LUCAS MOTA DE OLIVEIRA

NICOLLAS LOPES NEVES

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO EM UMA EMPRESA DE SOFTWARE PARA POSTOS DE COMBUSTÍVEIS NA CIDADE DE JUIZ DE FORA**

Trabalho de conclusão de curso apresentado como requisito para obtenção do título de Bacharel em Sistemas de Informação.

ORIENTADOR: RICARDO SILVA CAMPOS

Juiz de Fora

2019

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO EM UMA EMPRESA DE SOFTWARE PARA POSTOS DE COMBUSTÍVEIS NA CIDADE DE JUIZ DE FORA**

**Lucas Mota Oliveira\***

**Nicollas Lopes Neves\***

**Ricardo Silva Campos\*\***

**RESUMO**

O presente trabalho tem por objetivo realizar um estudo de caso em uma empresa de criação e suporte de sistemas para postos de combustíveis. A partir deste estudo, será proposta a política de segurança da informação da empresa. Para isso, foi feita uma revisão sistemática da literatura com o intuito de verificar as boas práticas e técnicas para elaborar uma boa política da segurança da informação. Assim, um estudo de caso foi realizado através da aplicação de um questionário de questões abertas, utilizando-se o software MAXQDA para analisar qualitativamente os dados. Foi montada uma matriz SWOT da empresa com a sua estrutura de organograma e fluxograma das atividades de suporte ao cliente. O resultado desta análise culminou na elaboração da política de segurança da informação da empresa, cuja meta é melhorar o controle de riscos e vulnerabilidades das informações e seus colaboradores, baseando-se na ISO 27001 e ISO 27002, além de boas práticas.

**Palavras-chave:** Política de segurança da informação, ISO 27001, ISO 27002.

***ABSTRACT***

*This work presents a case study of a company that offers software creation and support for gas stations. A proposal of information security policy for the company is formulated through this study. A systematic literature review was conducted to verify good practices and how to develop a satisfactory information security policy.*

*The case study was done via a questionnaire application, and the collected data was qualitatively analyzed by MAXQDA. A SOWT matrix of the company was assembled with organization hierarchy structure and the customer support activity flowchart. The outcome of this study is the information security policy, for improving the control of risks and vulnerabilities intrinsic from information and company’s employees. This document was based on ISO 27001 and ISO 27002 standards, along with good practices.*

***Keywords:*** *Security information policy, ISO 27001, ISO 27002.*

\*Bacharelando em Sistema de Informação – Faculdade Metodista Granbery.

\*\* PHD em Modelagem Computacional UFJF – Faculdade Metodista Granbery.

# 1 INTRODUÇÃO

A segurança da informação é uma área pertencente à computação que preza pela segurança dos dados, de maneira a garantir que estes dados não sejam obtidos por pessoas que não deveriam ter acesso a essas informações.

Os três pilares da segurança da informação são: confidencialidade, integridade e disponibilidade. Basicamente, a equipe responsável por manter esses pilares tem como função proteger o sistema de uma maneira que ele fique o mais seguro possível, visto que nenhum sistema é totalmente seguro.

A segurança da informação está intimamente associada aos riscos que estão sujeitos os dados de uma organização qualquer. Devido à importância deste ativo, o desenvolvimento de políticas de segurança da informação tem se tornados mais necessário dentro das instituições, seja ela pública ou privada. Uma boa gestão da segurança garante que as ameaças sejam combatidas de forma mais efetiva.

A política de segurança da informação é feita para controlar e proteger determinados dados, virtuais ou físicos, com uma série de normas a serem seguidas, hierarquias de acessos a informações e treinamento de pessoal. Existem algumas normas para estas ações, como por exemplo a ISO 27001:2013 e a ISO/IEC 27002:2015, que consistem em normas a serem seguidas para garantir a segurança das informações.

Um grande problema que se desenvolve nas organizações é a confiabilidade nas pessoas que estão interagindo com as informações importantes dos setores, que, se utilizadas indevidamente, podem causar vários problemas de vulnerabilidade de dados. Atualmente este assunto tem ficado cada vez mais frequente entre as empresas e governos, com o objetivo de abordar a vulnerabilidade de dados e confiabilidade no humano que as conduz, pois este pode ser corruptível e, por conseguinte, criar uma brecha para ataques e obtenção de informação sigilosa das organizações para uso indevido.

O objetivo deste artigo concentra-se em estudar a organização, levantando informações de seus problemas no tocante a segurança de suas informações, políticas já existentes. As análises serão feitas por aplicação de questionário em uma entrevista, analisar os dados, gerar o documento sobre as políticas de segurança da informação para a empresa.

**2 MOTIVAÇÃO**

A segurança da informação é algo muito importante dentro de qualquer empresa seja ela pública ou privada. Com o avanço da tecnologia, as vulnerabilidades podem ser identificadas facilmente por pessoas especializadas em cometer crimes de roubo de informação e invasão de sistemas. É imprescindível a preocupação com uma política de segurança de informação, acrescida da gestão dos colaboradores, para que a cultura da política seja absorvida e praticada por eles. A vulnerabilidade de informações é um risco para gestão da segurança da informação.

