLA is a formal agreement between the two mentioned parts targeting the establishment of a mutual comprehension of the services, priorities and responsibilities.

Among the benefits of SLA application, one can firstly appoint the protection of the service provider from false expectations of the client by pre-establishing and documenting acceptable and achievable levels of performance regarding the user and service supplier respectively. In this sense, a point of reference concerning the client expectations is defined, thus giving stability to the deal alongside the monitoring of mutual agreed service quality indicators. Another benefit from using SLAs is the security it brings to the client by providing him less costly options in case of a non-accomplishment of the agreed expectations. By contracting a service without SLAs, the client becomes subject of costly alternatives such as renegotiating the contract, paying fines or recurring to lawsuits if the level of quality does not attend to what as expected and the service receiver (BERSSANETI, 2006).

4.7.2 SLA types

According to Sturm, Morris and Jander (2000), there are three types of SLAs as follows:

a) In-house SLAs;
b) External SLAs; and
c) Internal SLAs.

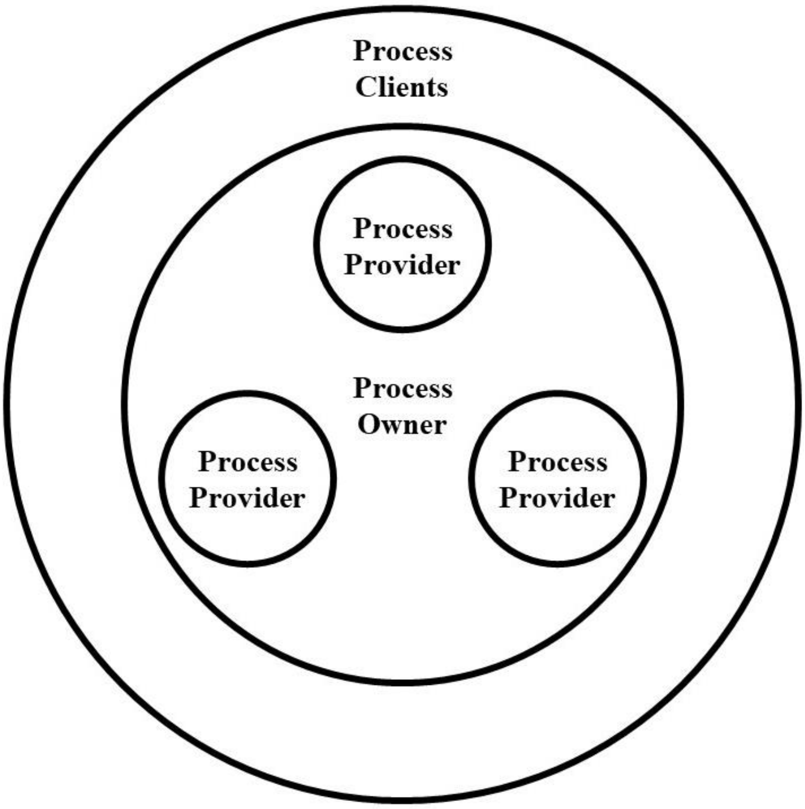
Their differences consist of the formality given to each creation process of the deal, the language employed as well as possible consequences in case the agreed service level is not fulfilled. However, the content of each agreement and the creation process itself remain fundamentally the same for each SLA type (STURM, MORRIS AND JANDER, 2000).

In-house SLAs correspond to deals between the service provider and an internal client. Although these parts are within the same organization, the establishment of SLAs can be advantageous to guarantee an overall higher reliability level. External SLAs occur between the service provider and an external client (other organization) and requires more caution on its preparing since it legally bonds two different organizations as well as legal revisions. Finally, internal SLAs are used by the service provider to measure the performance of different groups within itself. This third type of SLA is linked with annual performance reports and provides mechanisms to assign to groups and individuals their specific part among a broader service. In this case, its intentions and commitments might be incorporated in other documents such as objectives and goals (BERSSANETI, 2006).

4.7.3 SLA development process

Even though individual SLAs can be developed in an isolated form between the provider and service user, it is generally more profitable to develop a family of SLAs in the context of a business general process. In this sense, it is essential for the service provider to acknowledge the response capabilities of its internal and third-party processes (BERSSANETI, 2006). **Figure 7** illustrates a diagram exposing the relationships between the process owner, the process client as well as the business general process providers.

Figure 7- SLAs in the context of a business general process

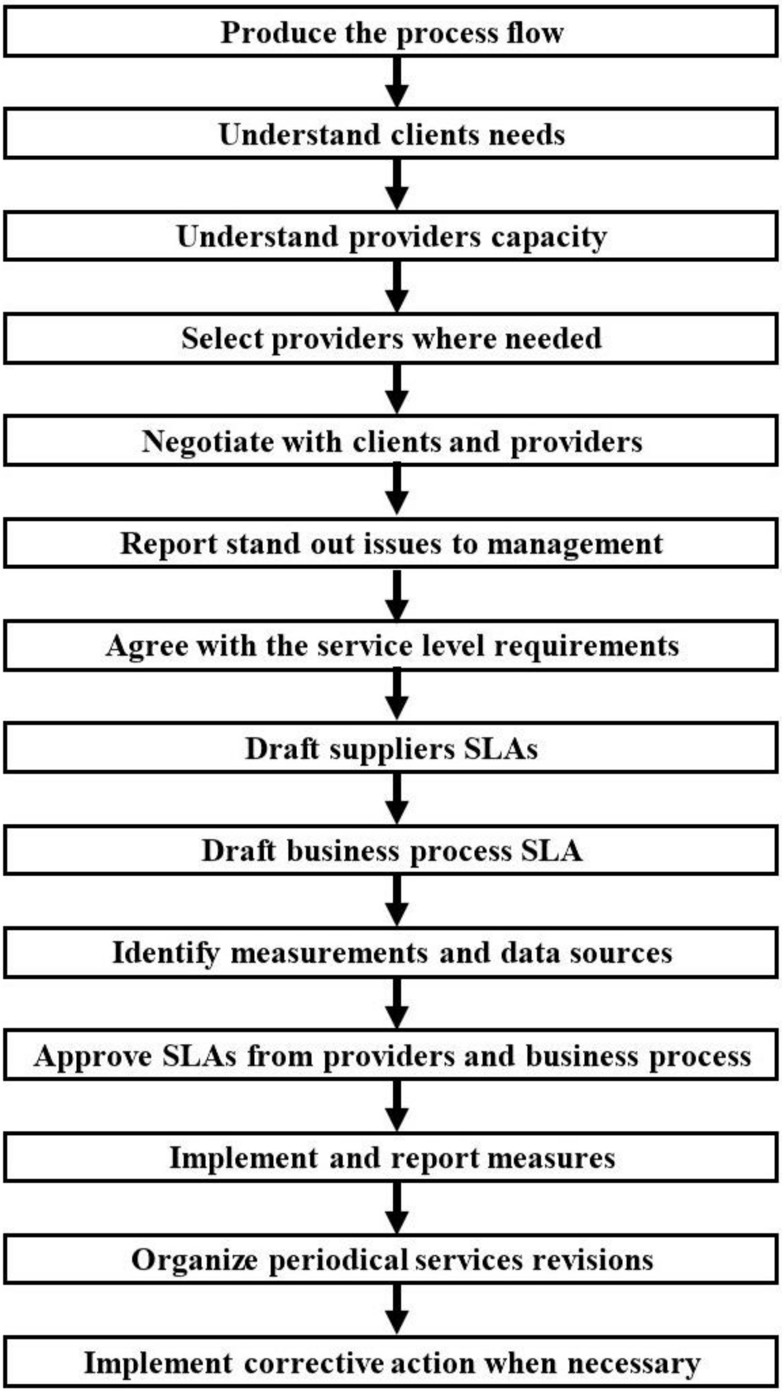


Adapted from BERSSANETI, 2006.

The process owner is responsible for managing the business processes as well as its overall quality. The process client can be external or a function inside the organization requiring the output of the specific process. The process providers supply individual services such as IT systems or manual operations and possibly being an external organization (BERSSANETI, 2006).

With this put, the diagram of **Figure 8** shows the role of the process owner regarding both the development for the business general SLA process alongside the client and the development of individual SLAs from the general process providers. Although this development process can be seen as a sequence of fourteen steps, it is probable that, in practice, interactions and overlay of steps occur.

Figure 8 - SLA process development


Produce the process flow
Understand clients needs
Understand providers capacity
Select providers where needed
Negotiate with clients and providers
Report stand out issues to management
Agree with the service level requirements
Draft suppliers SLAs
Draft business process SLA
Identify measurements and data sources
Approve SLAs from providers and business process
Implement and report measures
Organize periodical services revisions
Implement corrective action when necessary

Adapted from BERSSANETI, 2006.

According to Berssaneti (2006), the first step consists of producing a diagram containing a detailed flow of the business general process and it is among the process owner responsibility. This is a valuable means for identifying the various process providers as well as all the interdependencies between activities. Also, it is recommended that the diagram should be distributed and reviewed by everyone participating on it.

For the second step, it is pointed the focus on the real necessities of the client, not his desires. In this case, the process owner might need to work alongside the client to clarify the business needs. Additionally, it is important to identify and understand the clients' priorities to make a distinction between must-have and nice-to-have requirements.

Once the clients' needs are properly understood, the third step objective is to recognize the capabilities of the providers. For the case of when the providers have flexibility on what they deliver, it should be distinct what is flexible from what is not as well as the limits and costs concerning these flexibilities.

The fourth step is composed of selecting providers where they are required. There are cases where this is not possible due to internal restrictions privileging the usage of in-house providers. When these constraints do not exist, however, external providers should be selected mainly considering the client needs as well as other aspects such as costs.

After the selection, the fifth step consists of linking the agreement details to the providers. In case a provider cannot deliver what was considered necessary, a new discussion with the client is needed possibly leading back to the second step of understanding the client needs.

For the sixth step, any unresolvable matter during the negotiation should be brought to the organization senior management. The decision for these issues should be based upon the required performance the organization needs along with the costs it is prepared to deal with.

During the seventh step, a complete definition of the performance requirements should be made and approved by the all the involved parts.

For the eighth step, the providers should draft the SLA of their respective contributions to the general process. The drafts should then be analyzed by the process owner, the one to receive the service. New negotiations among the client, process owner and providers might arise with the probable identification of deeper issues during this step.

At this nineth step, by knowing the SLA from the providers as well as the requirements of the service level, the process can draft the SLA for the general process. Part of this is achieved by combining and aggregating the SLAs from the providers to obtain an end-to-end visualization. In this step, it is important that the process is reviewed by the client to guarantee an alignment between performance and requirements. Also, this assures the providers are capable of the attending to their obligations.

Regarding the tenth step, SLA measures should focus on a small amount of key performance indicators. These will provide the required information to determine if the process is running accordingly as well as anticipated warning to management. They also should:

a) Echo the aspects of major importance to the client;
b) Monitor items with high impact over the process;
c) Monitor trends to allow anticipated corrective actions; and
d) Be highlighted to all the parts involved with the usage and provision of the process.

In case of unavailability of automatic measurement methods, manual methods should be considered periodically or when issues regarding the process provision arise.

The eleventh step consist of approving the SLAs of the providers and business process. The first group will be signed by the process owner alongside managers directly responsible for the service provision. The general process SLA should be signed by the highest hierarchical management level of both the client and process owner respective organizations. Theirs' signatures indicate an acceptance of the contract terms and compromises both parts to provide the required resources to allow the achievement of the agreed performance level during the proposed time span.

The twelfth step of this process is composed of implementing and reporting pre-planned measurements during the development of the general process. Three aspects to consider are:

a) The reports emission frequency;
b) At which process steps performance measurements require the aggregating of data from providers; and
c) The reports should highlight any identified failure on attending to the required performance standards and register any action taken to correct the issue.

The thirteenth step of consists of organizing periodical meetings to review the service and the SLA performance as well as agree on any required corrective action. Providers should also be included if necessary. Additionally, these meeting should bring discussions concerning future plans between the client, process owner or providers that might affect the service provision as well as any achievable performance improvement the client could request for example.

Finally, the fourteenth step is composed of implementing corrective actions when necessary, in other words, if the required performance have not been achieved.

With these fourteen steps, the development of the SLA process should be completed. However, as mentioned, SLA is a contract. Thus, the next phase consists of documenting what was agreed.

In this sense, Sturm, Morris and Jander (2000) appointed fourteen aspects of attention should be considered during the contract phase. Because such issues are not among the main scope of this final paper, these aspects are only briefly presented as follows:

a) Aspect 1: Parts of the deal;
b) Aspect 2: Duration;
c) Aspect 3: Scope;
d) Aspect 4: Limitations
e) Aspect 5: Objectives of service level;
f) Aspect 6: Indicators of service level;
g) Aspect 7: Non-accomplishment;
h) Aspect 8: Add-ons;
i) Aspect 9: Exclusions;
j) Aspect 10: Reports;
k) Aspect 11: Management;
l) Aspect 12: Reviews;
m) Aspect 13: Corrections; and
n) Aspect 14: Approvements.

4.8 NBR ISO 27001: 2013

4.8.1 Introduction

The International Organization for Standardization (ISO) is a non-governmental independent organization based on Geneva, Switzerland, focused on developing international standards on several areas based on the consensus of experts (as well as other organizations such as the International Electrotechnical Commission and the International Telecommunication Union) to be adopted by other organizations (especially companies); raising public awareness regarding standardization; and promoting teaching and training for standardization. ISO’s structure is composed by the General Assembly, a meeting consisted of its members and Principal Officers set up annually. Below it, there is the ISO Council, constituted of 20 members in a rotational scheme, being the main governance body of ISO.

Its foundation dates to the post-World War 2 scenario in 1947 after 65 delegates from 25 countries have encountered to debate International Standardization. As of the present day, ISO have 167 members, each of which corresponding to a country, 808 technical committees and subcommittees focused on standards development and 24366 International Standards with some of the most well-known standards being the follow:

e) ISO 1000, for the International System of Units;
f) ISO 9001, for Quality Management Systems;
g) ISO 14001, for Environmental Management Systems;
h) ISO 31000, for Risks Management; and
i) ISO/IEC 27001, for an Information Security Management.

Each country-member has its own association representing it at ISO. For the case of Brazil, the southern-American country is represented in the form of the Brazilian Association of Technical Standards (ABNT in Portuguese). In this sense, taking into consideration the company this paper will be based on, the ISO/IEC 27001 for this project is in the form of the Brazilian NBR ISO 27001: 2013 version.

This document is a set of standards co-developed with the IEC providing requirements for the implementation of an Information Security Management System (ISMS), first published in 2005 and updated in 2013 as of its most recent version. Supported and influenced by risks management, the ISO 27001 focuses on the protection of three key elements of information:

a) Confidentiality: the information is not to be available or disclosed to unauthorized people, entities or processes;
b) Integrity: the information is complete and accurate, and protected from corruption; and
c) Availability: the information is accessible and usable as and when authorized users require it.

Among some of the benefits of one organization adopting this set of standards, the following can be appointed:

a) Physical access control;
b) Firewall policies;
c) Security staff awareness programs;
d) Procedures for monitoring threats;

e) Incident management procedures; and

f) Encryption.

Concerning its structure, the NBR ISO 27001 is organized in eleven clauses ordered from 0 to 10, with the first three clauses referring in the following order to the Introduction, Scope, Normative References, and Terms and Definitions. The 4 to 10 clauses are the mandatory requirements this final paper is based on except for the tenth clause – Continuous Improvement.

4.8.2 Clause 4 - Context of the organization

The fourth clause of the NBR ISO/IEC 27001: 2013 have four subclauses with the objective of prompting the organization in question on gaining knowledge on the context it is inserted as well as understand its stakeholders needs and expectations to determine the ISMS's scope.

These subclauses are the following:

a) 4.1 – Understanding the organization and its context;

b) 4.2 – Understanding the needs and expectations from the stakeholders;

c) 4.3 – Determining the ISMS's scope; and

d) 4.4 – Information Security Management System.

For the first subclause, the organization must map its relevant internal and external aspects relevant for its purpose which might affect its capability of achieving the pre-established goals with the ISMS.

On the second subclause, the organization must determine the relevant stakeholders regarding the ISMS. After this, theirs' requirements should be appointed.

The third subclause prompts the organization to establish the limits of its ISMS by determining its limits. This should be done based on what was considered on the previous subclauses of Clause 4 as well as the interfaces and dependencies between activities performed by the organization in question and external ones. Also, the scope should be available as documented information.

For the fourth subclause, the organization must design, implement, maintain and continuously improve its ISMS according to ISO's standards.

4.8.3 Clause 5 - Leadership

This clause focuses on guaranteeing the commitment of the organization’s top management towards the ISMS by the form of concrete actions such as the implementing of an information security policy as well as the definition of roles and responsibilities regarding the ISMS.

It is organized in three subclauses:

a) 5.1 – Leadership and commitment;

b) 5.2 – Policy; and

c) 5.3 – Responsibilities and organizational roles.

On the first subclause, the top management’s commitment towards the ISMS should be demonstrated by a set of actions. These include the assurance of an alignment of between the ISMS goals and the organization’s strategic direction as well as an integration of its processes with the ISMS. Also, the leadership must assure a proper provision of resources towards the ISMS and communicating the importance of fulfilling the requirements of this set of standards.

The second subclause establishes an information security policy ought to be implemented by the top management on the organization. This policy should be anchored to defined guidelines such as being aligned with the organization’s purpose along with the inclusion of the information security objectives and its commitment towards the ISMS continuous improvement. Additionally, not only the policy must be properly documented, but also communicated to all stakeholders.

For the third subclause, the top management is prompt to assure the respective roles and responsibilities regarding information security are properly defined and clearly communicated through the organization. In this sense, roles for assuring the ISMS is in accordance with the ISOs requirements as well as communicating the ISMS’s performance to top management should be delegated.

4.8.4 Clause 6 – Planning

By managing sensitive information, one organization is automatically inserted in a risk environment concerning security. Therefore, to properly manage the risks and provide compliance towards its stakeholder, not only they should be mapped and communicated, but also treated with specific processes. Clause 6 of NBR ISO/IEC 27001 focuses on the planning of such management aspects.

4.8.4.1 Subclause 6.1 – Actions to manage risks and opportunities

While planning its ISMS, an organization must consider the topics concerning subclauses 4.1 and 4.2 as well as determine the risks and opportunities ought to be contemplated to:

a) Assure the ISMS can achieve its pre-established goals;

b) Prevent or reduce undesired effects; and

c) Achieve continuous improvement.

Also, the organization must plan not only actions to consider these risks and opportunities, but how to integrate and implement such actions with the existing processes of the ISMS as well as measuring theirs' effectiveness.

Concerning the information security risks evaluation, the organization should define a process for evaluating these risks. Such process must fulfill the following guidelines:

a) Establish information security risks criteria not only for accepting these, but to evaluate it performance;

b) Assure the information security risks evaluations return comparable, valid and consistent results;

c) Identify information security risks regarding confidentiality, integrity and information availability within the ISMS scope. Additionally, each risk should have a designated responsible;

d) Analyze the information security risks by evaluating the potential effects if they materialize, estimating the probability of such materialization and determining the levels of risk;

e) Evaluate the analyzed risks by comparing them with risks criteria defined as well as prioritizing them for treatment; and

f) Retaining the information documented regarding the risk evaluating process.

The treatment of information security risks should also be established as a process in the organization according to the following requirements:

a) Appropriately select the information security treatment options considering the risks evaluation results;

b) Determine all the necessary controls to implement the selected options. Such controls might come up from within the organization as well as from external sources;

c) Compare such control with the ones presented in Annex A[1, 2] to verify if a necessary control is omitted;
d) Develop a statement of applicability containing the necessary controls as well as the reasons for excluding or adding other control regarding Annex A;
e) Prepare an information security risks treatment plan;
f) Obtain the required approvals from the ones responsible for information security risks treatment plan as well as the acceptance of residual risks; and
g) Retain the documented information regarding information security risks treatment process.

4.8.4.2 Subclause 6.2 – Security management objective and the respective planning to achieve it

The organization must establish the information security objectives for the relevant functions and levels. Such objectives must:

a) Be consistent with the information security policy;
b) Be quantifiable (if appliable);
c) Be in accordance with the applicable information security requirements and the results from the risks evaluation and treatment;
d) Be communicated; and
e) Be updated appropriately.

Also, the organization should retain the documented information concerning the information security objectives.

When developing the plan for achieving such objectives, the organization must determine:

a) What is to be done;
b) The required resources;
c) Who is the responsible;
d) When will it be concluded; and

[1] Annex A contains a list with 114 controls and its objectives. The users of NBR ISO/IEC 27001: 2013 are instructed to use the annex to assure no control is omitted.

[2] The objective controls are implicitly included on the controls. These Annex A objectives are not exhaustive, thus additional controls and objectives might be necessary.

e) How will the results be evaluated.

4.8.5 Clause 7 - Support

This clause refers to the establishment of the appropriate people, infrastructure, materials and other resources to assure a proper implementation, operation and continuous improvement of the ISMS. It is composed of five subclauses:

a) Resources;
b) Competences;
c) Awareness;
d) Communication; and
e) Information documentation.

The first subclause determines the organization should select and provide the necessary resources to establish, implement, maintain and improve the ISMS.

For the second subclause, the organization determine the required competences from its direct subordinates that affects the ISMS performance. In this sense, the competence of such people must be assured based on education, training and the appropriate expertise. If such competences do not currently exist, actions should be taken to acquire them as well as measuring the effects of these actions. Finally, the documentation concerning this topic should be stored as evidence.

In relation to the third subclause, the organization must guarantee its workforce is aware of the information security policy as well as theirs' contributions towards the ISMS effectiveness (including the benefits of its improvement). They should also be aware of the consequences of a non-accordance with the ISMS' requirements.

For the fourth subclause, internal and external communications relevant to the ISMS must by determined by the organization. This should include:

a) What to communicate;
b) When to communicate;
c) Who communicates;
d) Who to be communicated; and
e) The communication process.

The fifth subclause establishes the inclusion of documenting the information required by the NBR ISO/IEC 27001: 2013's set of standards as wells as information considered as necessary by the organization. It should be noted that the coverage of the documented information might vary depending on the organization size, activities, workforce competence as well as the complexity of its processes. Also, when updating or creating a new documented information regarding the ISMS, the organization must assure its proper identification and description, format and critical analysis followed by its approval concerning adequacy. Finally, the information in respect of this Norm must be properly controlled, assuring the following aspects:

a) Availability and use adequacy (when and where required);
b) Be properly protected;
c) Distribution, access, recover and usage;
d) Storage and preservation (including its legibility);
e) Updates control (such as versions control); and
f) Retention and availability.

Additionally, external information considered as relevant by the organization for planning and operating the ISMS must be properly identified and controlled.

4.8.6 Clause 8 - Operation

Eighth clause of this Norm determines how the established ISMS from previous clauses should operate. It contains three subclauses:

a) 8.1 – Operational planning and control;
b) 8.2 – Information security risks evaluation; and
c) 8.3 – Information security risks treatment.

For the first subclause, the organization should plan, implement and control the necessary processes to attend to the information security requisites as well as to implement the action determined by subclause 6.1. Also, the organization should implement the plans required by subclause 6.2 to achieve its information security objectives.

Besides this, to assure the processes are running as planned, the organization must keep the information properly documented. Furthermore, planned changes should be controlled and the effects of unplanned changes must be critically analyzed with the organization providing actions to mitigate any adverse effect as necessary. Outsourced processes should also be mapped and controlled.

The second subclause determines periodic planned risks evaluations by the organization or when significant changes are proposed considering the established risks criteria. Moreover, the information regarding this process should be documented and stored.

Within the third subclause, the organization must implement the security information risks treatment plan as well as document and retain the information from this process and its results.

4.8.7 Clause 9 - Performance evaluation

NBR ISO/IEC 27001: 2013 nineth clause helps the organization on evaluating the ISMS performance by setting monitoring, measuring, analyzing and auditing requirements to be followed. It is composed of three subclauses:

a) 9.1 – Monitoring, measurement, analysis and evaluation
b) 9.2 – Internal audit; and
c) 9.3 – Top management’s critical analysis

For the first subclause, the organization should evaluate the ISMS performance by assuring the following aspects:

a) What needs to be monitored and measured, including information security controls and processes;
b) The methods for monitoring, measuring, analyzing and evaluating, as applicable, to assure valid results;
c) When should the monitoring and measurement occur;
d) What should be monitored and measured;
e) When should the results be analyzed and evaluated;
f) Who is to perform the analysis and evaluation of such results; and
g) Documenting and retaining the information regarding this set of steps as evidence of monitoring.

The second subclause establishes the organization should periodically conduct planned internal audits to provide information on how the ISMS is in accordance with its own set of requirements and the ones determined by NBR ISO/IEC 27001: 2013, as well as if it is effectively implemented and maintained. The organization should also:

a) Plan, establish, implement and maintain an audit program, including its frequency, methods, roles, planning requisites and reports. Such program should consider the importance of pertinent processes as well as the results from previous audits;
b) Define the scope and criteria for each audit;
c) Select auditors and conduct audits assuring objectiveness and impartiality of the auditing process;
d) Assure the audit results are properly reported; and
e) Retain the documented information as evidence of audit programs and results.

The third subclause determines the organization’s top management must critically analyze the ISMS during planned intervals. This analysis should include the following aspects:

a) The status of previous critical analysis actions performed by top management;
b) Relevant internal and external changes concerning the ISMS;
c) Review of the ISMS performance, including trends on non-accordance and corrective actions, monitoring and results from measurement, audit results, fulfillment of the information security objectives;
d) Review of stakeholders;
e) Risks evaluation results as well as the status of the risks treatment plans; and
f) Opportunities for continuous improvement.

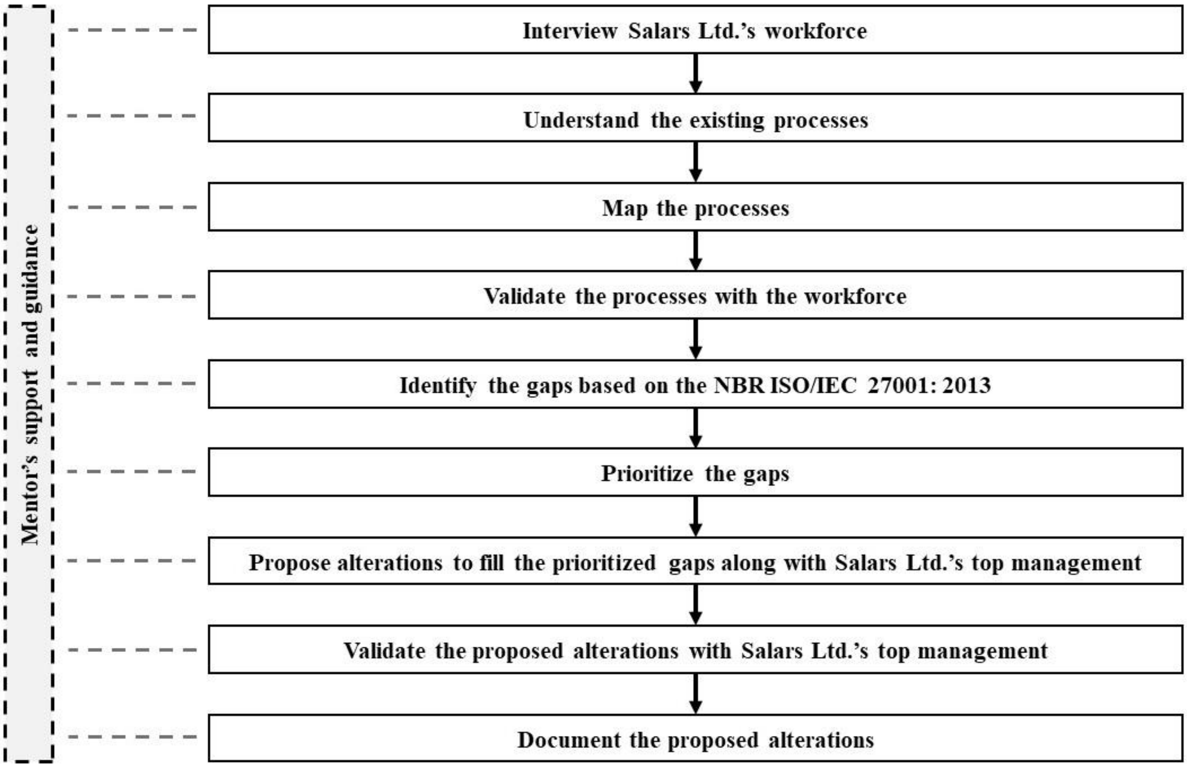
The output from such critical analysis by the top management should also include decisions regarding mapped improvement opportunities as well as any identified demand of changing aspects of the ISMS. Furthermore, the information of this critical analysis process should be documented and stored as evidence.

5 METHODOLOGY

This final paper will be based on available information from Salars Softwares e Soluções Ltd. existing documentation, interviews set with its partners and the rest of its workforce if necessary as well as direct observations regarding its current situation. Also, a frequent set of follow-up and guidance meetings with this study mentor is expected.

The project is to be structured in a series of recurring processes, each corresponding to a clause from NBR ISO/IEC 27001: 2013. Although adaptions might occur depending on the specificity and the demands of each clause as well as the context of Salars Softwares e Soluções Ltd., a generic flow illustrated by **Figure 9** can be drafted.

Figure 9 - Work process of the final paper


Mentor's support and guidance
Interview Salars Ltd.'s workforce
Understand the existing processes
Map the processes
Validate the processes with the workforce
Identify the gaps based on the NBR ISO/IEC 27001: 2013
Prioritize the gaps
Propose alterations to fill the prioritized gaps along with Salars Ltd.'s top management
Validate the proposed alterations with Salars Ltd.'s top management
Document the proposed alterations

Source: author.

The first step consists of gathering general information regarding Salars Softwares e Soluções Ltd.'s business context, revenue model, products, environment as well as other data with the objective of obtaining an overview of its reality.

After this, the second step focuses on understanding the company processes by also interviewing its workforce, however this time with the purpose of documenting its processes concerning the scope of this final paper. By using second step as an input, in third step the processes are mapped as flowcharts based on the Business Process Modeling Notation (BPMN) with the software Bizagi™ from the company Bizagi Ltd.

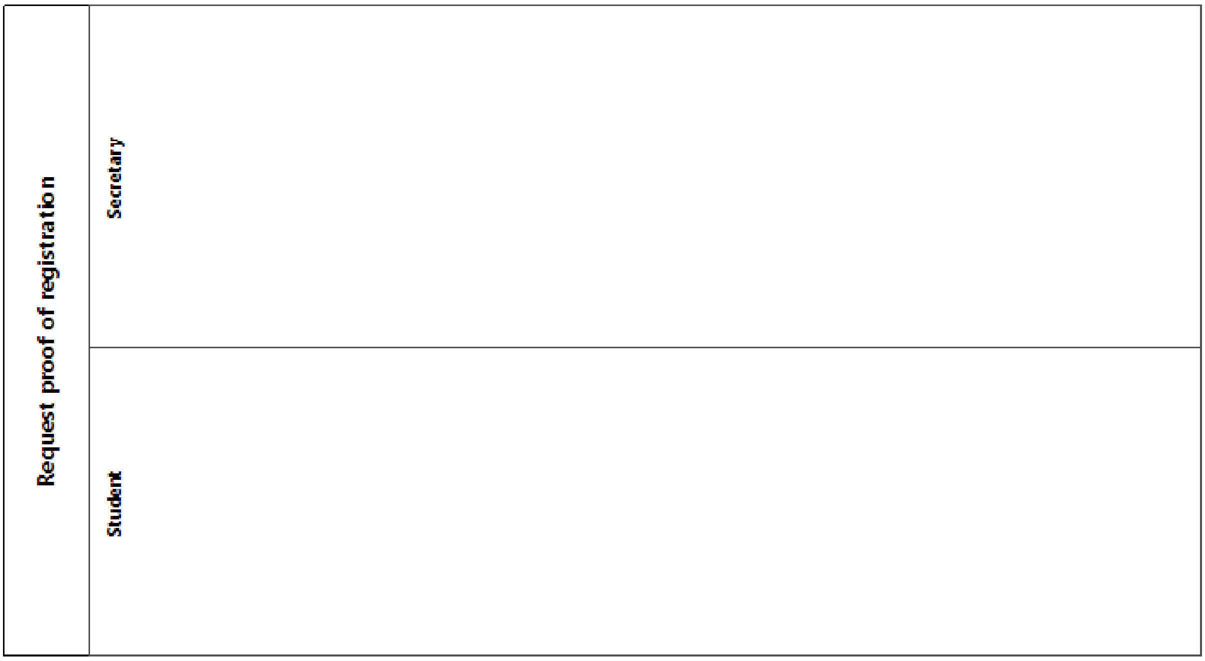
The BPMN notation is a graphic representation of easy understanding having basic elements to demonstrate the hierarchy of activities making possible the occurrence of processes within an organization and it is based on the PDCA cycle (LONGARAY, 2017). With this notation, there are seven key elements allowing a precise representation of the existing processes as follows:

j) Pool;

k) Lane;
l) Activity;
m) Data object;
n) Event;
o) Flow; and
p) Gateway.

Pool and Lane elements are the base foundations for developing BMPN models. The former has the purpose of informing the process laid out and the latter representing its owners (LONGARAY, 2017). **Figure 10** illustrates the relationship between these two elements:

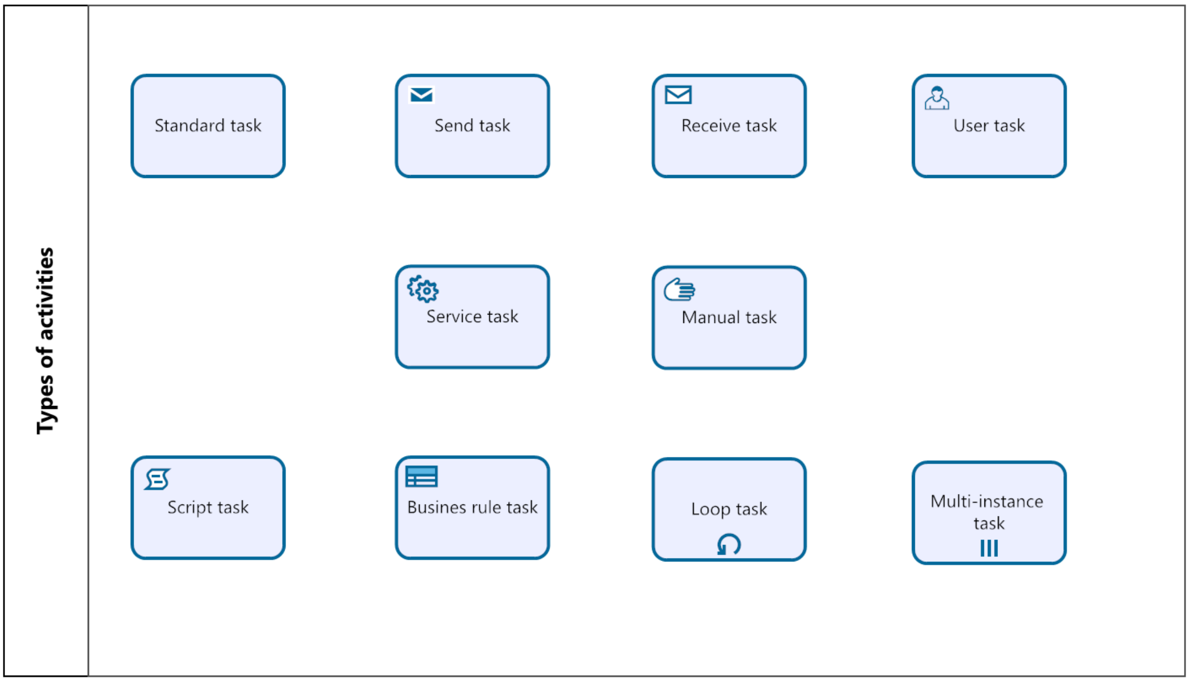
Figure 10 - Pool and lane



Source: adapted from Longaray, 2017.