O uso intensivo da tecnologia tem provocado algumas transformações bem significativas para a humanidade, uma espécie de revolução digital. Com o grande crescimento da rede mundial de computadores, a Internet, houve também um crescimento contínuo de transações eletrônicas, caracterizando os tempos atuais como era da informação. Desta maneira, há pessoas habilidosas em tecnologia que agem intencionalmente para prejudicar as empresas (Souza, J. G. S.; Almeida, R. F.; Kussama, L; Arima, C. H.; Galegale, N. V., 2015).

As dificuldades encontradas por algumas organizações em avaliar riscos de suas atividades, especialmente em relação à segurança de dados e as possíveis vulnerabilidades da TI, podem ocasionar brechas e consequentemente, ataques de criminosos. O processo de gestão de riscos, por sua vez, trata dos riscos relacionados à segurança da informação. Há um grande interesse por parte dos gestores na identificação dos riscos na segurança da informação, pois se consegue obter um maior controle dos impactos disso no negócio (Moraes, D. P.; Muylder, C. F.; Barros, L. C.; Oliveira, J. G.; Carneiro, S. D., 2015).

# 3 EMBASAMENTO TEÓRICO

**3.1 ISO/IEC 27001**

A norma ISO 27001 é o padrão internacional para a gestão da segurança da informação. A norma tem como objetivo criar um processo de controle das informações da organização, necessário para a criação um projeto e que reflete nos objetivos do negócio. A avaliação de riscos também faz parte da norma, auxiliando no levantamento de vulnerabilidades e ameaças, permitindo que seja elaborada uma lista de que podem ser priorizadas com base no nível de risco que representa a informação. Contudo o entendimento da situação da segurança da informação será obtido, com isso a elaboração de políticas de segurança da informação, controle de riscos e vulnerabilidades serão criados e implementados.

Ao adotar a norma podem-se obter vários benefícios como: Identificação de riscos e definição de controles para gerenciá-los ou eliminá-los, flexibilidade para adaptar os controles a todas as áreas ou a áreas selecionadas da empresa, ganhar a confiança das partes interessadas e dos clientes, que sabem os dados estão protegidos. (BSI, 2019).

**3.2 ISO/IEC 27002**

Criada em 1995 pelas organizações internacionais Organização Internacional de Normalização e a Comissão Eletrotécnica Internacional, através do fornecimento de um guia completo de implementação, ela descreve como os controles podem ser estabelecidos. Estes controles, por sua vez, devem ser escolhidos com base em uma avaliação de riscos dos ativos mais importantes da empresa. O seu principal objetivo é estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Basicamente a norma se baseia em: definir os ativos (qualquer coisa que tenha valor para a empresa), controle dos riscos, diretrizes que orientam o que deve ser feito e como, a segurança da informação, recursos que processa as informações, incidentes de vulnerabilidades, análise avaliação, gestão e tratamento dos riscos.

Com a implementação dos princípios da norma será possível a conscientização sobre a segurança da informação, o controle de ativos e informações, implantação de políticas de controles, identificar e corrigir pontos fracos, organizar os processos e mecanismos de controle, redução de custos com a prevenção de incidentes de segurança da informação (ABNT, 2005).

**3.3 Segurança da Informação / Política**

É essencial a criação ou atualização de uma política de segurança da informação que seja coesa com a estratégia da empresa, mas que consiga tratar adequadamente a gestão dos dados. Uma das partes mais importante seriam as responsabilidades dos colaboradores da organização para sua aplicação. O planejamento da gestão da segurança da informação é necessário para que a política seja bem feita e precisa. (FONTES, 2012). Contudo a informação é um ativo importante da empresa, por este motivo todo o ambiente e equipamentos utilizados para processá-la devem ser cuidadosamente protegidos, pois a informação tem um valor muito grande para a organização e seu vazamento, ou utilização indevida seria muito crítico para o negócio. (FONTES, 2006).

O fator humano influencia na segurança da informação, pois a confiança e a prática da política da segurança da informação é algo volátil por interferência humana. Um dos problemas encontrados em vários casos de roubos de informações, uso indevido de dados, possui algo muito importante por trás, a Engenharia Social. Engenharia social está ligada a persuasão de pessoas, geralmente aplicada por pessoas que sabem o que estão fazendo. Essas pessoas se passam por boas, querendo ajudar, se aproveitam de das vulnerabilidades humanas e obtém o que querem. É necessário agir estrategicamente na segurança da informação, estabelecendo um grau de importância para cada informação durante o planejamento estratégico da organização, é necessário que se torne uma cultura organizacional da empresa para ser seguida espontaneamente e com responsabilidade. (LYRA, 2015).

Com o quadro incerto que se encontra em todo tipo de organização ao tratar suas informações, sejam elas confidenciais ou não, torna-se fundamental só o profissional da área de tecnologia da informação, mas também os demais responsáveis por algum tipo de informação que comprometa a organização, serem orientados, instruídos e comprometidos ao melhor tratamento e cuidados com as informações, todos os integrantes da organização devem estar dentro do propósito de cuidar dos dados e seguir as estratégias dispostas pela empresa (PEIXOTO, 2006). É indicado que na estrutura organizacional da empresa exista uma área responsável pela segurança das informações, (geralmente há um comitê de riscos para tal tarefa) onde deve iniciar o processo de elaboração da política de segurança da informação e coordenar sua implantação, aprová-la e revisá-la, além de designar funções de segurança para os colaboradores devidos. Entretanto as pessoas de áreas críticas da instituição devem participar do processo de elaboração. Além disso, é recomendável que a política de segurança da informação seja aprovada pela mais alta cúpula da empresa, ou seja, o profissional mais considerável da organização (T.C.U., 2012).