Activities can be defined as part of the process execution flow aggregating to the input. In the BPMN, there are ten types of it as illustrated by **Figure 11** and described by **Table 4**.

Figure 11 - BPMN types of activity



Source: adapted from Logaray, 2017.

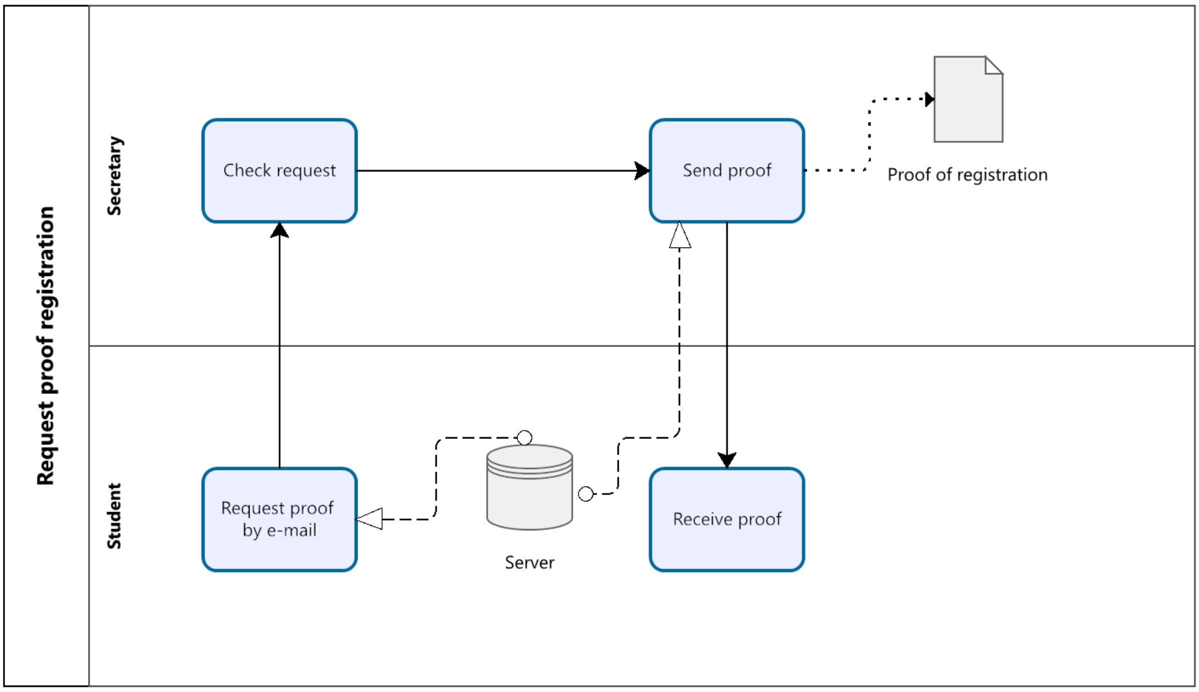
Table 4 - Description of each BPMN type of activity

Type of activity	Description
Standard	Does not require a thorough explanation due to its simplicity
Send	Used when there is a demand to exchange messages with an external actor for the conclusion of the activity in question
Receive	Analogous to the send activity, the external actor receives the sent message
User	Executed by a single person with a computational support
Service	Provides to an external participant information enabling him to accomplish his task
Manual	Neither a computational nor a mechanic resource is used
Script	Informs when a script format code is used on software demonstrations
Business rule	Must meet the established business rules to be accomplished
Loop	Must be executed multiple times until the task is accomplished
Multi-instance	Its execution is similar to the Loop one, however it uses data objects for its conclusion

Source: adapted from Longaray, 2017.

Data objects are all types of files, systems and directories used for a task accomplishment. Flow element is the direction the process moves from its beginning to its conclusion (LONGARAY, 2017). Such elements are illustrated by **Figure 12**.

Figure 12 - Data object and flow elements



Source: adapted from Logaray, 2017.

Events are graphic demonstrations allowing the identification of when a given process starts or is concluded (LONGARAY, 2017). There are three types of events:

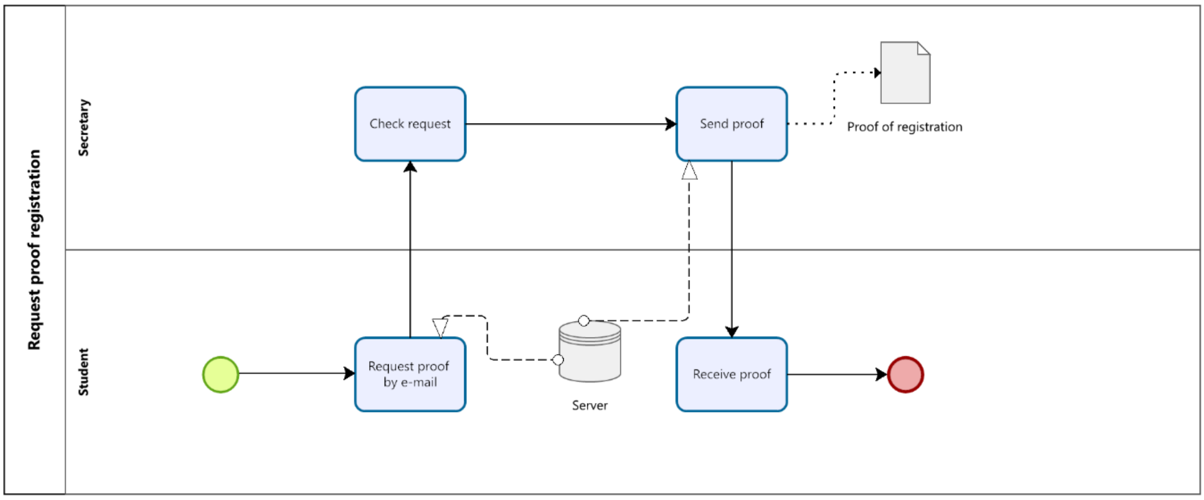
a) Start event – activates the process as a result of external events or due to the conclusion of a prior process;

b) Intermediate event – occurs during the process and is activated by a variety of triggers, generally as a response of errors; and

c) End event – concludes the process allowing the sending of start information for the beginning of other processes.

These are illustrated by **Figure 13**.

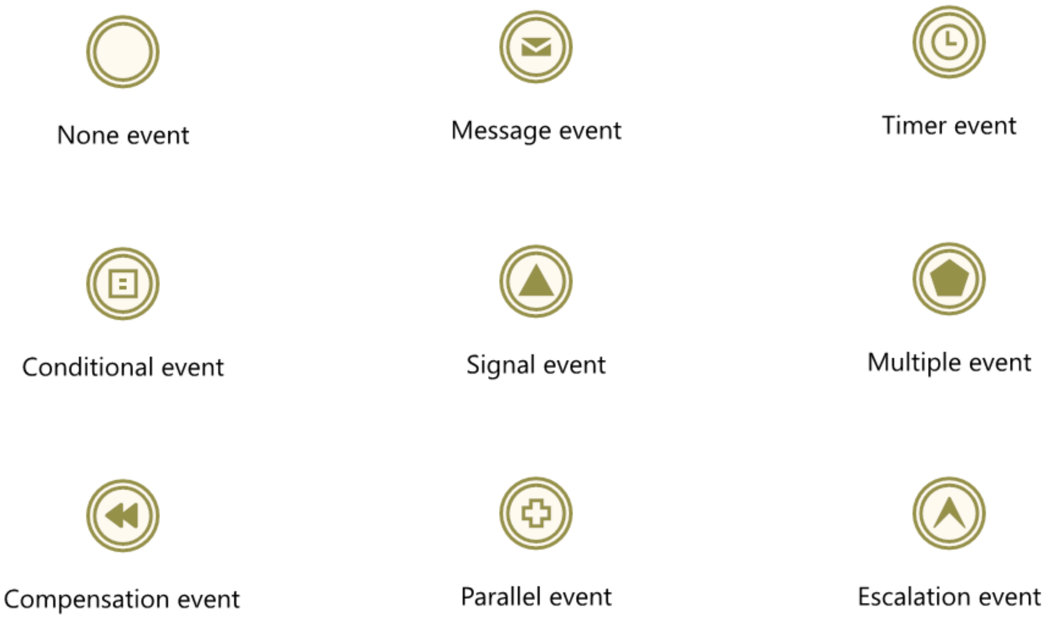
Figure 13 - Events on BPMN



Source: adapted from Longaray, 2017.

There are nine types of intermediate events illustrated and described, respectively, by **Figure 14** and **Table 5**.

Figure 14 - Types of intermediate events



Source: adapted from Longaray, 2017.

Table 5 - Types of intermedia events description

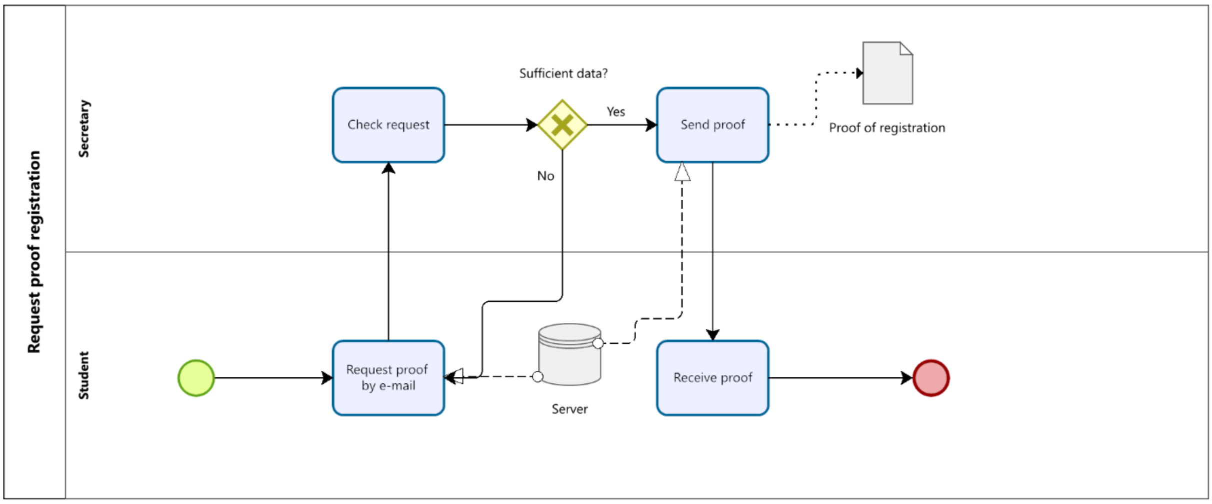
Type of event	Description
Standard	Standard general event
Message	Informs when an activity is started by the reception of messages

Timer	Determines the time limit for the activity conclusion
Conditional	Temporarily suspends a task for the update of a pending information
Signal	Restarted right after the solution of the pendency identified in the conditional event
Multiple	Set the start of other concomitant activities
Compensation	Allow the adding of a second process, substituting the first one which is cancelled due to a continuity problem caused by the requester
Parallel	Allows the execution of various activities
Escalation	Similar to the compensation type of event, however with the continuity problem being due to the actor himself, who transfer the activity to another substitutive process

Source: adapted from Longaray, 2017

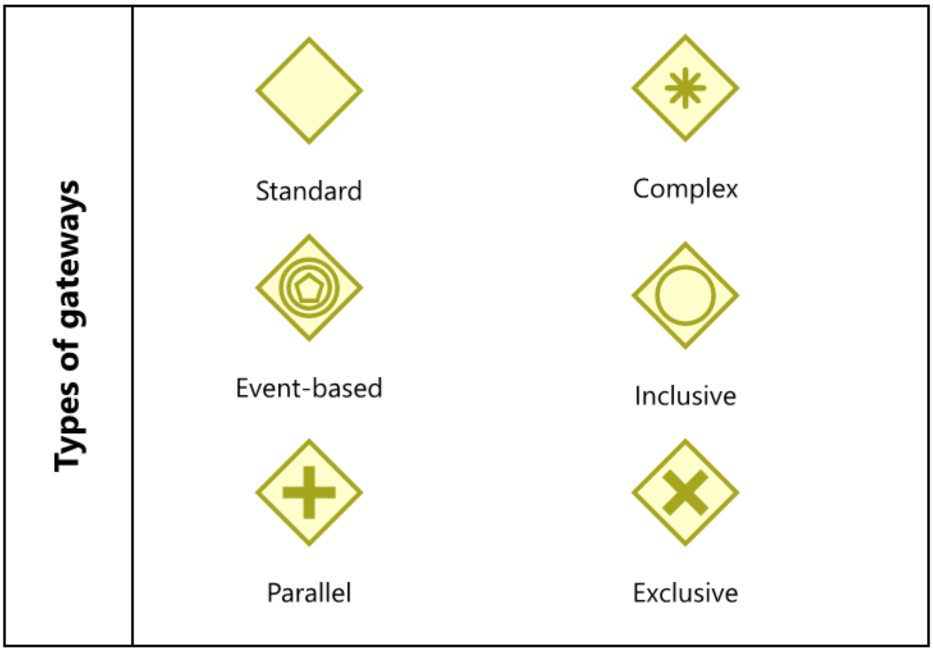
Gateways are used to control the interactions between the activities in a process as well as its overall flow (LONGARAY, 2017). **Figure 15** and **Figure 16** illustrate, respectively, an example of a gateway usage and the types of gateways. **Table 6** describes each gateway type.

Figure 15 - Example of gateway usage



Source: adapted from Longaray, 2017.

Figure 16 - Types of gateways



Source: adapted from Longaray, 2017

Table 6 - Gateways description

Type of gateway	Description
Standard	Allows for two options: either advance towards the next step or return to the previous one
Complex	Initialized only when a series of prior parameters is accomplished. Used when a certain number of variables are necessary to authorize a new process
Event-based	According to the requester need, occurs only when a certain activity is executed originating more than one process
Inclusive	Allows the entrance of various flow arrows: aggregates the activities and allows their flow to one or more sequential activities
Parallel	The flow is split in two that are executed parallelly
Exclusive	The process flow through only one of the exits

Once the processes are mapped with the BPMN notation, these will be validated with Salars Softwares e Soluções Ltd. workforce to assure conformity between what happens in the company with what was documented. After this, the gap analysis is done, also conjunctly with Salars Softwares e Soluções Ltd. workforce, by comparing whether each requisite of the NBR ISO/IEC 27001: 2013 is attended by the company's processes concerning data security. In this sense, each requirement is given a score reflecting its implementation status as shown by **Table 7**.

Table 7 - Gap analysis score criterion

Implementation status	Score
Fully attends	0
Partially attends	1
Does not attend	2

Source: author

With the gaps identified, a prioritization step will take place to map the most relevant ones based on the company context. Thus, each requirement is given a score consisted of the product of three variables:

a) The implementation status score given during the gap analysis;

b) The requirement overall impact on Salars Softwares e Soluções Ltd.'s ISMS and market performance; and

c) The effort demanded to fulfill the gap in question.

Each requirement impact score will be calculated along with Salars Softwares e Soluções Ltd. top management during the set of interviews expected for this step. **Table 8** demonstrates how this scoring is set.

Table 8 - Requirement impact score criterion

Impact on the ISMS performance	Score
The corresponding requirement is a nice-to-have attribute and its absence represents minor implications on the ISMS performance with a very low degree of relationship and dependency with other requirements	1
The corresponding requirement is a nice-to-have attribute and its absence limits other nice-to-have functionalities of the ISMS	2
The corresponding requirement is a nice-to-have attribute and its absence limits other must-have functionalities of the ISMS	3
The corresponding requirement is a must-have attribute	4

The corresponding requirement is a must-have attribute with its absence causing major implications on other must-have functionalities	5

Source: author

The effort criterion is another variable to be considered in the prioritization step due to the limited time and resources of this final paper. Thus, **Table 9**, adapted from Moreira (2021), represents a description of each effort level with its corresponding score.

Table 9 - Requirement effort score criterion

Level	Definition	Score
Process design	Design of a completely new process	1
Development of a complex document	Design of a long document, with a high degree of content complexity and technicality	2
Process alteration	Altering the way a process is executed involving document modifications as well as raising awareness of the alterations with the ones involved	3
Development of a simple document	Design of a short document, with a low degree of content complexity and technicality	4
Document alteration	Alterations, such as modification, updates, inclusions and exclusions of elements, on existing documents	5

Source: adapted from Moreira, 2021.

After the overall score is given for each requirement, the requirements are going to be ranked with the top scoring ones being selected for the next step of proposing alterations to fill the identified gaps relative to the NBR ISO/IEC 27001: 2013. The solutions proposal execution is going to be based on four aspects.

a) The theory presented in Chapter 4;
b) Salars Softwares e Soluções Ltd.'s workforce and top management business and operation context knowledge to ensure an alignment between the solutions and the company's reality;
c) The mentor's support, knowledge and guidance; and

d) External sources if needed, possibly including experts for domains with a high level of technicity concerning data and information security.

After the solutions are validated, they will be documented in an appropriate format considering their specificity.

6 RESULTS AND DISCUSSION

6.1 METHODOLOGY REVISION

With the beginning of this second part of the work, it was noted the need to change the methodology to be used to implement the ISMS and, consequently, the work plan. Thus, it was defined that the ISMS to be designed would meet all the requirements in the standard NBR ISO/IEC 27001:2013 in order to make the organization suitable for certification. Consequently, there would no longer be a prioritization of requirements since all should be satisfied.

The reasons for this were due to considerations pointed out by the CEO that, although a non-certifiable ISMS would contribute to the organization's information security, the gains from this (in sales, reputation and information security terms) would be small compared to a certified ISMS. In addition, due to the high allocation of all the company's manpower in view of its current context, both partners considered that there would be hardly any resources and availability to operate a non-certifiable ISMS and implement at the same time one that meets the requirements of the standard. Thus, it was decided to comply with the request of the company's top management.

With this, it was decided to conduct a review of the order in which the design of processes aiming to meet the Clauses of the standard would follow seeking a more agile and efficient approach since it was noticed that the order presented in NBR ISO/IEC 27001:2013 had certain inadequacies that would bring difficulties in its implementation. Thus, Wens (2019) proposes an approach formed by 10 steps which was understood to be more appropriate to implement the standard considering the context of the company. Such an approach is presented by Table 10.

Table 10 – 10-Steps implementation plan

Step	Activities

1	1. Buy the ISO/IEC 27001 standard. 2. Appoint an information security officer (or a comparable role) and assign responsibilities and authorities to this role to ensure that the management system meets the requirements (5.3). 3. Appoint a project leader (this may be the security officer mentioned above) and make a project plan. 4. Make sure to get the necessary resources for the project (7.1). 5. (Re)organize your document management (7.5).
2	1. Perform a context analysis (4.1 and 4.2). 2. Use the outcome of the context analysis to determine the scope of your management system (4.3). 3. Determine all outsourced processes within the scope (8.1). 4. Determine the risks for the management system as a whole and implement actions to address these risks (6.1.1).
3	1. Define a process for risk assessment that meets the requirements of the Standard and your own requirements (6.1.2). 2. Define a process for risk treatment that meets the requirements of the

	Standard and your own requirements (6.1.3). 3. Define a process for managing competence that meets the requirements of the Standard and your own requirements (7.2). 4. Define a change-management process that meets your own requirements (8.1). 5. Determine which processes must be monitored and measured and how this must take place (9.1). 6. Determine an audit program and define a process for conducting internal audits (9.2)
4	1. Perform the risk assessment process defined in step 3. The results of this initial assessment give you an impression of the current status of your information security risks (6.1.2) 2. Perform the risk treatment process defined in step 3 and determine the necessary controls (6.1.3) 3. Compare the controls that you have determined with those in Annex A and produce a SoA (6.1.3) 4. Formulate a risk treatment plan for unacceptable risks 5. Obtain risk owner's approval for this plan and risk owner's acceptance of the residual risks (6.1.3).

5	1. Establish an information security policy (5.2). Take the results of the initial risk assessment into account 2. Establish measurable information security objectives (6.2). Take the results of the initial risk assessment into account (6.2c) 3. Publish and communicate your information security policy (5.2) 4. Determine which information security objectives should be monitored and measured and how this should take place (9.1) 5. Develop awareness training for all persons doing work under the organization’s control (7.3) 6. Request quotes from accredited certification bodies and choose a date for the certification audit (see chapter “Certification audits”)
6	1. Implement your risk treatment plan (6.1.3/8.3) 2. Implement your communication plan (7.3) 3. Make a schedule for all necessary actions and monitor this schedule (8.1) 4. Determine which processes should be monitored and measured and how this should take place (9.1)

	5. Determine which controls should be monitored and measured and how this should take place (9.1) 6. Start using your process for managing competence (7.2) 7. Organize awareness training for all persons doing work under the organization’s control (7.3)
7	1. Ensure that processes, controls, and plans are monitored and measured, and retain documented information as evidence of the results (9.1) 2. Perform a full internal audit and retain documented information as evidence of the results (9.2)
8	1. Correct all established nonconformities and, where possible, remove the causes of nonconformities (10.1) 2. Make necessary improvements to the management system (10.1 and 10.2)
9	1. Prepare a management review (9.3). Collect relevant information about the management system and think of questions that can be submitted to top management to have your management system reviewed 2. Perform a management review (9.3) and ensure that all review comments, decisions, and necessary actions are documented

	3. Plan and perform the actions that (possibly) come from the management review
10	1. Demonstrate that your management system is effectively implemented and maintained by performing an additional risk assessment at this time, so that you can compare the results of this assessment with the results of your first assessment (see step 4). If all went well, your information security management system has made a positive contribution to the development of your information security risks

Source: adapted from Wens, 2019

6.2 PROCESSES MAPPING

Once the company did not have any documentation regarding the execution of its processes, it was understood as necessary that these were determined and mapped using the BPMN language. With the processes displayed in flowcharts, a greater alignment among all those involved is achieved in the project due to its visual representation. . Also, with clearly determined processes, it is easier to specify the scope of the ISMS - which will be done later - as well as to determine risks and opportunities for improvement. Finally, the existence of documented processes, even if not those required by the standard, facilitates the certification of the organization due to the reasons stated above.

Thus, 14 processes were mapped. The process by which this was done involved cycles of interviews and validations with the CEO. Some processes highlighted below were not mapped with flowcharts, since their execution does not involve a logical order that can be displayed in a flowchart. For such processes, another way of documenting them was stipulated as a next step. The processes in are listed below:

a) Onboarding of clients;

b) Clients' system update;

c) Clients’ exclusion;

d) Clients’ password change;

e) Entry of employees;

f) Departure of employees;

g) Change of employees’ equipment;

h) IT Infrastructure management;

i) Database management (no flowchart);

j) Source code repository management (no flowchart);

k) Internal passwords management (no flowchart);

l) Workforce training (no flowchart);

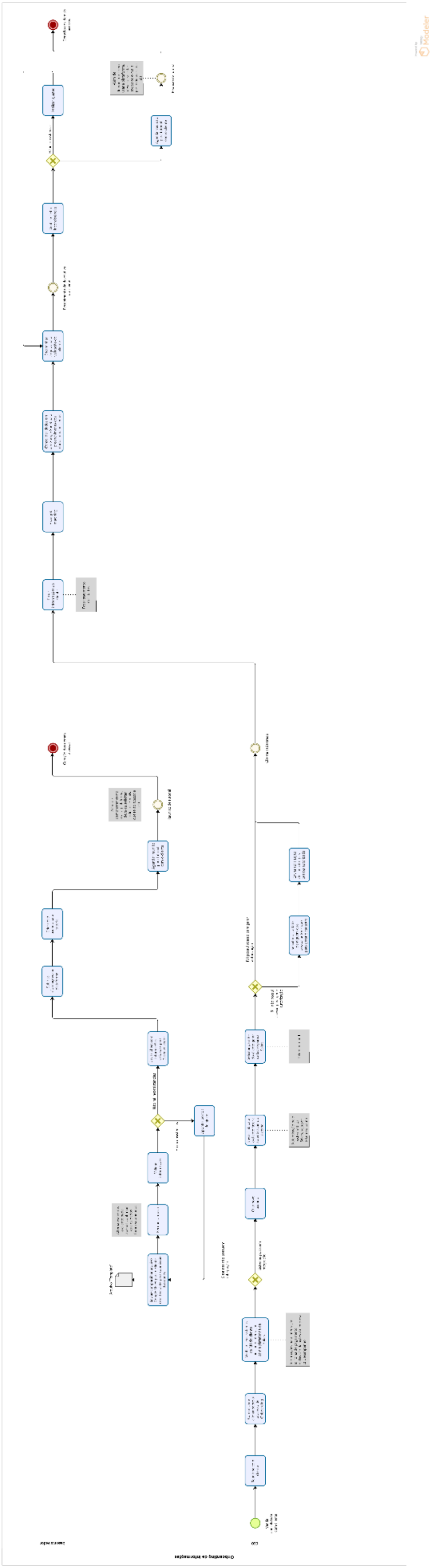
m) Backup management (no flowchart);

n) Response to incidents; e

o) Products’ maintenance and updates (no flowchart).

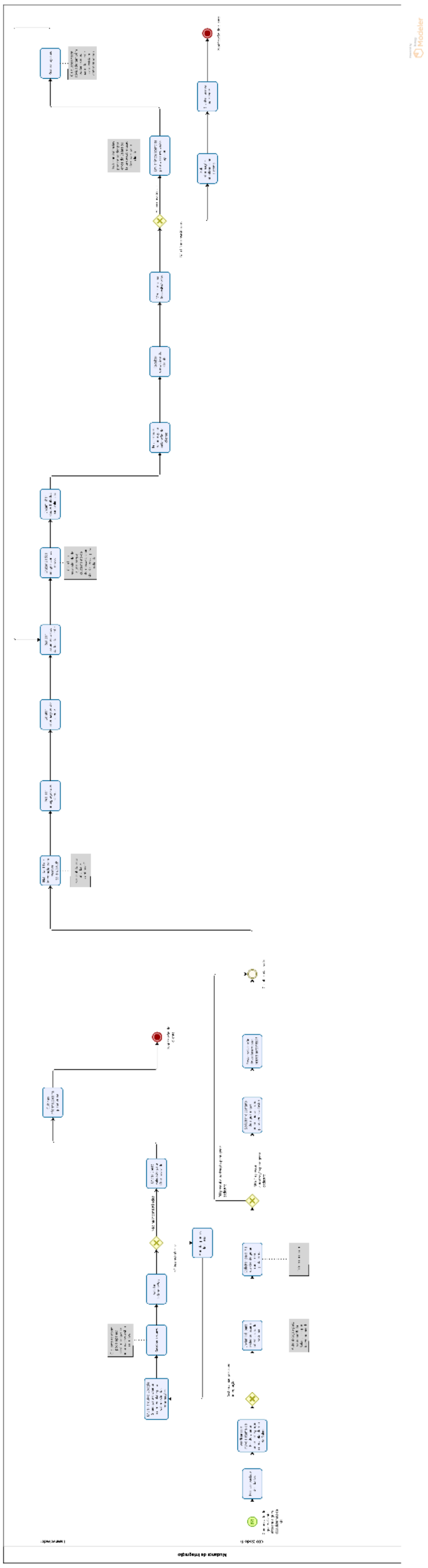
It is worth pointing out that the processes were documented in Portuguese, since this is a Brazilian company. The flowcharts of the mapped processes are presented below:

Figure 17- Onboarding of clients



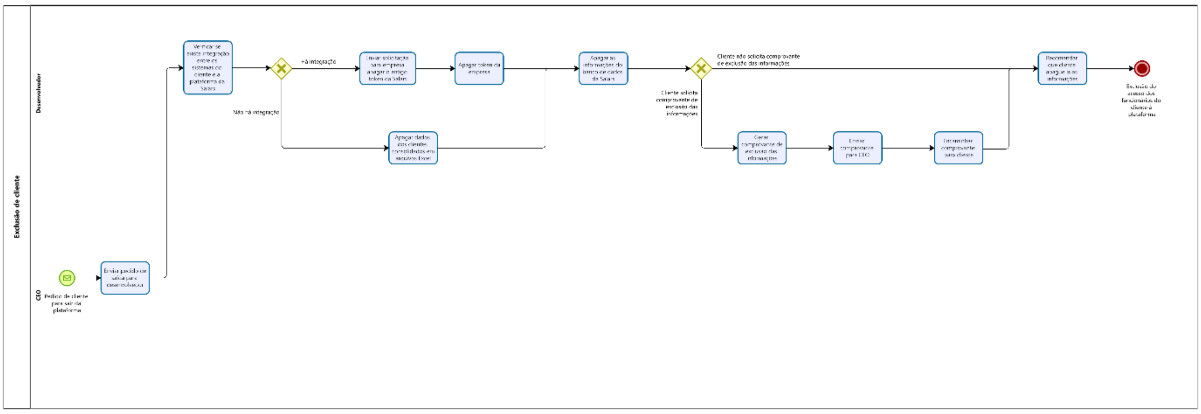
Source: author.

Figure 18- Clients' system update



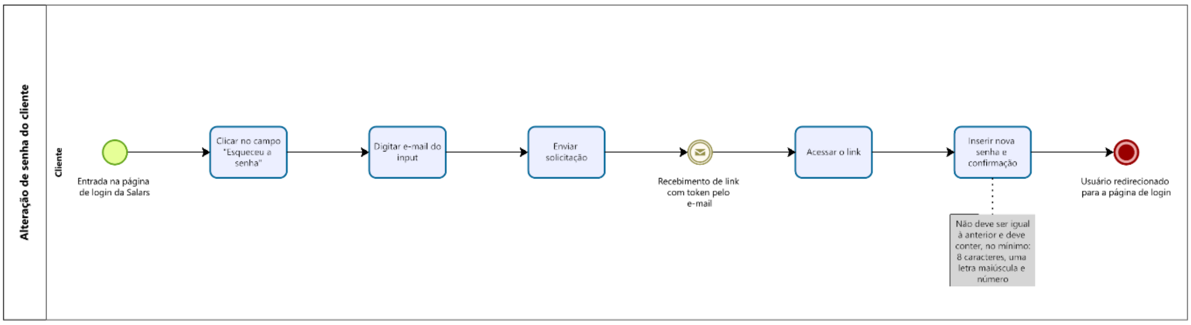
Source: author.

Figure 19 - Clients' exclusion


Exclusão de cliente
Desenvolvedor
CEO
Pedido de cliente para sair da plataforma
Enviar pedido de saída para desenvolvedor
Verificar se existe integração entre os sistemas do cliente e a plataforma da Salars
Há integração
Não há integração
Enviar solicitação para empresa apagar o antigo token da Salars
Apagar token da empresa
Apagar dados dos clientes consolidados em arquivos Excel
Apagar as informações do banco de dados da Salars
Cliente não solicita comprovante de exclusão das informações
Cliente solicita comprovante de exclusão das informações
Gerar comprovante de exclusão das informações
Enviar comprovante para CEO
Encaminhar comprovante para cliente
Recomendar que cliente apague suas informações
Exclusão do acesso dos funcionários do cliente à plataforma

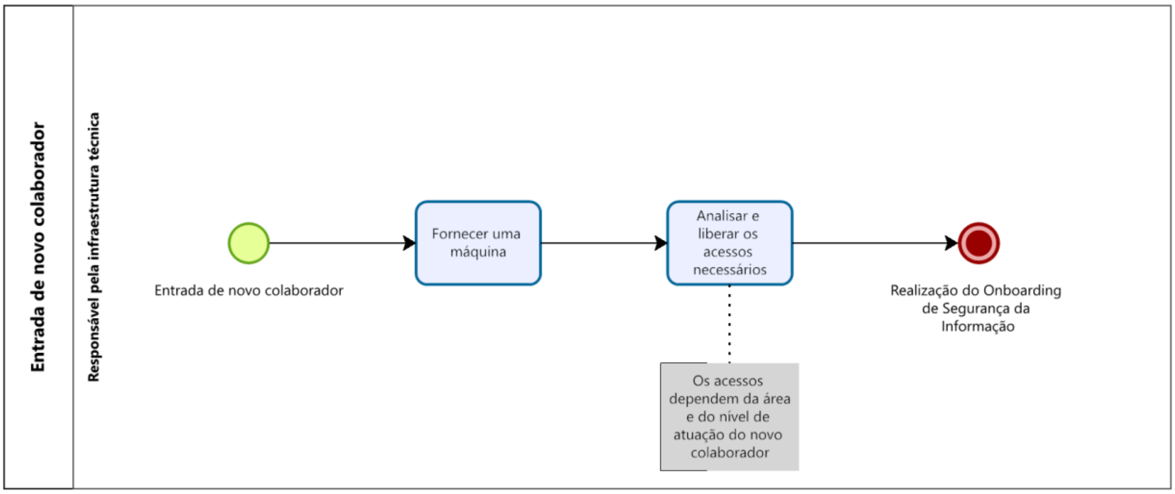
Source: author.

Figure 20 - Clients' password change


Alteração de senha do cliente
Cliente
Entrada na página de login da Salars
Clicar no campo "Esqueceu a senha"
Digitar e-mail do input
Enviar solicitação
Recebimento de link com token pelo e-mail
Acessar o link
Inserir nova senha e confirmação
Não deve ser igual à anterior e deve conter, no mínimo: 8 caracteres, uma letra maiúscula e número
Usuário redirecionado para a página de login

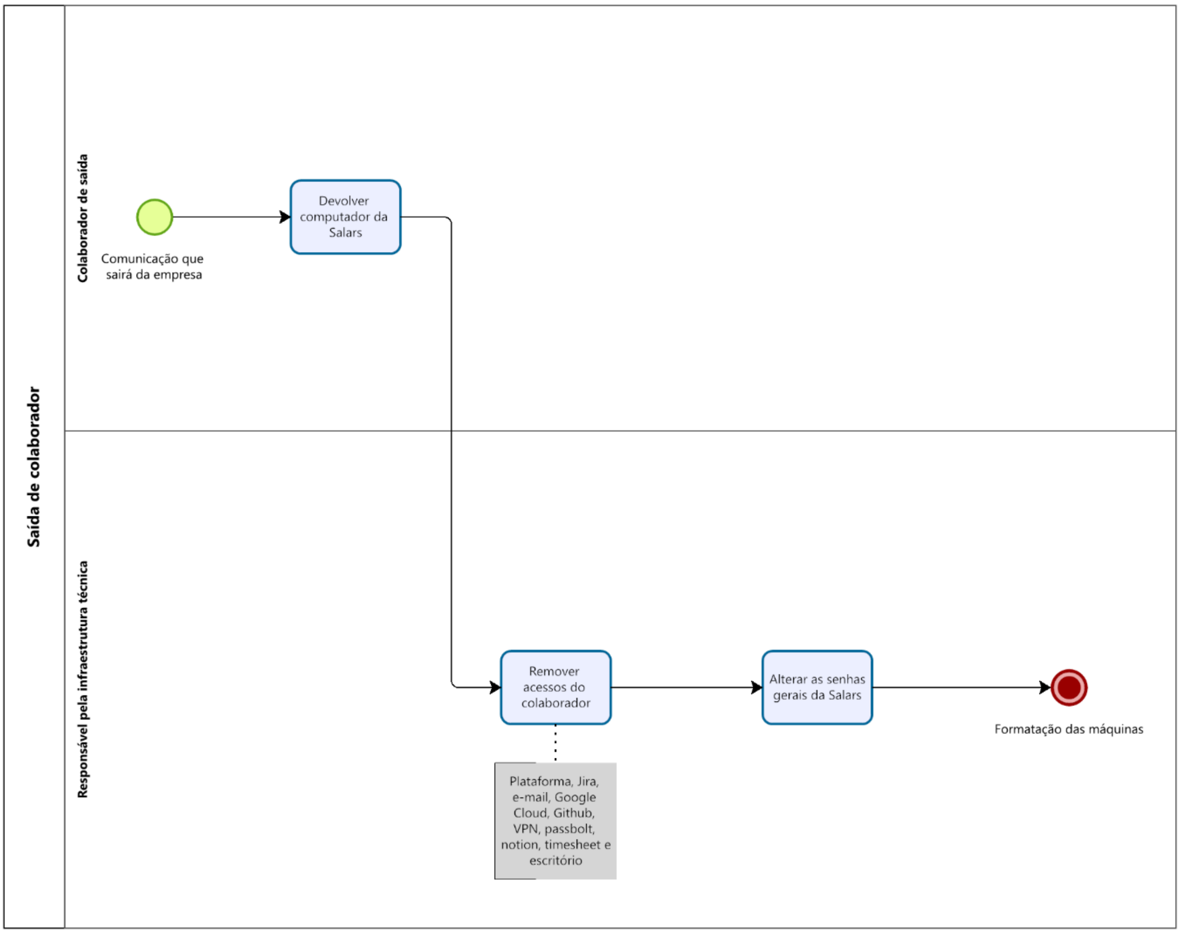
Source: author.