A análise da política e gestão da segurança da informação contribuirá para tornar visível a relevância e urgência do assunto para uma empresa, como objetivo mapear os riscos e vulnerabilidades para então tornar o negócio mais seguro. Questões relacionadas à segurança da informação vêm cada vez mais gerando preocupação entre as empresas, pois aplicada de maneira adequada, visa proteger a organização de possíveis ameaças que comprometam os negócios. É relevante informar que a segurança da informação não está ligada somente a área da TI, abrange também questões de segurança do espaço físico, dados em nuvem, entre outros.

Para Goodrich e Tamassia (2013) a tendência natural é associar segurança da informação com um contexto totalmente digital, porém o acesso à informação digital encontra-se em algum espaço físico e para acessar a informação é necessária uma interface entre o espaço físico e digital, portanto devem ser incluídas nas políticas de segurança da informação – PSI’s das organizações medidas corretivas e preventivas para proteção da interface física, por exemplo, proteção dos locais onde estão os computadores, detectar acesso de pessoas não autorizadas, alarmes, entre outros. Segundo Sêmola (2014, p.15) o maior desafio das organizações é identificar “ameaças, vulnerabilidades, riscos, sensibilidades e impactos, a fim de permitir adequado dimensionamento e modelagem da solução”. Dessa forma, é importante que as empresas tenham adotadas PSI’s para garantir que suas informações não sofram nenhuma alteração indesejada ou inadequada.

É nítido que as PSI’s são extremamente importantes e necessárias para a continuidade dos processos das organizações, pois tem como intuito proteger todas as etapas pela qual a informação passa na entidade, sejam elas físicas ou por meio de tecnologia. O sucesso da aplicação da PSI está relacionado diretamente ao comprometimento e à atuação da alta administração para com os outros colaboradores da empresa, quanto maior o envolvimento do nível estratégico com os procedimentos de preparação e adoção de políticas, maior será a probabilidade de a PSI ser eficaz e efetiva, é necessário que esse envolvimento seja instituído formalmente e por escrito, assegurando o cumprimento (TCU, 2012).

**4 TRABALHOS RELACIONADOS**

O trabalho de (SERAFIM, 2017) analisou a existência de políticas de segurança da informação adotadas em um órgão da administração pública estadual. Utilizando a metodologia descritiva e qualitativa com estudo de caso realizado na Controladoria Geral do Estado da Paraíba, realizando um questionário e entrevistas com os colaboradores para coleta de dados. Toda a coleta foi feita com o dirigente máximo da organização, para obter conhecimento de sua percepção sobre diversos pontos da implementação da segurança da informação. Todas as análises de dados utilizadas foram: análise descritiva para o questionário e análise qualitativa para a entrevista.

Na análise qualitativa foi usado o software MAXQDA (MAXQDA é um software para análise de dados qualitativos e métodos mistos em pesquisas acadêmicas, científicas e comerciais). Pode-se concluir que existem algumas Políticas de Segurança da Informação implantadas, como backup, antivírus, controles de acesso, porém foi constatado que existem alguns problemas e dificuldades para uma boa prática de política como capacitação dos prestadores de serviço, a falta de interesse dos funcionários e a falta de um manual contendo todas as políticas de segurança da informação disponibilizado para todos os colaboradores da organização. Após estas análises retiradas das pesquisas o gestor do entrevistado pôde elaborar estratégias de consolidação das políticas da segurança da informação e todo o ambiente de segurança.

(SOUZA, 2017), realizou uma análise de tratamento da segurança da informação na gestão de riscos em uma instituição de ensino público federal. O estudo foi feito analisando os aspectos de riscos que envolvem a organização de segurança e infraestrutura, as políticas de segurança de segurança da informação, normas e procedimentos, junto ao treinamento dos colaboradores. Foram aplicados questionários para levantamento e análise de dados sobre a prática de segurança da informação dentro da governança da tecnologia da informação. Os resultados se basearam na aplicação dos componentes de segurança na instituição, podendo ter uma manutenção e compreensão do ambiente de riscos e vulnerabilidades. Também foi usado o software MAXQDA para análise dos dados levantados.

A análise nos trabalhos relacionados foi realizada sob a perspectiva de ataques e vulnerabilidades nas organizações e falhas na própria aplicabilidade de normas e procedimentos de sua política de segurança da informação e o quão falho isto pode estar em uma organização. Em especial, salienta-se sempre a importância de um bom entendimento do ambiente de segurança por parte dos colaboradores, para que eles saibam como aplicar e garantir que as melhorias sejam feitas da melhor forma possível.

**5 ESTUDO DE CASO**

**5.1 Metodologia**

Será criado um questionário para coleta de informações da organização de forma qualitativa, que será aplicado em uma entrevista direta com o gestor. Os dados coletados via entrevista serão analisados qualitativamente com o software MAXQDA, que permite a visualização de maiores detalhes das informações. Será montada uma matriz SWOT da empresa com a sua estrutura de organograma e fluxograma da atividade de suporte ao cliente. A partir desta análise será elaborada a política de segurança da informação da empresa, com o intuito de melhorar o controle de riscos e vulnerabilidades das informações e seus colaboradores, baseando-se na ISO 27001 e ISO 27002, além de boas práticas. O resultado será uma contribuição muito efetiva para a empresa e seus processos, auxiliando a melhoria de seu processo de governança da tecnologia da informação e riscos.

**5.2 A Empresa**

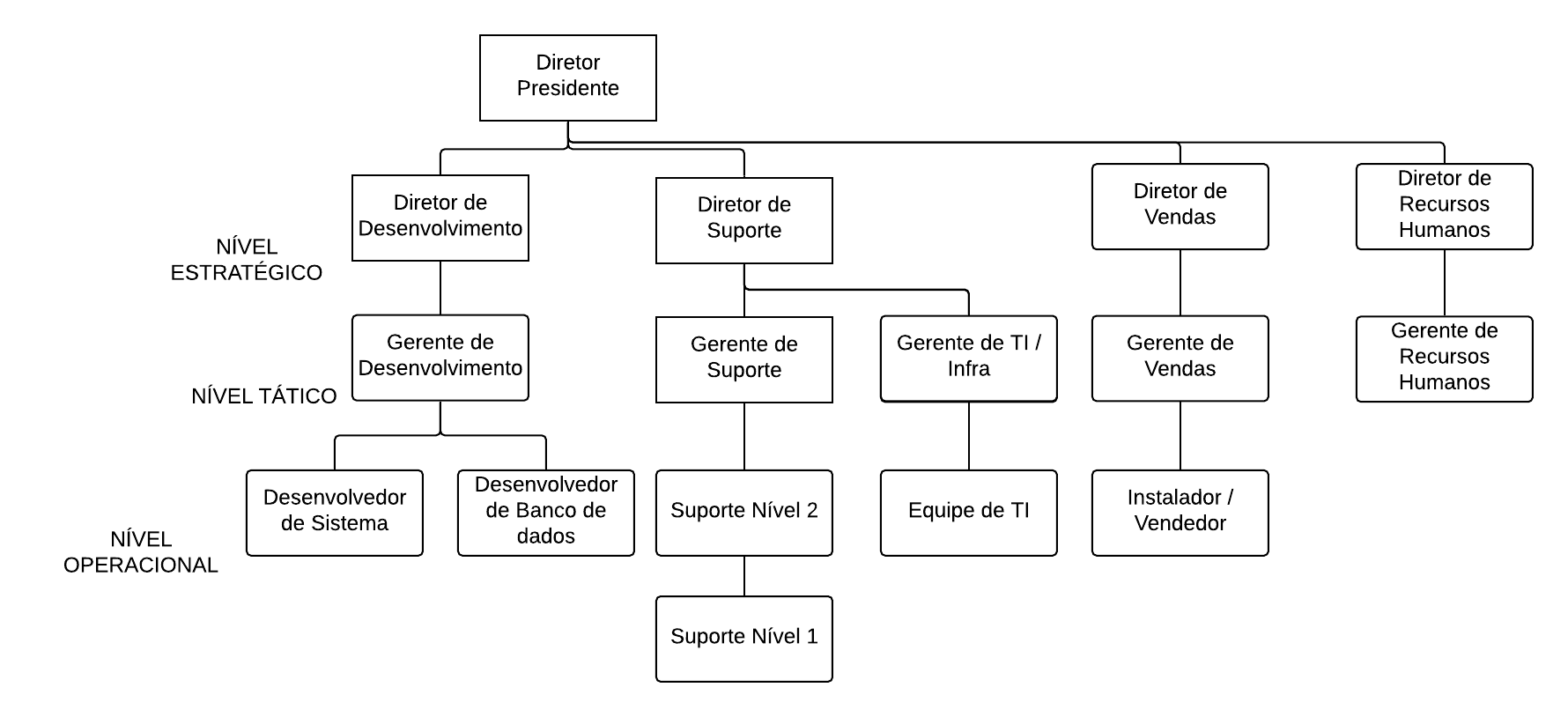
A organização foi criada em 1994, situada na cidade de Belo Horizonte, com filiais, e uma delas está em Juiz de Fora, onde está sendo feito o estudo de caso.

A empresa oferece um *software* para postos de gasolina que reduz o consumo de recursos, custos operacionais, margens de erro e retrabalho. O objetivo é simplificar, organizar e tornar mais seguro os processos de trabalho, através de relatórios gerenciais que auxiliam nas tomadas de decisão e permitem uma análise contextualizada e dirigida. O sistema possui vários módulos integrados, como: automação de bomba de combustíveis, medição de tanque de combustível, controle de ponto de funcionário, entre outros.

**5.3 Organograma**

Inicialmente foi analisado todo o organograma da empresa, para a compreensão de como funcionam os níveis estratégicos, táticos e operacionais.

**Figura 1 – Organograma da Empresa**

****

Fonte: JUIZ DE FORA. Empresa – Estrutura.