Figure 21- Entry of employees


Entrada de novo colaborador
Responsável pela infraestrutura técnica
Entrada de novo colaborador
Fornecer uma máquina
Analisar e liberar os acessos necessários
Os acessos dependem da área e do nível de atuação do novo colaborador
Realização do Onboarding de Segurança da Informação

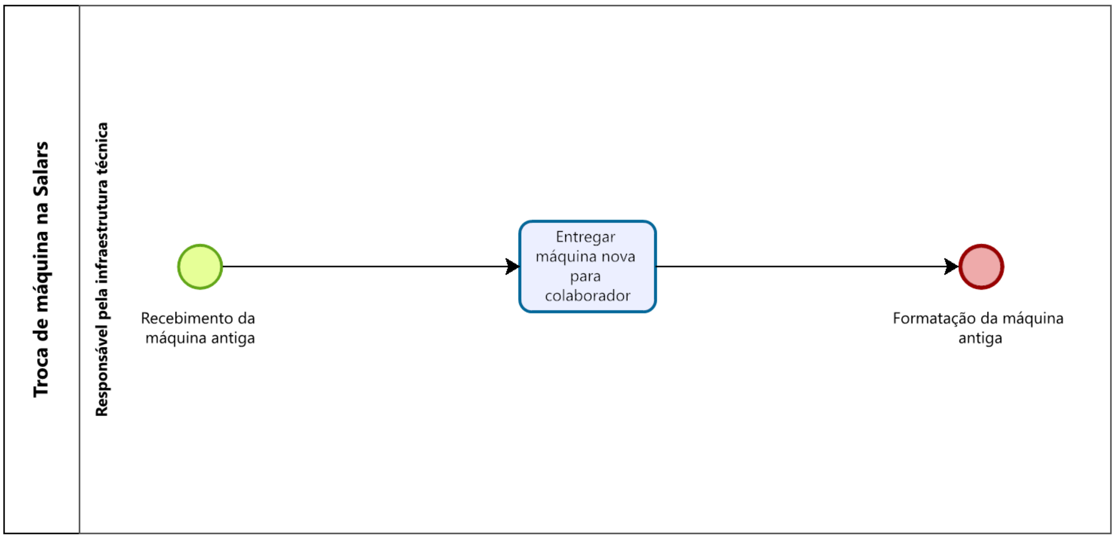
Source: author.

Figure 22- Departure of employees


Saída de colaborador
Colaborador de saída
Responsável pela infraestrutura técnica
Comunicação que sairá da empresa
Devolver computador da Salars
Remover acessos do colaborador
Plataforma, Jira, e-mail, Google Cloud, Github, VPN, passbolt, notion, timesheet e escritório
Alterar as senhas gerais da Salars
Formatação das máquinas

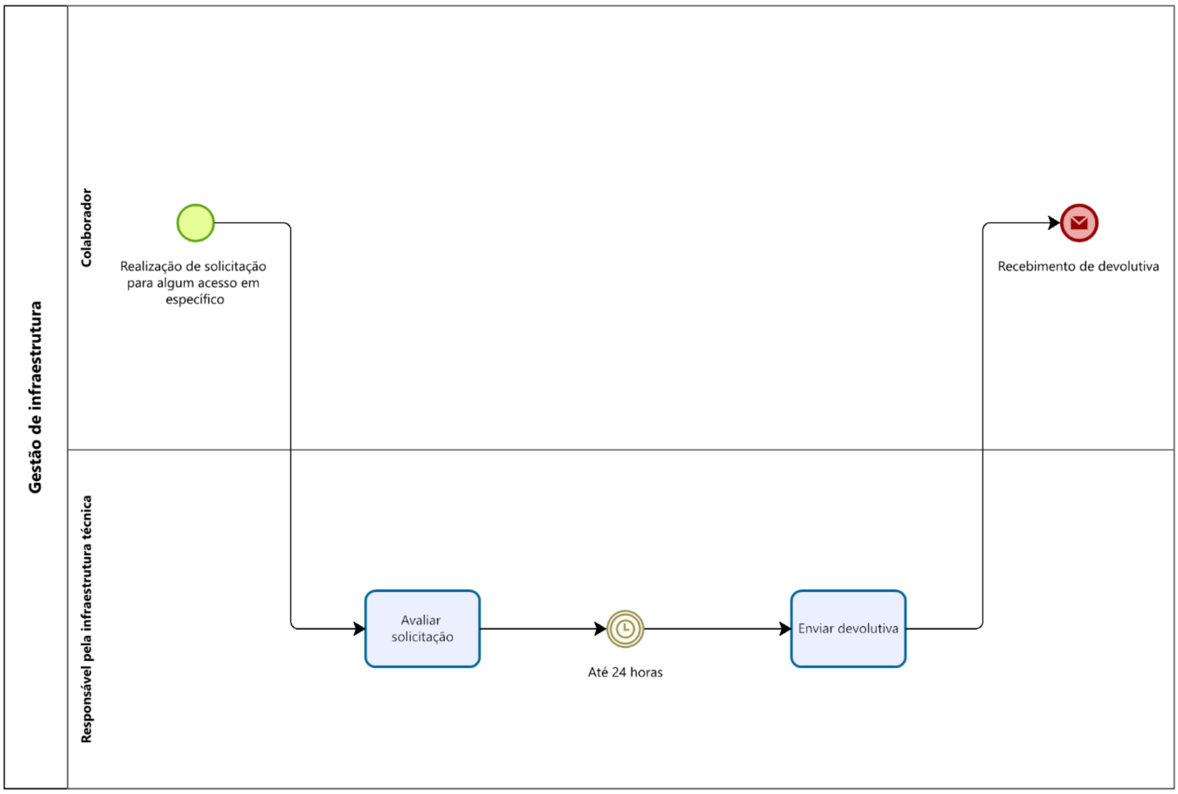
Source: author.

Figure 23 - Change of employees’ equipment


Troca de máquina na Salars
Responsável pela infraestrutura técnica
Recebimento da máquina antiga
Entregar máquina nova para colaborador
Formatação da máquina antiga

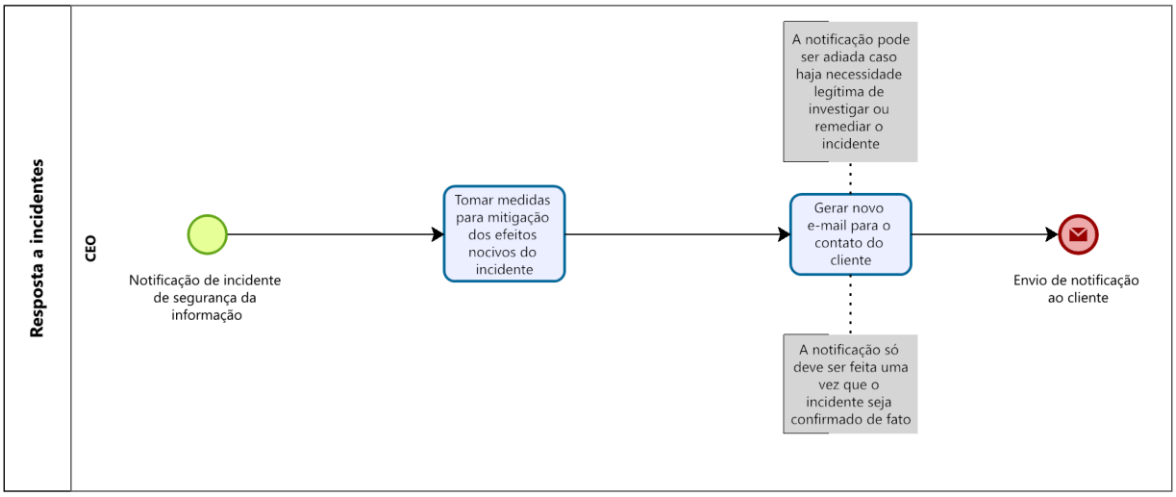
Source: author.

Figure 24 - Infrastructure management


Gestão de infraestrutura
Colaborador
Responsável pela infraestrutura técnica
Realização de solicitação para algum acesso em específico
Avaliar solicitação
Até 24 horas
Enviar devolutiva
Recebimento de devolutiva

Source: author.

Figure 25- Response to incidents


Resposta a incidentes
CEO
Notificação de incidente de segurança da informação
Tomar medidas para mitigação dos efeitos nocivos do incidente
A notificação pode ser adiada caso haja necessidade legítima de investigar ou remediar o incidente
Gerar novo e-mail para o contato do cliente
A notificação só deve ser feita uma vez que o incidente seja confirmado de fato
Envio de notificação ao cliente

Source: author.

6.3 ISMS'S PROCESSES DESIGN

The way by which the processes designed are described obey the following structure:

a) Which requirements of the standard NBR ISO/IEC 27001:2013 the designed process meets;
b) List of documents generated to manage the process;
c) Process objectives;
d) Period in which the process should be executed;
e) Process flowchart;
f) The process owner;
g) Inputs and outputs of the process;
h) Description;
i) Results achieved;
j) Results analysis;
k) Improvement topics; and
l) Process's validity and management.

6.3.1 Organization's Context

This process is intended to ensure the organization's compliance with the following requirements of the standard:

a) 4.1 – internal and external issues;
b) 4.2 – interested parties and their's necessities; and
c) 4.3 – ISMS's scope

For the process management, 4 documents were elaborated:

a) ContextoDaOrganizacao.bpm – Bizagi file in which the flowchart was developed;
b) ContextoDaOrganizacao.docx – Microsoft Word file describing the process;
c) ContextoDaOrganizacao.pdf – PDF file describing the process; and
d) ContextoDaOrganizacao.png – picture file showing the flowchart.

This process must satisfy 6 objectives:

a) Define/review the ISMS's scope;
b) Determine/review the aspects internal and external to the organization which affect its ability to achieve the defined ISMS objectives;
c) Determine/review who the stakeholders are as well as their needs in the context of information security;
d) Define/review the scope of the ISMS;

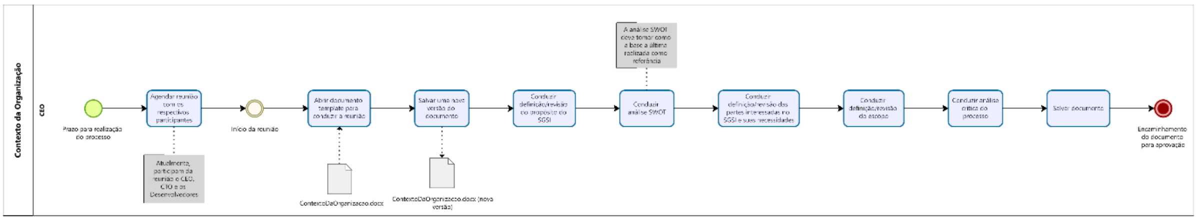
e) Ensure compliance of Salars Softwares e Soluções Ltd. with the NBR ISO/IEC27001: 2013 standard; and

f) Contribute to the continuous improvement of ISMS.

In terms of execution frequency, this process must be executed in the last 5 working days of each month. If the process cannot be executed within the stipulated period, a justification must be inserted in the respective field present on the document's cover ContextoDaOrganizacao.docx.

Figure 26 below shows the flow chart of the designed process:

Figure 26 - Organization's Context


Contexto da Organização
CEO
Prazo para realização do processo
Agendar reunião com os respectivos participantes
Atualmente, participam da reunião o CEO, CTO e os Desenvolvedores
Início da reunião
Abrir documento template para conduzir a reunião
ContextoDaOrganizacao.docx
Salvar uma nova versão do documento
ContextoDaOrganizacao.docx (nova versão)
Conduzir definição/revisão do propósito do SGSI
A análise SWOT deve tomar como a base a última realizada como referência
Conduzir análise SWOT
Conduzir definição/revisão das partes interessadas no SGSI e suas necessidades
Conduzir definição/revisão do escopo
Conduzir análise crítica do processo
Salvar documento
Encaminhamento do documento para aprovação

Source: author.

The owner of the process in question was defined as the CEO of Salars Softwares e Soluções Ltd.

Its inputs are:

a) Latest version of the ContextoDaOrganizacao.docx document.

Its outputs are:

a) New version of the ContextoDaOrganizacao.docx document.

The process is entirely conducted by the CEO of Salars Softwares e Soluções Ltd. and starts from the deadline set for its completion. Besides the CEO, the CTO and the Developer Team must also participate in the execution of this process.

The process begins from the moment the deadline for its realization arrives, when the scheduling of the Context of the Organization meeting must be done together with the other participants. In the meeting, the most recent version of the document ContextoDaOrganizacao.docx should be used as a basis for conducting and documenting the process.

With the document opened, it must be saved firstly in a new version to preserve the version history. Next, the team should review the purpose of the ISMS. If it no longer corresponds to what the team believes to be appropriate, they should update it with a justification.

After this, one must raise the issues internal and external to the organization that affect the ability of the ISMS to fulfill its defined purpose and achieve the expected results. To do so, a SWOT analysis of the ISMS context must be performed, as shown in **Table 11**. In this step, one must point out which are the internal factors (Strengths and Weaknesses) and external factors (Opportunities and Threats) that contribute or compromise the satisfaction of the ISMS purpose stipulated by the team. Thus, in the Dimension column of the table, it must be specified whether the point raised is a strength, weakness, opportunity or threat to the organization. In the Description column of the table, it must be described in a precise and intelligible way what the issue raised is about. In case of exclusion or change of one of the points of the SWOT Analysis, the change must be described and justified in the Controle de Versões field of the document ContextoDaOrganizacao.docx. In addition, the dimensions must remain grouped for better organization.

Once the survey of internal and external issues is concluded, the ISMS stakeholders and their respective needs translated into requirements must be reviewed. To do this, **Table 12** is used as a reference, which consists of two columns - Stakeholder and Requirements for the ISMS. For better organization and clarity, if the same stakeholder has more than one requirement, they should be separated by a paragraph. In case of exclusion or change of one of the points of the table, the team must describe and justify the change made in the Controle de Versões field of the document ContextoDaOrganizacao.docx.

Next, critically evaluating the previous steps, it is up to the team to review and, if deemed appropriate, update the scope of the ISMS.

With this, the process in question must undergo a critical evaluation by its participants, who must highlight possible points of improvement to be redesigned in the process aiming at its continuous improvement. The control and registration of such critical evaluations must also be included in a separate chapter of the document ContextOrganization.docx.

Finally, the team must save the newly generated document and forward it to the organization's CTO for approval. As for the old version, it must be stored together with the others for later consultation and preservation of the version history.

This ends the process.

In terms of the results generated, the purpose of the ISMS to be generated by the company was defined in a meeting with the partners as "to ensure the security and reliability of our products and services provided to our clients and to provide them with the assurance that we adequately manage information security risks". From this, a SWOT analysis was conducted, which produced the following results. These, as well as the upcoming tables and figures regarding the results from the processes executed, are shown in Portuguese:

Table 11 - SWOT Analysis

Dimensão	Descrição
S	Parceria com fundos de Venture Capital, o que traz ganhos de escala para obtenção de clientes. Além disso, consegue-se um know-how e calibração mais rápida do produto
S	Empresa fundada dentro da Taqtile, o que confere alto apoio em relação a desenvolvimento de estratégias e produtos, além de acesso a pessoas com ampla experiência no campo de aplicativos e desenvolvimento de softwares
S	Orientação e amplo apoio de investidores anjos estratégicos, dentre eles fundadores de unicórnios na LATAM e diretores de RH de grandes empresas. Isso confere maior know-how em RH e fácil acesso a possíveis novos investidores
S	Agilidade na tomada de decisões devido ao tamanho da empresa
S	Maior conhecimento de RH frente aos competidores
W	Pouco conhecimento prévio de assuntos de RH, o que sequestra parte do tempo da Alta Gestão que poderia ser usado para prospecção e leva a refinamentos da solução
W	Não adequação à Lei 13709/2018 (Lei Geral de Proteção de Dados)
W	Pouco conhecimento da jurídico geral para além da LGPD
W	Pouco conhecimento a respeito da ISO/IEC 27001 e como implementá-la adequadamente
W	Mão de obra limitada e altamente alocada
W	Foco momentâneo da Alta Gestão em geração de clientes e investimento para a Salars em detrimento de questões como segurança da informação
W	Ausência de um ISMS
W	Baixa orientação estratégica para Segurança da Informação, a qual não se encontra dentro de nenhum dos objetivos estratégicos

W	Cultura de *compliance* não consolidada
W	Dependência de investidores para autossustentação
W	Ausência de processos e regras formais documentados
W	Ausência de uma cultura de documentação
W	Baixa conscientização a respeito de segurança da informação
W	Não realização de uma auditoria interna para identificação de gaps organizacionais
W	Alta dependência dos fundadores devido à ausência de processos. O negócio não roda sem a atuação direta e constante dos fundadores
W	Plataforma não permite a integração e acesso a informações com parcela relevante dos softwares de RH disponíveis
O	Tendência global de startups com enfoque em remuneração, tanto nos EUA quanto na Europa
O	Já existe um unicórnio do ramo nos EUA, o que validaria parcialmente a solução de forma conceitual
O	Lei em andamento no Congresso Nacional que passaria a obrigar as empresas de antemão a divulgar a faixa salarial em vagas de emprego
O	Gap para maior entendimento do mercado e geração de novas soluções/aprimoramento das atuais por se tratar de um mercado ainda muito pouco explorado especialmente no Brasil e América Latina
T	Novos concorrentes locais com muito mais capitalização
T	Concorrentes internacionais já consolidados que podem passar a operar no Brasil. Pave (unicórnio dos EUA) está se expandindo para a Europa, o que pode indicar futuras movimentações
T	Alterações repentinas no texto da LGDP (insegurança jurídica e política)
T	Risco de se manchar a imagem frente ao mercado e stakeholders relevantes em caso de falha grave de gestão de segurança da informação

Source: author;

Observing the table, it draws attention the fact that there is no knowledge about the legislation within the organization, which may indicate the existence of a significant amount of non-compliance of the product and the company with the requirements of the law, especially

Law 13709/2018 (LGPD). This brings serious legal and reputational risks to the company especially in case there is a legal action against itself alleging such deficiencies. Moreover, it is noted the high allocation of manpower coupled with the absence of a culture of compliance, information security and documentation, factors that pose challenges to the implementation of an ISMS that fully meets the standard.