**5.4 Coleta de Dados**

A coleta de dados foi executada em contato com o gestor da empresa, após isto a aplicação do questionário na entrevista. Essa entrevista foi efetuada com base em um roteiro semiestruturado, contemplando questões sobre políticas de segurança da informação, resistência na implementação da segurança da informação, qualidade das informações prestadas, conhecimento dos funcionários sobre as políticas adotadas, suas responsabilidades, bem como os benefícios da implementação de políticas, suas dificuldades, e as considerações como gestor numa posição primordial dentro da organização para adoção das políticas.

Esse roteiro teve como objetivo guiar o tema, permitindo que o entrevistado pudesse se expressar livremente e se aprofundar sobre o assunto e a sua experiência no tema. No caso específico desta pesquisa, a técnica de coleta de dados da entrevista se justifica, conforme Selltiz et al. (1967, p.273), por ser uma técnica que se enquadra para obter as “informações sobre o que as pessoas sabem, creem, esperam, sentem ou desejam, pretendem fazer ou fizeram, bem como sobre suas explicações ou razões a respeito das coisas precedentes”. Abaixo está a entrevista transcrita:

**Lucas: No contexto da empresa, toda a estrutura da mesma: dados, processos, áreas, o que deseja proteger?**

Respondente: Nas nossas conversas e as explicações sobre esta área para nós foi muito importante, abriu os nossos olhos para isto, então queremos proteger o máximo possível do nosso ativo (dados) que são nossos e de clientes, para que possamos crescer melhor e mitigar as nossas falhas. Queremos proteger também o nosso colaborar de ser menos vulnerável e suscetível a cometer falhas que comprometam a nossa organização.

**Lucas: A organização possui gestão de riscos? Como é feita?**

Respondente: Não gerenciamos os riscos de forma correta, porque é sempre em forma de apagar incêndios, não prevemos os problemas por não ter este controle, na hora que acontece temos muita dificuldade em lidar para resolver.

**Lucas: A empresa possui hierarquia e classificação a acesso de dados pelos colaboradores (integridade, confidencialidade e disponibilidade)?**

Respondente: Essa parte é bem solta, pois quando precisa um funcionário tem acesso a qualquer informação além de autonomia para alterar sem nem mesmo padronizar ou comunicar o superior.

**Lucas: Quais as maiores limitações e necessidades da empresa no quesito segurança da informação?**

Respondente: Sentimos que não cuidamos bem da nossa segurança, não entendemos como funciona, qual a importância de tudo isso, contudo temos uma necessidade muito grande de aprender a nos proteger e controlar os nossos riscos e falhas.

**Lucas Existe o uso de alguma ferramenta, controle de acesso, para auxiliar na segurança das informações?**

Hoje nós utilizamos firewall do Windows e antivírus não pago. O controle de acesso é meio falho porque não possui uma padronização, e nem um alinhamento mais detalhado para os colaboradores.

**Lucas: Qual o histórico de falhas e vulnerabilidades que a organização possui?**

Respondente: Como utilizamos ferramentas de acesso remoto para prestar o suporte do software muitas vezes colocamos senhas padrões, mas pela baixa capacidade do pessoal de entender melhor a segurança dos dados, acabam ocorrendo acessos de outras pessoas se passando por nossa empresa para acessar os clientes, como já aconteceu várias vezes. Também houveram casos dos nossos colaborados baixarem coisas com vírus e infectar a rede, perdendo e corrompendo informações.

**Lucas: Os colaborados são capacitados minimamente para fazer uso dos dados da empresa?**

Respondente: Os nossos colaboradores e equipes sabem o básico de como se precaver, mas entendemos que não possuem o direcionamento certo para garantir a segurança dos dados, mas isso podemos resolver com treinamentos e adoção de culturas usando o endomarketing.

**Lucas: Em caso de um incidente, a organização possui um gerenciamento dos mesmos ou um plano de controle, com pessoas responsáveis para atuar na correção e dar continuidade ao negócio?**

Respondente: Infelizmente não temos o controle desses incidentes, o que acontece na hora sem previsão, nós tentamos resolver o mais rápido possível, mas as vezes demora ou não conseguimos e temos que parar o cliente para fazer uma manutenção mais profunda, isso gera muita insatisfação por parte deles e acaba nos prejudicando.

**Lucas: Há por parte da organização um comprometimento e aceitação da criação da política da segurança da informação e sua implementação?**

Respondente: Sim, gostamos muito da ideia e estamos comprometidos a ajudar, implementar e garantir que seja executada. Os colaboradores estão bem receptivos a tudo isso, o que torna fácil para vocês e para nós.

**Lucas: A organização possui controle do uso de dispositivos físicos de armazenamento de dados?**

Respondente: Não há bem um controle, pedimos para tomar cuidado ao usar estes tipos de dispositivos, sempre checar se não há vírus ou arquivos estranhos, mas infelizmente não controlamos e não passamos de forma mais rígida para os colaboradores.

**5.5 Tratamento e Análise de Dados**

A entrevista acima foi transcrita conforme procedimentos do software selecionado para análise, para que seja possível avaliar as respostas obtidas. Nesse caso, o processo para a análise do conteúdo da entrevista, ocorreu por meio do software MAXQDA, versão demonstrativa.