Once the SWOT analysis was done, a mapping of the ISMS stakeholders and theirs' requirements was performed, which can be found in **Table 12** below:

Table 12 - Interest parties and their's requirements

Parte interessada	Requisitos para com o ISMS
Clientes atuais	Proteção de informações sensíveis referente à folha de pagamento como: gasto por cargo e total; divisão e distribuição de cargos; plano de carreira; divisão homens/mulheres por hierarquia; divisão de salário entre homens e mulheres. Ter a garantia de que o ISMS está em aderência com a Lei 13709/2018 (LGPD). Ter a garantia de que o ISMS esteja certificado de acordo com a norma ISO/IEC 27001: 2013. Ter a garantia de que os dados e informações de seus funcionários não estejam sob risco de exposição e vazamento. Ter a garantia de possuir livre e facilitado acesso aos dados fornecidos que são utilizados pelo software. Ter a garantia de possuir um acesso exato, claro e transparente de seus dados fornecidos a qualquer momento que assim o desejar
Potenciais clientes	Idem cliente com a adição de que alguns exigem um ISMS certificado
Fundos de VCs	Evitar uma possível mancha em sua reputação com eventual vazamento de dados

Funcionários dos clientes	Ter a proteção individual de seus dados e garantia de privacidade. Ter a garantia de que o ISMS está em aderência com a Lei 13709/2018 (LGPD).
Familiares dos funcionários	Ter a proteção individual de seus dados e garantia de privacidade
Governo (Agência Nacional de Proteção de Dados)	Garantir aderência com a Lei 13709/2018 (LGPD), recolhimento de impostos (trabalhistas, renda)
Mão de obra da Salars	Possuir os treinamentos e capacitações apropriados para a operação do ISMS. Executar os processos do ISMS e a política de informação tal qual foram desenhados/planejados. Ter a garantia de que seus dados e informações pessoais estejam devidamente protegidos.
Alta gestão da Salars	Ter a garantia de que o ISMS cumpra com os seus objetivos. Ter garantia de que os objetivos de negócio não sejam comprometidos por ocorrências de segurança do ISMS. Participar e liderar ativamente a implementação do ISMS, comunicação da política de segurança da informação, atribuição de papéis e responsabilidades e prover os recursos necessários para implementação e operação do ISMS. Gerenciar o ISMS e operá-lo tal qual foi desenhado e planejado.
Salars	Garantir que o acesso e uso dos dados dos clientes estejam devidamente amparados na Lei 13709/2018 e claramente explicitados nos contratos com o devido consentimento de uso. Tal

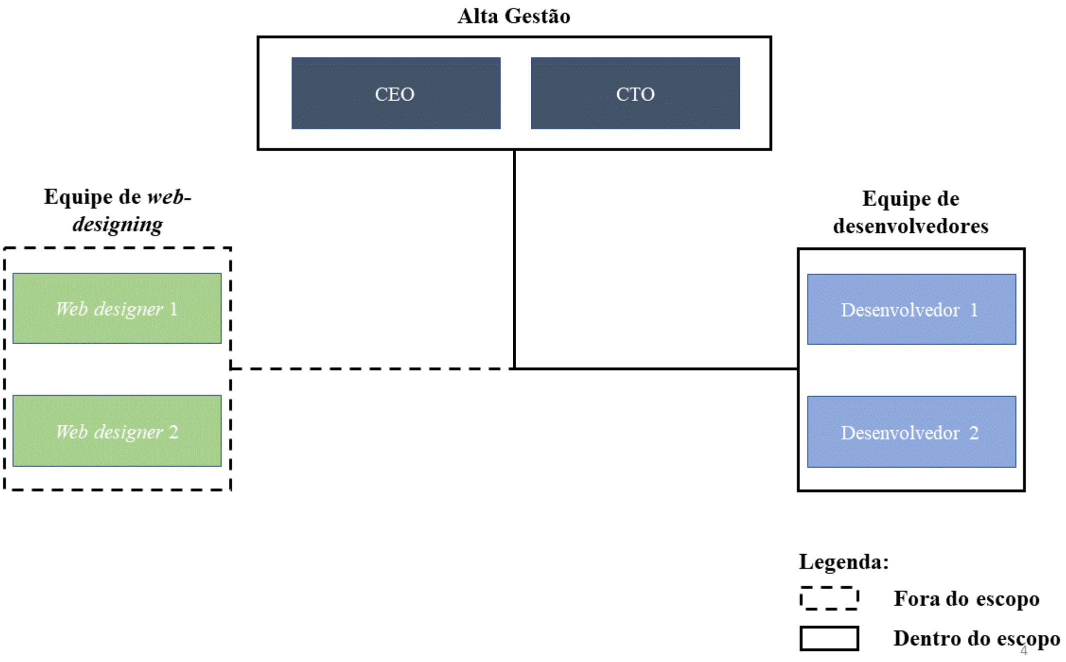
	consentimento deve se dar não apenas pela empresa contratante, mas de seus funcionários

Source: author.

Once again, there is a high probability that there are no functionalities in the developed product that meet the requirements of the LGPD. However, it is also necessary, as the next step of this project, to specify which are the requirements of the law in question (as well as others that may exist related to information security) and translate them into requirements to be implemented. For each requirement ought to be satisfied, a person responsible for its implementation will be defined as well as its deadline, work plan, resources needed, a person responsible for its approval as well as a routine for its monitoring and possible adjustments to be made.

Subsequently, the scope of the ISMS was defined as applicable to the processes outlined in 6.2 of this document and comprised of the following organizational chart:

Figure 27 - Organizational perspective over the ISMS's scope



Source: author

For the critical analysis of the process, Table 13 below must be filled with the opportunities for improvement identified in this process as well as the proposed redesign. Besides this, the date in which the opportunity for improvement was pointed out must be inserted. As the process has not yet been autonomously executed by the company, there are no opportunities mapped at the moment. Furthermore, it is important to point out that the next processes also count with this step and use a table with the same structure as the one presented below, in way it was not considered necessary to show it repeatedly in this final paper.

Table 13 - Process's critical evaluation

Data (dd/mm/aaaa)	Oportunidade de melhoria identificada	Redesenho proposto

Source: author.

Finally, it was stipulated that the process will formally take effect in the organization in January 2023. The person responsible for its approval is the company's CTO (Partner 2), who must sign the Microsoft Word document referring to this process, authorizing the execution of its latest version.

6.3.2 ISMS's Risks and Opportunities

This process is intended to ensure the organization's compliance with the following requirements of the standard:

a) 6.1.1 - ISMS's general risks and opportunities.

For its management, 5 documents were elaborated:

a) RiscosOportunidadesSGSI.bpm – Bizagi file in which the flowchart was developed;
b) RiscosOportunidadesSGSI.docx – Microsoft Word file describing the process;
c) RiscosOportunidadesSGSI.pdf – PDF file describing the process;
d) RiscosOportunidadesSGSI.png – picture file showing the flowchart; and
e) RiscosOportunidadesSGSI.xlsx - file to conduct and carry out the process.

This process must satisfy 6 objectives:

a) Identify eventual risks that could compromise the proper functioning of the ISMS operation and the achievement of its objectives;

b) Identify eventual opportunities that the ISMS and its full operation bring to the organization, whether in financial terms, image promotion, among others;

c) Manage the risks raised in order to reduce them;

d) Manage the opportunities raised in order to enhance and promote them;

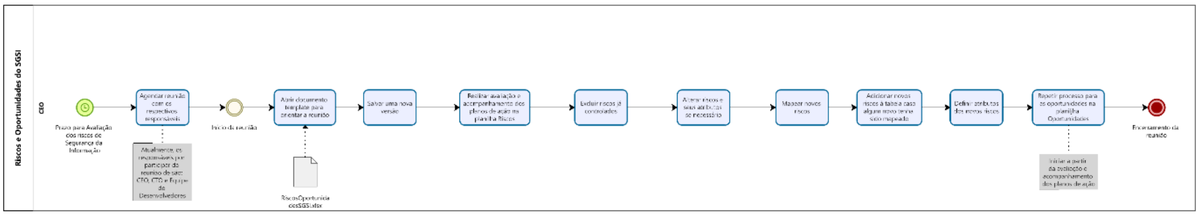
e) Ensure compliance of Salars Softwares e Soluções Ltd. with the NBR ISO/IEC27001: 2013; and

f) Contribute to the continuous improvement of the ISMS.

In terms of execution frequency, this process must be executed in the last 7 working days of each month. If the process cannot be executed within the stipulated period, a justification must be inserted in the respective field present on the document's cover RiscosOportunidadesSGSI.docx..

Figure 28 below shows the flow chart of the designed process:

Figure 28 - ISMS’s Risks and Opportunities


Riscos e Oportunidades do SGSI
CEO
Prazo para Avaliação dos riscos de Segurança da Informação
Agendar reunião com os respectivos responsáveis
Atualmente, os responsáveis por participar da reunião de são: CEO, CTO e Equipe de Desenvolvedores
Início da reunião
Abrir documento template para orientar a reunião
RiscosOportunidadesSGSI.xlsx
Salvar uma nova versão
Realizar avaliação e acompanhamento dos planos de ação na planilha Riscos
Excluir riscos já controlados
Alterar riscos e seus atributos se necessário
Mapear novos riscos
Adicionar novos riscos à tabela caso algum novo tenha sido mapeado
Definir atributos dos novos riscos
Repetir processo para as oportunidades na planilha Oportunidades
Iniciar a partir da avaliação e acompanhamento dos planos de ação
Encerramento da reunião

Source: author.

The owner of the process in question was defined as the CEO of Salars Softwares e Soluções Ltd.

Its inputs are:

a) Most recent version of the RiscosOportunidadesSGSI.xlsx document.

Its outputs are:

a) Newer version of the RiscosOportunidadesSGSI.xlsx document.

The process is entirely driven by the CEO of Salars Softwares e Soluções Ltd. The CTO and the Developer Team must also participate in its execution.

The process starts from the deadline stipulated. With that, the CEO must schedule a meeting with the CTO and the Developer Team to conduct a survey, analysis and evaluation of risks and opportunities - as well as their respective action plans - relative to the ISMS's ability to meet its purpose.

Once the meeting starts, the CEO should use as a basis for conducting the risk assessment the document RisksOpportunitiesSGSI.xlsx in its latest version and save a new version for editing while preserving the history of previous versions. The file consists of two worksheets (Risks and Opportunities), each containing tables with the same structure for managing risks and opportunities. The tables are structured around the following columns:

a) ID: number to identify the risk/opportunity;

b) Risk/Opportunity: detailed and intelligible description of the risk/opportunity in question;

c) Action: action plan for the risk/opportunity described in a detailed and intelligible manner. The field must be structured in a way to break down the action plan into its macro activities, which must be separated by paragraphs and numbered sequentially (to generate a paragraph inside a cell in Excel, use Alt + Enter in Windows);

d) Resources needed: the resources needed to implement the action plan must be determined. This field must follow the same organization logic of the Action column;

e) Deadline: deadline for implementing the action plan;

f) Evaluation of results: in this field the team must describe how the action plan and its follow-up will be evaluated, and who will be responsible for it;

g) Comments: field to be filled in by the person responsible for the approval of the risk/opportunity. The way to fill it out will be detailed below; and

h) Status: status of implementation of the action plan (Not started, In progress, Completed).

After that, the team must open the Risks spreadsheet from the file and perform a follow-up and evaluation of the action plans defined for each risk. The objective of this activity is to verify if the action plans stipulated in the last execution of this process are reaching the expected results (or heading towards it). If this is not the case, the action plan and its respective attributes must be reviewed and, if necessary, changed in order to meet the deadline and achieve the results. In this case, it is up to the person responsible for evaluating the results of the action plan to determine, together with the person responsible for the action plan, the causes of such nonconformity and what measures will be taken for a course correction, registering such points in the Comments column.

Next, risks that are no longer a threat to the achievement of ISMS objectives (either through successful implementation of action plans or other factors) in the judgment of the person responsible for their assessment should have their Status field updated to Completed. However, despite this status, the risk should not be deleted from the table, but should be monitored up by the person responsible for its assessment at an appropriate frequency - at least once between successive runs of this process.

After that, the other risks should be reviewed and their attributes changed if deemed necessary by the meeting participants and if the approver agrees with the change in question. If this occurs, the approver must register the change made in the Comments column.

The team must then insert any new risks mapped by the participants and define their attributes.

With this, the fraction of the process referring to risks is concluded and the one referring to opportunities begins. Thus, the team must access the Opportunities spreadsheet from the file and carry out the same sequence of activities described above from the action plans' monitoring and evaluation step.

Finally, the process in question should go through a critical evaluation by its participants, who should highlight possible improvement points to be redesigned in the process aiming its continuous improvement. The control and registration of such evaluations are done in a table like **Table 13** of this document.

After this, the newly generated document must be saved and forwarded to the organization's CTO for approval. As for the old version, it must be stored with the others for later consultation and preservation of the version history, and the process ends.

Finally, it was stipulated that the process will formally take effect in the organization in January 2023. The person responsible for its approval is the company's CTO, who must sign the Microsoft Word document referring to this process, authorizing the execution of its latest version.

In a first execution of this process, 7 risks for ISMS were raised and their respective action plans stipulated as presented in **Table 14**.

Table 14 - ISMS’s Risks

ID	Risco	Responsável	Ação	Recursos necessários	Prazo	Avaliação de resultados	Comentários	Status
1	O SGSI não é operacionallizado apropriadamente, pois os processos não são seguidos tal como definidos	Olavo + CEO	1. Desenhar os processos de forma clara, precisa, inteligível e sem gerar ambiguidades. Isso pode ser feito gerando-se uma documentação padrão para todos os processos a serem desenhados, os quais seguirão a mesma estrutura 2. Revisar os processos desenhados e sua estrutura com os executores e mapear pontos de ambiguidade ou inadequação. Corrgir tais pontos e validá-los 3. Estipular prazos de revisão e análise crítica com frequência maior no início para eventuais ajustes 4. Tornar fácil o acesso à documentação dos processos desenhados de modo a permitir seu acesso aos seus usuários para consulta e organizá-los de forma lógica 5. Estipular processo de treinamento para novos funcionários	1. Tempo dos envolvidos no processo	16/11/2022	CEO e CTO avaliam e aprovam estrutura padrão dos processos a serem desenhados		Em andamento
2	Pouca adequação do SGSI à legislação aplicável devido ao baixo conhecimento da Alta Gestão sobre o tema	CTO	1. Mapear a legislação aplicável ao contexto da Salars 2. Priorizar as leis mais críticas 3. Avaliar se a organização possui a capacidade necessária para traduzir e implementar as exigências da legislação em requisitos do SGSI 4. (OPCIONAL) Contratar especialistas externos para auxiliar no plano de ação risco caso se julgue necessário	1. Tempo dos envolvidos no processo 2. Aporte financeiro caso se necessite de uma consultoria externa sobre o tema	20/12/2022	Um consultor externo e com experiência e qualificação no tema valida se os requisitos foram traduzidos de forma adequada		Não iniciado
3	SGSI mal desenhado de modo a tomar excessivamente o tempo da Alta Gestão dos processos de negócio	Olavo + CEO	1. Desenhar os processos de forma clara, precisa, inteligível e sem gerar ambiguidades. Isso pode ser feito gerando-se uma documentação padrão para todos os processos a serem desenhados 2. Validar de forma frequente a estrutura, conteúdo e frequência estipulada para execução do processo com o CEO para garantir alinhamento ao contexto da organização e conferir a agilidade requerida	1. Tempo dos envolvidos no processo	22/12/2022	CEO e CTO avaliam criticamente a fluidez e adequação dos processos frente às outras demandas, ajustando o SGSI conforme necessário		Em andamento
4	SGSI altamente dependente da Alta Gestão para operar de forma apropriada	Olavo + CEO	Apesar de ser um risco válido, por se tratar de uma empresa com pouco mais de 1 ano de existência e contar com apenas 4 funcionários efetivamente, os processos (incluindo o SGSI) demandarão uma participação mais assertiva e frequente da Alta Gestão no curto e médio prazo	1. Tempo dos envolvidos no processo	N/A	N/A		Concluído
5	Baixo conhecimento interno sobre como auditar o sistema tendo a Norma como referência de modo a produzir resultados pouco confiáveis e pouco precisos	Olavo	1. Mapear os requisitos exigidos pela Norma para auditoria do SGSI 2. Averiguar se a organização satisfaz ou pode satisfazer no curto prazo tais requisitos 3. Caso se confirme a capacidade organizacional, desenhar o processo de auditoria interna com eventuais auxílios externos tendo em vista a garantia com a conformidade 4. Caso não se confirme a capacidade organizacional, contratar uma auditoria externa (neste caso, a responsabilidade passa a ser do CTO)	1. Tempo dos envolvidos no processo	10/12/2022	Um consultor externo e com experiência e qualificação no tema valida se o eventual processo de auditoria interna a ser realizado pela própria organização segue os requisitos da Norma principalmente no que diz respeito à imparcialidade e objetividade das avaliações		Em andamento
6	Poucos recursos para operacionalizar o SGSI e melhorá-lo continuamente	CEO	1. Desenho de processo/rotina voltado para mapeamento e análise recorrente de eventuais demandas por recursos para que o SGSI funcione adequadamente. Tal rotina deverá possuir uma maior frequência no início para haver uma atuação mais rápida e direta por parte da Alta Gestão	1. Tempo dos envolvidos no processo	07/12/2022	CTO		Em andamento
7	Inadequação do SGSI frente a novos produtos, processos, estrutura e outras mudanças pelas quais a organização poderá passar	CEO	1. Desenho de processo/rotina para mapeamento e análise de eventuais mudanças no contexto da organização tendo em vista o SGSI. Tal processo deverá ser executado com maior frequência no curto prazo tendo em vista a volatilidade do contexto no qual a organização está inserida	1. Tempo dos envolvidos no processo	24/11/2022	CTO		Concluído

Source: author.