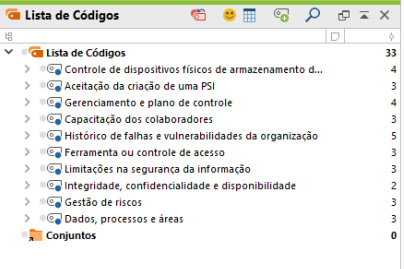
O MAXQDA é utilizado para a análise qualitativa de dados não estruturados, através da atribuição de categorias, codificação de segmentos de texto é possível apresentar os resultados. O MAXQDA proporcionou a análise do conteúdo obtido pela entrevista, de modo qualitativo. Posteriormente, à codificação seguiu-se a análise e comparação dos dados apresentados nas tabelas e mapas que o programa oferece para a mais correta visualização dos resultados. (MAXQDA 12,2017)

**5.6 Resultados**

O questionário apresentado anteriormente mostra as percepções do gestor sob a sua empresa. A partir disto, percebe-se a necessidade da implantação de política de segurança da informação. Com a codificação realizada a partir do software de análise qualitativa MAXQDA, há dez codificações para a Segurança da Informação que pode ser visto na (FIGURA 2).

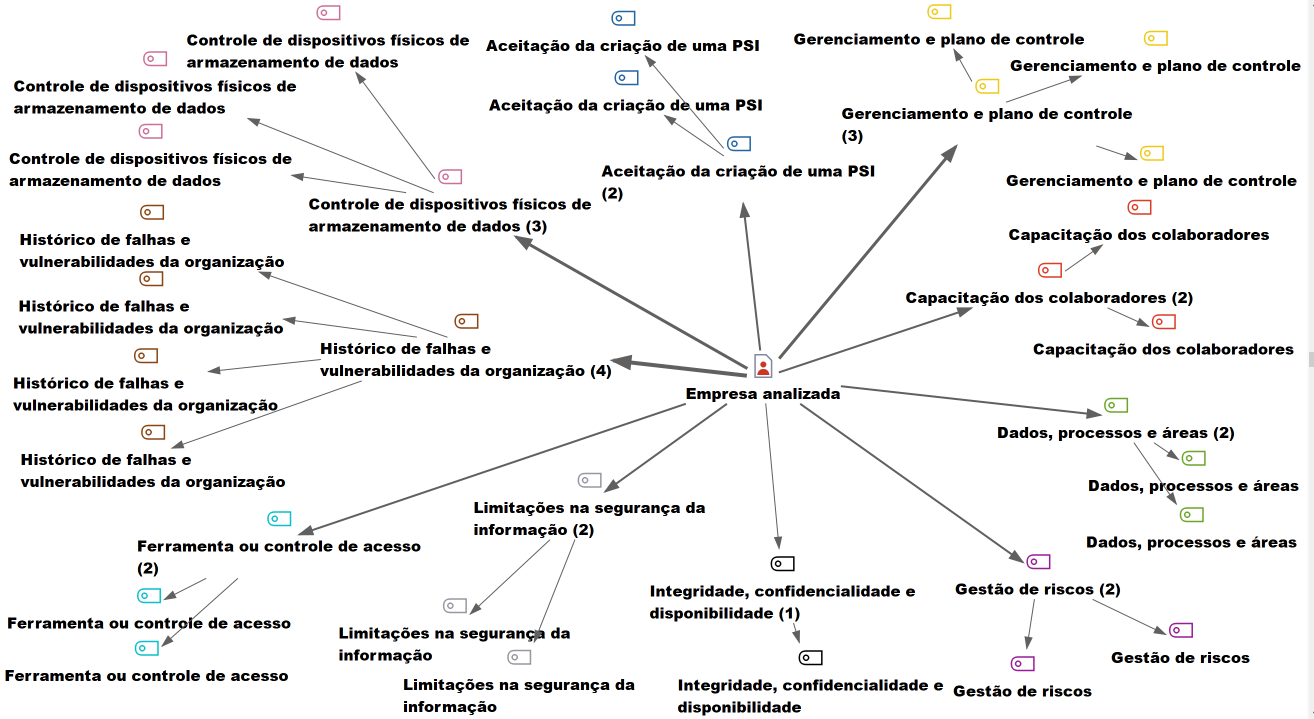
São elas: o controle de dispositivos físicos de armazenamento de dados, a aceitação da criação de uma política de segurança da informação, o gerenciamento e plano de controle, a capacitação dos colaboradores, histórico de falhas e vulnerabilidades da organização, as ferramentas ou controle de acesso, as limitações na segurança da informação, a integridade, confidencialidade e disponibilidade, a gestão de riscos e os dados, processos e áreas.

**Figura 2 – Frequência dos Códigos - Implementação de Políticas de Segurança da Informação**



Fonte: Elaboração própria, 2019.

**Figura 3 – Mapa das tribulações da Organização**



Fonte: Elaboração própria, 2019.

Os impasses da organização também podem ser observados por meio do mapa gerado a partir das respostas da entrevista, pelo software MAXQDA, como mostra a figura 3. Podemos observar pelas linhas mais grossas e pela quantidade do número de frequência, que as partes mais importantes se concentram em: Histórico de falhas e vulnerabilidades da organização, Controle de dispositivos físicos de armazenamento de dados e Gerenciamento e plano de controle. Com isso, a empresa poderá mapear áreas mais críticas que necessitam de maiores cuidados, para então melhorar a segurança.

**5.7 Matriz SWOT**

A Análise SWOT (forças, fraquezas, oportunidades e ameaças) é uma ferramenta utilizada para fazer análise de cenário (ou análise de ambiente), sendo usado como base para gestão e planejamento estratégico de uma corporação ou empresa, mas podendo, devido a sua simplicidade, ser utilizada para qualquer tipo de análise de cenário.

Estas análises de cenários se dividem em ambiente interno (Forças e Fraquezas) e ambiente externo (Oportunidades e Ameaças). As forças e fraquezas são determinadas pela posição atual e se relacionam, quase sempre, a fatores internos. Já as oportunidades e ameaças são antecipações do futuro e estão relacionadas a fatores externos. O ambiente interno pode ser controlado pelo individuo, uma vez que ele é resultado das estratégias de atuação definidas por ele mesmo. Desta forma, durante a análise, quando for percebido um ponto forte, ele deve ser ressaltado ao máximo; e quando for percebido um ponto fraco, o indivíduo deve agir para controlá-lo ou, pelo menos, minimizar seu efeito. (FERREIRA, Douglas, 2009).

**Figura 4 – Análise SWOT da empresa**

|  |  |  |
| --- | --- | --- |
|  | **Favorável** | **Desfavorável** |
| **Interno** | **Forças** | **Fraquezas** |
| * Vontade e disposição de melhorar. * Disponibilidade de aplicação de novos processos. * Aceitação dos colaboradores. * Disponibilidade de investimento em treinamentos. | * Vulnerabilidade dos colaboradores. * Pouco controle de segurança da informação. * Pouco gerenciamento de riscos a informação. * Métodos para a continuidade do negócio. * Controlo de incidentes. |
| **Externo** | **Oportunidades** | **Ameaças** |
| * Estruturação de política de segurança da informação. * Criação de auditorias. * Gestão de riscos e continuidade do negócio. * Capacitação dos colaboradores em uso da TI. | * Incidentes. * Transferência indevida de informações; * Exploração indevidada de dados de forma passiva e ativa. * Uso de dispositivos de armazenamento de dados indevidos. |

Fonte: Elaboração própria, 2019.

**6 A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

Dado o objetivo final do estudo de caso, abaixo está contida a política de segurança da informação inicial da organização.

Leia com atenção e procure segui-la.

**Introdução:**

A Tecnologia da Informação, está cada vez mais presente nas empresas, mudando radicalmente os hábitos e a maneira de comunicação, sendo de vital importância a definição de normas de segurança que visem disciplinar o uso da tecnologia da informação. Baseando-se nas normas ISO/IEC 27.001 e NBR ISO/IEC 27.002 foi a Política de Segurança da Informação – PSI inicial.

**Objetivo:** Definir responsabilidades e orientar a conduta dos usuários das tecnologias da empresa, visando a continuidade dos negócios através da confidencialidade, da integridade e da disponibilidade das informações.

**Aplicação:**

A presente PSI aplica-se a todos os usuários de TI e a qualquer colaborador ou pessoa que utilize de informações da empresa ou dos seus clientes.

**Princípios:**

A informação produzida ou recebida como resultado de sua atividade profissional pertence à empresa. A segurança da informação depende de pessoas comprometidas, processos gerenciais de controle e sistemas de segurança da informação. É necessário a postura ética daqueles que utilizam as informações, caso a divulgação indevida serão acionados os poderes judiciais.

**Responsabilidades:**

A empresa entende que o sistema de segurança da informação somente será eficaz com o comprometimento de TODOS!

## **Usuários**

* Respeitar esta Política de Segurança da Informação
* Responder pela guarda e proteção dos recursos computacionais colocados á sua disposição para o trabalho;
* Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
* Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software.
* Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc;
* Assegurar que as informações e dados de propriedade da empresa não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável hierárquico.
* Relatar para o seu responsável hierárquico e à Gerência de TI, o surgimento da necessidade de um novo software para suas atividades.
* Responder pelo prejuízo ou dano que vier a provocar a organização ou a terceiros, em decorrência da não obediência as diretrizes e normas aqui referidas.

## **Dos Responsáveis Hierárquicos:**

* Apoiar e zelar pelo cumprimento desta PSI, servindo como modelo de conduta para os colaboradores sob a sua gestão.
* Atribuir na fase de contratação e de formalização dos contratos individuais de trabalho, prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI.
* Autorizar o acesso e definir o perfil do usuário junto ao gestor de liberações da área de TI,
* Autorizar as mudanças no perfil do usuário junto ao gestor de liberações da área de TI,
* Educar os usuários sobre os princípios e procedimentos de Segurança da Informação,
* Notificar imediatamente ao gestor de liberações da área de TI quaisquer vulnerabilidades e ameaças a quebra de segurança;
* Assegurar treinamento para o uso correto dos recursos computacionais e sistemas de informação;
* Advertir formalmente o usuário e aplicar sanções cabíveis quando este violar os princípios ou procedimentos de segurança, relatando imediatamente o fato ao gestor de liberações da área de TI.
* Obter aprovação técnica do gestor de liberações da área de TI antes de solicitar a compra de hardware, software ou serviços de informática.
* Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