It can be stated that two of the risks identified are already controlled through the design of processes or other factors. As for risk 4, although the ISMS is not designed to work exclusively under the dependence of the company's top management, it is expected that its implementation and operation will require a more assertive and present participation of the partners, especially at this early stage of the company's trajectory, when manpower and resources are quite scarce. For Risk 7, the Organization's Context process would contribute to the management of this risk once the SWOT Analysis contemplates the issues addressed in the risk and its frequency was purposely increased to be done at least once a month considering the volatile context in which the organization finds itself today.

Besides the risks, 5 opportunities that demand action in order to generate satisfactory results for the organization were identified in **Table 15**.

Table 15 - ISMS's Opportunities

ID	Oportunidade	Responsável	Ação	Recursos necessários	Prazo	Avaliação de resultados	Comentários	Status
1	Geração de receita imediata devido à captura de clientes céticos com a certificação	CEO + Desenvolvedores	1. Uma vez que o SGSI esteja plenamente desenhado e estruturado, ainda que não operando, comunicar tais clientes sobre a implementação com a possibilidade de mostrar os processos e os avanços realizados - CEO 2. Na página oficial e redes sociais da organização, inserir um cronograma de progresso na implementação da Norma dando transparência ao processo - Densenvolvedores	1. Tempo	mar/23	Medição e acompanhemento da taxa de captação de clientes céticos antes e depois da medida ser concluída pelo CTO		Não iniciado
2	Melhor aceitação e confiança do mercado com a organização destravando a obtenção contínua de novos clientes	CEO	1. Promoção de estratégia de marketing para extrair o maior valor comercial possível com a obtenção da Norma	1. Tempo 2. Aporte financeiro caso se terceirize a estratégia de marketing	jan/23	Medição e acompanhemento da taxa de captação de novos clientes céticos antes e depois da medida ser concluída pelo CTO		Não iniciado
3	Redução dos danos caso a Salars seja processada	N/A	N/A	N/A	N/A	N/A		Não iniciado
4	Diminuição da probabilidade de a organização ser processada devido à segurança e privacidade da informação	N/A	N/A	N/A	N/A	N/A		Não iniciado
5	Melhorar a reputação da empresa como segura e responsável frente aos demais stakeholders além dos clientes facilitando possivelmente a captação de mais recursos	CEO + Desenvolvedores	1. Enviar comunicado oficial a respeito do processo de implementação do SGSI além de quando a organização obter a certificação - CEO 2. Promoção de estratégia de marketing para extrair o maior valor comercial possível com a obtenção da Norma - CEO 3. Na página oficial e redes sociais da organização, inserir um cronograma de progresso na implementação da Norma dando transparência ao processo - Densenvolvedores	1. Tempo 2. Aporte financeiro caso se terceirize a estratégia de marketing	jan/23	Verificação de uma maior facilidade em negociações e maior surgimento de possíveis novos investidores e parceiros. Além disso, verificação de menores queixas e reclamações por parte dos clientes devido à falta de um SGSI e de uma certificação com a Norma - CTO		Não iniciado

Source: author

It can be seen that no action plan was initiated in this case and two of them were not described either. This is because these issues are not considered to be a priority at the present time of this project since they all depend on a actually implemented ISMS to manifest themselves. Thus, it was stipulated that the action plans will be designed and their implementation will begin in early 2023, when it is expected that the entire ISMS will be designed and determined, leaving only its execution and occasional adjustments.

6.3.3 Information Security Risks Mapping and Evaluation

This process is intended to ensure the organization's compliance with the following requirements of the standard:

a) Clause 6.1.2 – Information security risks evaluation.

For the process management, 5 documents were elaborated:

a) AvaliacaoDeRiscos.bpm – Bizagi file in which the flowchart was developed;
b) AvaliacaoDeRiscos.docx – Microsoft Word file describing the process;
c) AvaliacaoDeRiscos.pdf – PDF file describing the process;
d) AvaliacaoDeRiscos.png – image file of the generated flowchart; and
e) RiscosSegurancaDaInformacao.xlsx – file to conduct and carry out the process.

This process must satisfy 10 objectives:

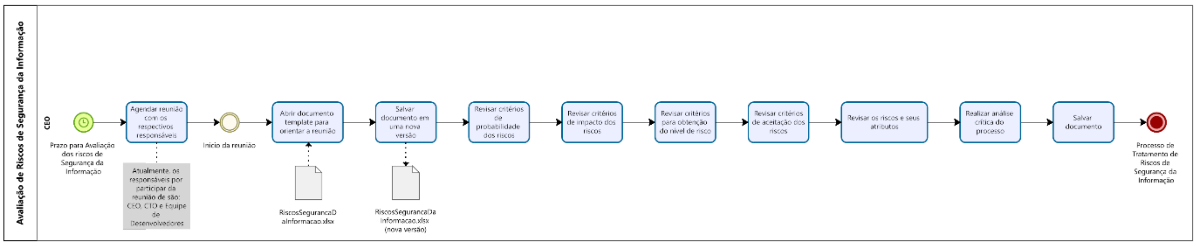
a) Ensure that information security risk assessments are done in a standardized manner allowing for comparable results over time;
b) Ensure compliance of Salars Softwares e Soluções Ltd. with the NBR ISO/IEC27001: 2013 standard;
c) Establish/review the information security risk probability criteria;
d) Establish/review the information security risk impact criteria;
e) Establish/review the risk level criteria for information security risks;
f) Establish/review the information security risk acceptance criteria;
g) Establish/review the information security risks and their respective attributes;
h) Establish/review those responsible within Salars Softwares e Soluções Ltd. for managing each risk;
i) Establish/review the priority levels associated with each information security risk; and

j) Contribute to the continuous improvement of ISMS.

In terms of execution frequency, this process must be executed in the last 7 working days of each month. If the process cannot be executed within the stipulated period, a justification must be inserted in the respective field present on the front cover of the document AvaliacaoDeRiscos.docx.

Figure 29 below shows the flow chart of the designed process:

Figure 29 - Information Security Risks Mapping and Evaluation


Avaliação de Riscos de Segurança da Informação
CEO
Prazo para Avaliação dos riscos de Segurança da Informação
Agendar reunião com os respectivos responsáveis
Atualmente, os responsáveis por participar da reunião de são: CEO, CTO e Equipe de Desenvolvedores
Início da reunião
Abrir documento template para orientar a reunião
RiscosSegurancaDaInformacao.xlsx
Salvar documento em uma nova versão
RiscosSegurancaDaInformacao.xlsx (nova versão)
Revisar critérios de probabilidade dos riscos
Revisar critérios de impacto dos riscos
Revisar critérios para obtenção do nível de risco
Revisar critérios de aceitação dos riscos
Revisar os riscos e seus atributos
Realizar análise crítica do processo
Salvar documento
Processo de Tratamento de Riscos de Segurança da Informação

Source: author.

The owner of the process in question was defined as the CEO of Salars Softwares e Soluções Ltd.

Its inputs are:

a) Most recent version of the RiscosSegurancaDaInformacao.xlsx document.

Its outputs are:

a) Newer version of the RiscosSegurancaDaInformacao.xlsx document.

The process is entirely conducted by the CEO of Salars Softwares e Soluções Ltd. and starts from the stipulated deadline for conducting a new Information Security Risk Assessment considering the present ISMS scope. Besides the CEO, the CTO and the Developers Team must also participate in the execution of this process.

Once the meeting starts, the CEO should use as a basis for conducting the risk assessment the document RiscosSegurancaDaInformacao.xlsx in its most recent version. The file should then be saved in a new version for editing while preserving the history of previous versions.

Firstly, the probability criteria for the occurrence of information security risks must be reviewed considering the current context of the processes determined in the ISMS scope. These criteria are found on the Probability sheet in the file. Currently, the probability attribution criteria are configured as follows:

Table 16 - Probability criteria for information security risks

Probabilidade	Nota	Descrição
Muito baixa	1	Menos de uma vez por ano
Baixa	2	1 vez por ano
Média	3	Entre 2 e 6 vezes por ano
Alta	4	Entre 7 e 11 vezes por ano
Muito alta	5	1 vez por mês ou mais

Source: author.

After this, the impact criteria of the information security risks must be reviewed considering the current context of the processes determined in the ISMS scope. These criteria are found in the Impact sheet of the file. Currently, the probability attribution criteria are configured as follows:

Table 17 - Impact criteria for information security risks

Impacto	Nota	Descrição
Muito baixo	1	Incidente pontual que não afeta de forma significativa o cliente e sem implicações legais à organização. Não há prejuízo na credibilidade e imagem da organização perante os demais stakeholders
Baixo	2	Incidente que pode trazer uma insatisfação pontual por parte do cliente, porém sem implicações legais à organização. A credibilidade e imagem da organização perante os demais stakeholders é rapidamente recuperada
Médio	3	Incidente que pode trazer uma insatisfação generalizada por parte de um cliente, possivelmente levando-o a encerrar seu contrato com a organização, porém sem implicações legais à organização. A credibilidade e imagem da organização perante os demais stakeholders é afetada de forma pouco significativa, e recuperável no curto prazo
Alto	4	Incidente que provavelmente levará ao encerramento do contrato do cliente com a organização possivelmente gerando insatisfação dos demais clientes, trazendo inclusive implicações legais não graves. A credibilidade e imagem da organização é afetada de forma significativa, dificultando a obtenção de novos clientes, investidores e recursos. A recuperação da credibilidade se daria apenas no médio prazo

Muito alto	5	Grave incidente que provavelmente levará com que o cliente em questão, assim como outros, optem por encerrar o contrato com a organização, trazendo também graves implicações legais. A credibilidade e imagem da organização é criticamente afetada perante os demais stakeholders, tornando praticamente inviável a obtenção de novos clientes, investidores e recursos no médio prazo. Além disso, é possível que haja uma fuga de capitais da empresa. A recuperação da empresa só seria possível no longo prazo

Source: author.

Subsequently, the acceptance criteria for the information security risk levels must be reviewed, which is obtained by the product between the risk's probability and impact. These criteria can be found in the Acceptance Criteria spreadsheet in the file. The risk levels deemed unacceptable by the organization should be duly highlighted (red was used for this). Currently, the information security risk acceptance criteria are configured as follows:

Table 18 - Information security risk acceptance criteria

Impact Probability	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Source: author

After that, in the Risks spreadsheet of the file, each risk and their respective attributes must be reviewed and, if necessary, new risks must be added with their respective attributes duly determined considering the current context of the processes determined in the ISMS scope. The attributes of a risk are:

a) ID: number for risk identification;

b) Process: process by which the risk manifests itself;

c) The risk category. Currently, the categories defined are Confidentiality, Availability, and Integrity;

d) Risk description: field to describe in a detailed and intelligible way how the risk arises, manifests itself and what its possible consequences are;

e) The type of information involved with the risk in question. Currently, the types of information defined are Customer Information, and Customer Employee Information;

f) Causes: field to determine the root causes of the risk in question. Aiming to provide clarity and organization, this field must be structured in a way to separate the different causes in sequentially numbered paragraphs (to generate a paragraph within a cell in Excel, use Alt + Enter in Windows);

g) The probability, impact and risk level;

h) Acceptance criteria: field in which it is defined whether the risk in question is at an acceptable or rejectable level;

i) Responsible: the one responsible for implementing the action plan within the organization;

j) The Priority 1 field, in which the team defines the first priority level of risks to be treated. The priority levels should be determined according to the following logic:

1. 1: high priority;
2. 2: medium priority; and
3. 3: low priority.

k) The Priority 2 field, in which the second priority level of risks to be treated within the group defined in the Priority 1 field is defined. The priority levels in this case must be defined in increasing sequential order with 1 being for the highest priority risk within the group. In addition, within the same group, there cannot be risks with the same priority level;

l) Strategy: field in which team defines which of 4 possible risk treatment strategies will be used. The possible strategies are:

1. Accept: strategy in which the risk level does not represent a significant threat to the organization, which should define an action plan to only monitor it and keep it under control if the cost of dealing with it outweighs the gains. It is also worth noting that such a strategy should only occur if the level of risk in question has passed the acceptance criteria;
2. Reduce: strategy in which an action plan is established to reduce the level of the risk in question, either by reducing the probability of its occurrence or its impact;

3. Eliminate: strategy in which the risk ceases to exist because the causes that made its manifestation possible are eliminated; and

4. Outsource: the establishment and implementation of the risk treatment is transferred to a third-party organization, with the company requesting the outsourcing being only responsible for the follow-up of this implementation and its effectiveness.

The review of a present risk can have two outputs:

a) Risk update, in which one or more attributes of the risk in question are modified; and

b) Maintenance of risk and its attributes.

Next, the process in question must go through a critical evaluation by its participants, who must highlight possible points of improvement to be redesigned in the process aimed at its continuous improvement. The control and registration of such evaluations are done in a table such as **Table 13**.

After this, the newly generated document must be saved and forwarded to the organization's CTO for approval. As for the old version, it must be stored with the others for later consultation and preservation of the version history, and the process ends.

Finally, it was stipulated that the process will formally take effect in the organization in January 2023. The person responsible for its approval is the company's CTO, who must sign the Microsoft Word document referring to this process, authorizing the execution of its latest version. The process ends with the beginning of the Information Security Risk Treatment process.

From an interview with the company's CEO, 18 information security risks were identified. The risks are found in **Table 19** as follows:

Table 19 - Information security risks

ID	Processo	Categoria	Tipo de informação	Descrição do risco	Causas	Probabilidade	Impacto	Nível de risco	Critério de aceitação
1	Onboarding de clientes	Confidencialidade	Funcionário do cliente + Cliente	Vazamento da planilha com os dados durante comunicação por e-mail. Há dois momentos do processo em que isso pode ocorrer durante o processo: quando não há integração entre o sistema de RH do cliente e a plataforma da Salars e é necessário o envio e troca de informações sensíveis via e-mail por planilhas; ou durante a validação dos dados consolidados caso haja integração entre o sistema de RH do cliente e a plataforma da Salars	Conta hackeada, pessoas com acesso inadequado participando da interação	3	4	12	Rejeitado
2	Geral	Confidencialidade	Funcionário do cliente + Cliente	Hackeamento de conta do e-mail de um funcionário da Salars, o que levaria o hacker a ter acesso a todas as planinhas e dados armanzenados dos clientes e seus respectivos colaboradores no Google Drive a serem expostos	Falta de segurança do sistema de e-mail do Google em prevenir tais ataques. Displicência do colaborador em seguir os procedimentos de segurança estabelecidos	2	5	10	Rejeitado
3	Onboarding de clientes	Confidencialidade	Funcionário do cliente + Cliente	Vazamento do token do cliente com os dados durante comunicação por e-mail	Conta hackeada, pessoas com acesso inadequado participando da interação	3	4	12	Rejeitado
4	Onboarding de clientes	Confidencialidade	Funcionário do cliente + Cliente	Hackeamento da conta de e-mail de algum funcionário do cliente que possua acesso à senha da empresa à plataforma da Salars, o que exporia todos os dados submetidos	Externa	2	4	8	Rejeitado
5	Onboarding de clientes	Confidencialidade	Funcionário do cliente + Cliente	Durante a reunião de tutorial, exibir dados sensíveis do cliente a funcionários não autorizados para ter acessos a tais informações	Falta de comunicação clara de normas a serem seguidas sobre quem deve participar da reunião. Utilização de uma conta real com dados reais	4	2	8	Rejeitado
6	Onboarding de clientes	Confidencialidade	Funcionário do cliente + Cliente	Geração equivocada de restrição de acesso aos funcionários do cliente, o que possibilitaria acesso a dados não autorizadas para a pessoa em questão. Além disso, existiria uma probabilidade relevante de que tal incidente não seja detectado	Erro de comunicação sobre quais dados cada colaborador do cliente terá. Incompetência da Salars	2	3	6	Aceito
7	Atualização do sistema de clientes	Confidencialidade	Funcionário do cliente + Cliente	Vazamento da planilha com os dados durante comunicação por e-mail. Há dois momentos do processo em que isso pode ocorrer durante o processo: quando não há integração entre o sistema de RH do cliente e a plataforma da Salars e é necessário o envio e troca de informações sensíveis via e-mail por planilhas; ou durante a validação dos dados consolidados caso haja integração entre o sistema de RH do cliente e a plataforma da Salars	Conta hackeada, pessoas com acesso inadequado participando da interação	3	4	12	Rejeitado
8	Atualização do sistema de clientes	Confidencialidade	Funcionário do cliente + Cliente	Hackeamento da conta de e-mail de algum funcionário do cliente que possua acesso à senha da empresa à plataforma da Salars, o que exporia todos os dados submetidos	Externa	2	4	8	Rejeitado
9	Atualização do sistema de clientes	Confidencialidade	Funcionário do cliente + Cliente	Vazamento da planilha com os dados durante comunicação por e-mail. Há dois momentos do processo em que isso pode ocorrer durante o processo: quando não há integração entre o sistema de RH do cliente e a plataforma da Salars e é necessário o envio e troca de informações sensíveis via e-mail por planilhas; ou durante a validação dos dados consolidados caso haja integração entre o sistema de RH do cliente e a plataforma da Salars	Conta hackeada, pessoas com acesso inadequado participando da interação	3	4	12	Rejeitado
10	Atualização do sistema de clientes	Confidencialidade	Funcionário do cliente + Cliente	Vazamento do token do cliente com os dados durante comunicação por e-mail	Conta hackeada, pessoas com acesso inadequado participando da interação	3	4	12	Rejeitado
11	Atualização do sistema de clientes	Confidencialidade	Funcionário do cliente + Cliente	Geração de planilha para fazer o cruzamento de dados durante o processo a qual não é deleteda no término. Um hackeamento de um colaborador que não tenha deletado tal arquivo pode expor os dados nele contidos	Inexistência de uma política de gestão de arquivos	2	4	8	Rejeitado
12	Alteração da senha dos clientes	Confidencialidade	Funcionário do cliente + Cliente	Cliente não coloca uma senha forte o suficiente e é facilmente hackeado comprometendo os dados da empresa e de seus funcionários	Inexistência de uma trava que obrigue o cliente a ter uma senha suficientemente protegida	1	3	3	Aceito
13	Entrada de colaboradores na Salars	Confidencialidade	Funcionário do cliente + Cliente	Novo colaborador com pouco conhecimento a respeito de segurança da informação, o que facilita a ocorrência de incidentes	Ausência de treinamento de segurança da informação que seja efetivo em comunicar e ensinar os processos e normas de segurança segundo os requisitos do SGSI	3	4	12	Rejeitado
14	Entrada de colaboradores na Salars	Confidencialidade	Funcionário do cliente + Cliente	Acesso a sites ou materiais potencialmente perigosos em termos de segurança da informação	Ausência de bloqueio de sites e outros fatores potencialmente perigosos nas máquinas fornecidas aos funcionários da Salars	2	4	8	Rejeitado
15	Saída de colaboradores na Salars	Disponibilidade	Funcionário do cliente + Cliente	Dados presentes apenas na máquina do colaborador de saída são perdidos após a formatação do equipamento	Não averiguação de dados importantes que poderiam estar presentes apenas na máquina em questão	1	2	2	Aceito
16	Troca de máquinas	Disponibilidade	Funcionário do cliente + Cliente	Dados presentes apenas na máquina do colaborador de saída são perdidos após a formatação do equipamento	Não averiguação de dados importantes que poderiam estar presentes apenas na máquina em questão	1	2	2	Aceito
17	Gestão de infraestrutura	Confidencialidade	Funcionário do cliente + Cliente	Disponibilização de nível de acesso além da alçada do colaborador solicitante	Falta de padronização em relação aos dados que cada colaborador poderá ter acesso	4	1	4	Aceito
18	Gestão de senhas intenras	Confidencialidade	Funcionário do cliente + Cliente	Funcionário que recebe as credenciais de acesso de algum sistema da Salars por meios não seguros/protegidos é hackeado compromentendo a segurança de informações sensíveis	Falta de uma padronização segura para o envio e recebimento de acessos	2	4	8	Rejeitado

Source: author.

First of all, as expected, most of the risks relate to confidentiality (16 in all). Only two risks refer to the availability of information and none to its integrity. This is because the meeting in which this happened was attended only by the author and the CEO. The CTO and the two developers were unable to attend due to scheduling conflicts as well as due to their allocation. Also, it should be noted that the meeting with the CEO lasted for less than 1 hour. Thus, it is expected that in future interactions in which everyone in the company participates and which last longer, the number of risks and their variety with respect to their classification will increase substantially.

Another point to be highlighted refers to the causes pointed out for each risk. After a more detailed analysis of the document, it was noticed that the causes pointed out are not the root causes of the risks in question, since they do not refer to what should be done as an action plan to control them. Thus, in addition to more risks, it is expected that those to be added and reviewed will present this field with a more adequate content and that will facilitate the next steps of the ISMS implementation. For this, methods such as the 5 Whys and the Ishikawa Diagram will help in this revision. It is also expected that, after a few interactions, the company's employees will know how to raise and frame the risks in the proposed way by their own, considering the high level of training of all involved, something that would bring agility and efficiency to the project.

As for the other fields, such as Responsible and Strategy, these have not yet been filled in because it was decided to wait until all the risks had been raised and then distribute them to the responsibility of the company's employees in a more rational, logical and balanced way.

6.3.4 Information Security Risks Treatment

This process is intended to ensure the organization's compliance with the following requirements of the standard:

a) Clause 6.1.3 – Information security risks treatment

For the process management, 5 documents were elaborated:

a) TratamentoDeRiscos.bpm – Bizagi file in which the flowchart was developed;

b) TratamentoDeRiscos.docx – Microsoft Word file which describes the process;

c) TratamentoDeRiscos.pdf – PDF file which describes the process;

d) TratamentoDeRiscos.png – image file of the generated flowchart; and

e) RiscosSegurancaDaInformacao.xlsx – file to conduct and carry out the process.

This process must satisfy 4 objectives:

a) Define action plans to reduce the level of risks to an acceptable value in order to control them;

b) Manage and monitor the established action plans to ensure their implementation;

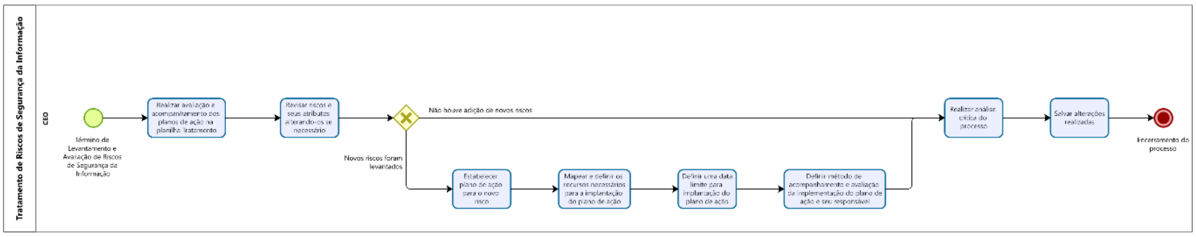
c) Ensure compliance of Salars Softwares e Soluções Ltd. with the NBR ISO/IEC27001: 2013 standard; and

d) Contribute to the continuous improvement of the SGSI.

In terms of execution frequency, this process must be executed in the last 7 working days of each month. If the process cannot be carried out within the stipulated timeframe, a justification must be inserted in the respective field present on the cover of the document TratamentoDeRiscos.docx.

Figure 30 below shows the flow chart of the designed process:

Figure 30 - Information Security Risks Treatment


Tratamento de Riscos de Segurança da Informação
CEO
Término da Levantamento e Avaliação de Riscos de Segurança da Informação
Realizar avaliação e acompanhamento dos planos de ação na planilha Tratamento
Revisar riscos e seus atributos alterando-os se necessário
Não houve adição de novos riscos
Novos riscos foram levantados
Estabelecer plano de ação para o novo risco
Mapear e definir os recursos necessários para a implantação do plano de ação
Definir uma data limite para implantação do plano de ação
Definir método de acompanhamento e avaliação da implementação do plano de ação e seu responsável
Realizar análise crítica do processo
Salvar alterações realizadas
Encerramento do processo

Source: author.

The owner of the process in question was defined as the CEO of Salars Softwares e Soluções Ltd.

Its inputs are:

a) Most recent version of the RiscosSegurancaDaInformacao.xlsx document.

Its outputs are:

a) Newer version of the RiscosSegurancaDaInformacao.xlsx document.

The process is entirely driven by the CEO of Salars Softwares e Soluções Ltd. The CTO and the Developer Team must also participate in its execution.

It begins with the end of the Information Security Risks Assessment process. Thus, with the file RiscosSegurancaDaInformacao.xlsx opened, team must access the Treatment worksheet to conduct this process. This worksheet consists of a table where each line refers to an action plan associated with a risk and has 14 fields (columns) to be filled in:

a) ID (already filled in the previous process);

b) Process (already filled in the previous process);

c) The risk category (already filled in the previous process);

d) Risk description (already filled in the previous process);

e) The type of information involved with the risk in question (already filled in the previous process);

f) Causes (already filled in the previous process);

g) The probability, impact and risk level (already filled in the previous process);

h) Acceptance criteria (already filled in the previous process);

i) Responsible (already filled in the previous process);

j) The Priority 1 field (already filled in the previous process);

k) The Priority 2 field (already filled in the previous process);

l) Strategy (already filled in the previous process);

m) Expected results: field to define what the action plan is expected to generate as a result regarding the risk in question. It is recommended that this field be quantified as far as possible in terms of the level of risk expected to be achieved as well as its impact and probability components;

n) Action: action plan for the risk described in a detailed and intelligible manner. The field must be structured in a way to break down the action plan into its macro activities, which must be separated by paragraphs and numbered sequentially (to generate a paragraph within a cell in Excel, use Alt + Enter in Windows) similarly to how the Causes field is structured;

o) Necessary resources: the team must determine the resources required to implement the action plan. This field should follow the same organizational logic as the Action column;

p) Deadline: deadline for action plan implementation;

q) Evaluation of results: in this field, the team must define who will be responsible for following up and monitoring the implementation of the plan in question. In addition, team must determine how the follow-up will be done;

r) Comments: field to be filled in by the person responsible for the approval of the risk/opportunity. How to fill it out will be detailed below; and

s) Status: action plan implementation status (Not Started, In Progress, or Completed).

With the spreadsheet open, the first activity to be performed is the follow-up and evaluation of the action plans defined for each risk. The objective of this activity is to verify if the action plans stipulated in the last execution of this process are reaching the expected results (or heading towards them).

If the action plan in question was implemented in its entirety and its associated risk is no longer an information security threat according to the judgment of the person responsible for its evaluation, the Status field must be completed as Completed. In addition, it is up to the person responsible for evaluating the action plan to define how the control and monitoring of this risk will be done to ensure that the implemented action plan is generating the expected results. This must be registered in the Comments field. Furthermore, a monitoring frequency appropriate to the risk in question must be established to prevent successive information security incidents from occurring due to a possible unforeseen loss of risk control without corrective measures being implemented.

If the action plan is being executed as planned, it is up to the person responsible for evaluating the results to register compliance in the Comments field. If this is not the case, the action plan should be reviewed and, if necessary, changed in order to achieve the expected results within the stipulated timeframe. In this case, it is up to the person responsible for evaluating the results of the action plan to determine, together with the person responsible for the action plan and the other participants in the meeting, the causes of this deviation and what measures will be taken to correct it. These points must be listed in an intelligible and structured way in the Comments field.

After this, if new risks have been mapped in the Information Security Risk Survey and Assessment process, the team must first determine in the Expected Results field what are the objectives (i.e., what is expected to be achieved) that the organization expects to achieve for the treatment of the risk in question. If possible and feasible, it is recommended to quantify these objectives to facilitate comparison and follow-up over time.

Next, in order to achieve expected results, the action plan used to treat the risk in question is determined. To do this, action plans should always be established based on the root causes determined previously and provide an explanation as to why these causes are eliminated or mitigated through the defined treatment. In addition, it should be noted that more than one action plan can be implemented for the treatment of a given risk if deemed necessary.

After that, the necessary resources, and the timeframe for implementing the action plan are defined, as well as the person responsible for evaluating the treatment and how this evaluation will be done.

Then, the Status field should be filled in as Not started and can only be changed to In Progress if it is found that the activities defined to implement the treatment are being carried out as planned.

Finally, the process in question must undergo a critical evaluation by its participants, who must highlight possible points of improvement to be redesigned in the process aiming at its continuous improvement. The control and register of such critical evaluations must be in **Table 13** of this document. With this, the newly generated document must be saved and forwarded to the organization's CTO for approval. Furthermore, it has been stipulated that the process will formally take effect in the organization in January 2023. The person responsible for its approval is the company's CTO, who must sign the Microsoft Word document referring to this process, authorizing the execution of its latest version.

In terms of the results generated with this process, it was decided not to carry it out yet due to a few factors. Firstly, due to the fact that the immediately previous process had not been completed (there are still risks to be added) and due to the lack of precision of the causes established for each risk. Thus, it was understood that rework would be avoided once all the risks have been surveyed and with their respective parameters filled in accurately, and that everyone in the company is aligned with the process.

However, three of the risks pointed out already have their respective action plans defined and implemented. These are risks ID 5, 7 and 9. The first of these refers to during the tutorial meeting, where sensitive customer data can be shown to unauthorized employees. To control the risk, therefore, action was taken on two fronts. The first of these is about communicating to the customer before the meeting to select only employees who may have access to that information that will be displayed. In parallel, the developer team created an account with fictitious data for the next tutorials with the customers. Risks 7 and 9 (concerning the Onboarding and System Update processes), which relate to the possibility of information leakage during the file exchange process via email when there is no integration between the customer's Human Resources system and the Salars platform, were treated with the same action plan. Once again, the developers have inserted a new functionality on the company's website where the client downloads the file with the template for filling in the information and deposits it, now with the information, in the same environment. This way, there is no more e-mail exchange and the risk is now controlled.

7 CONCLUSION AND NEXT STEPS

Although this work did not achieve the initially proposed objective in its entirety due to replanning, technical issues, availability issues and communication failures between the author and the company, the most relevant points of the standard have their processes designed and validated, leaving only the correct execution of the Information Security Risks Mapping and Evaluation and Information Security Risks Treatment processes to have all the necessary material to design the ISMS processes. The company signaled its intentions to continue with the proposed work, however increasing the availability and alignment of employees for the correct execution of the mentioned processes. Although few and simple, some measures to increase the information security in terms of process were already adopted for the information security risks of ID 5, 7 and 9.

Thus, it was stipulated as a goal that by the end of 2022, all processes and documents related to ISMS are already defined and validated so that, as of 2023, these processes can be executed. With this, it is expected that the organization will be ready for certification in the standard in question in March 2023.

Therefore, the next steps are to continue the project starting with the re-design of the processes mentioned above. Once the risks are clearly defined and fully described, these risks will be compared with the controls present in Annex A of the standard, seeking the implementation of all applicable controls, prioritizing the most critical ones. After this, the Statement of Applicability (SoA) document, required by the standard, will be generated. In it, the reasons for applying or not applying all the defined controls will be justified.

With these steps concluded, the next step is to define the information security objectives so that the information security policy can be documented. For this, a meeting has already been held between the author and an employee from Fundação Vanzolini seeking help in how such a document should be structured. Thus, with the Plan stage of the PDCA cycle under way, possible competencies, and organizational resources that the company must still obtain in order to have these competencies and resources determined are mapped. Also, indicators and monitoring routines are defined so that possible deviations from the route are quickly corrected, thus enabling the organization to enter the Do stage of the cycle.

8 REFERENCES

AMERICAN SOCIETY FOR QUALITY. American Society for Quality. **Site da American Society for Quality**. Disponivel em: <https://asq.org/quality-resources/total-quality-management/deming-points>. Acesso em: 8 jun. 2022.

ATKINS, B. Demystifying ESG: Its History & Current Status. **Forbes**, New York, Abril 2020. Disponivel em: <https://www.forbes.com/sites/betsyatkins/2020/06/08/demystifying-esgits-history--current-status/?sh=16e5a322cdd3>. Acesso em: 2 jun. 2021.

BERSSANETI, F. **Gerenciamento da capacidade produtiva de um sistema de educação a distância: coordenação das funções manutenação e gestão de contratos**. University of São Paulo. São Paulo, p. 187. 2006.

BERSSANETI, F. T.; BOUER, G. **Qualidade:** conceitos e aplicação em produtos, projetos e processos. 1. ed. São Paulo: Edgard Blücher, 2018. 192 p.

G1. G1. **Site do G1**, 2 dez. 2020. Disponivel em: <https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml>. Acesso em: 31 maio 2021.

INTERNATIONAL FINANCE CORPORATION. **Who Cares Wins**. International Finance Corporation. Washington, p. 32. 2005.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ABNT NBR ISO/IEC 27001**. International Organization for Standardization; International Electrotechnical Commission. Geneva, p. 36. 2013.

LEE, J.; BEN-NATAN, R. **Integrating Service Level Agreement**. Wiley. Indianapolis. 2002.

LONGARAY, A. et al. Proposta De Mapeamento De Processos Usando A BPMN: Estudo De Caso Em Uma Indústria Da Construção Naval Brasileira. **Revista Eletrônica de Estratégia & Negócios**, Florianópolis, v. 10, n. especial 1, p. 29, Abril 2017.

MOREIRA, G. **Análise de lacunas e proposta de melhoria para o Sistema de Gestão de Compliance de uma empresa de construção civil**. University of São Paulo. São Paulo, p. 109. 2021.

PALMA, G.; NETTO, W. G1. **Site do G1**, 19 mar. 2021. Disponivel em: <https://g1.globo.com/economia/tecnologia/noticia/2021/03/19/policia-federal-deflagra-operacao-contra-divulgacao-e-comercializacao-de-dados-pessoais-de-brasileiros.ghtml>. Acesso em: 31 maio 2022.

STURM, R.; MORRIS, W.; JANDER, M. **Foundations of Service Level Management**. Sams: [s.n.], 2000.

WENS, C. V. D. **ISO 27001 Handbook:** Implementing and auditing and Information Security Management System in small and medium sized business. [S.l.]: Publicado de forma independente, 2019.