## **Área de TI**

* Configurar os equipamentos e sistemas para cumprir os requerimentos desta PSI,
* Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.
* Restringir a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
* Garantir segurança do acesso e manter evidências que permitam a rastreabilidade para auditoria ou investigação.
* Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.
* Administrar, proteger e testar as cópias de segurança dos programas e dados ao negócio da empresa.
* Gerenciar o descarte de informações,
* Garantir que as informações de um usuário sejam removidas antes do descarte ou mudança de usuário.
* Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
* Atribuir contas e senhas identificáveis a pessoa física para uso de computadores, sistemas, bases de dados e qualquer outro ativo de informação.
* Proteger todos os ativos de informação da empresa contra códigos maliciosos e ou vírus.
* Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento dentro da empresa.
* Realizar inspeções periódicas de configurações técnicas e análise de riscos.
* Gerenciar o uso, manuseio e guarda de assinaturas e certificados digitais.
* Garantir assim que solicitado o bloqueio de acesso de usuários por motivo de desligamento da empresa,
* Propor as metodologias sistemas e processos específicos que visem aumentar a segurança da informação,
* Promover a conscientização dos colaboradores em relação a relevância da segurança da informação,
* Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.
* Implantar sistemas de monitoramento nas estações de trabalho, servidores, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede ‒ a informação gerada por esses sistemas pode ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
* Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

**Acesso:**

* Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade será dos usuários que dele se utilizarem. Se for identificada solicitação do gestor para uso compartilhado ele deverá ser responsabilizado.
* Os usuários deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo).
* É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.
* As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), não devem ser baseadas em informações pessoais, como próprio nome, familiares, nascimento, endereço, placa de veículo, nome da empresa, e ou não devem ser constituídas de combinações óbvias, como, “123456789”, data de aniverssário, entre outras.
* Os usuários devem proceder a troca de senha, caso suspeitem de quebra por terceiros.
* O Login e Senha devem ser imediatamente bloqueados quando se tornarem desnecessários.
* Tentativa de violação e burla de senhas de acesso, criptografia ou identificação biométrica se identificada será alvo de ação disciplinar.

**Recursos Computacionais:**

* Os recursos de TI alocados pela empresa aos seus usuários são destinados exclusivamente às atividades relacionadas ao trabalho.
* É proibida a intervenção do usuário para manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, bem como a transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros.

**Tela e Mesa Limpas:**

* O usuário deve cuidar para que papéis, mídias e imagens nos monitores não fiquem expostos ao acesso não autorizado.
* Os computadores deverão ser bloqueados por senha quando não estiverem sendo utilizados.

**Antivírus:**

* A empresa disponibiliza software corporativo de antivírus instalado para todos os usuários.
* A área de TI da organização não recomenda que o usuário remova ou altere as configurações do antivírus a fim de não comprometer a segurança que o fabricante do software proporciona.
* As checagens periódicas do disco rígido, HD, da estação de trabalho será programada para execução periódica.

**Armazenamento de Arquivos:**

* Todos os arquivos contidos nos servidores de rede ou nas estações de trabalho dos usuários devem ser exclusivamente de interesse empresa.
* É proibida a criação de pastas pessoais nos servidores de rede.
* O acesso às pastas departamentais nos servidores de rede exige autorização do responsável hierárquico e do gestor de liberações para o controle do acesso de cada usuário.
* A partir da implantação desta Política, todos os arquivos que não sejam do interesse da empresa deverão ser excluídos dos equipamentos para evitar problemas futuros.
* Proibido o uso de dispositovos de armazenamento e transferências de arquivos, tais como: HD portátil, pendrives, entre outros.

**Salvaguarda de Arquivos:**

* Compete ao gestor de continuidade da área TI criar e manter cópias de segurança (backups) apenas dos dados armazenados nos servidores de rede;
* Os usuários devem manter obrigatoriamente os documentos, planilhas, emails, apresentações, desenhos, e outros dados críticos da empresa, nas pastas departamentais dos servidores de rede;
* São de responsabilidade exclusiva do usuário a cópia de segurança (backup) e a guarda dos dados gravados da sua estação local de trabalho.

**Uso da Internet:**

* A Internet será para viabilizar a busca de informações e agilizar determinados processos da organização, sendo proibido o uso pessoal durante o horário de trabalho, podendo haver exceções.
* O uso indevido do acesso à Internet é de inteira responsabilidade do usuário, podendo o mesmo ser responsabilizado legalmente pelos danos causados.

**Considerações Finais:**

* Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da empresa. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.
* Todas as práticas que ameacem à segurança da informação serão tratadas com a aplicação de ações disciplinares, desde uma advertência verbal até decisões mais acentuadas, dado o grau do prejuízo para organização.

**8 CONSIDERAÇÕES FINAIS**

A informação é um ativo relevante que pode trazer grandes impactos para as organizações, e neste cenário de constantes evoluções da tecnologia da informação, os gestores devem buscar sempre aperfeiçoar seus mecanismos de segurança da informação, visando alcançar seus objetivos e proteger suas organizações de riscos, ameaças e vulnerabilidades. Devido à relevância do assunto, a presente pesquisa teve como objetivo principal identificar as dificuldades da organização e se dispõe de políticas de segurança da informação, por meio da coleta e análise de dados.

Após a análise dos dados foi possível identificar os caminhos a serem seguidos pela organização, em conjunto com seus colaboradores, para aprimorar seus processos de segurança das informações. Deste modo conclui-se que a política de segurança da informação e toda a transparência dos dados levantadospor este estudo de caso, disponibilizados para a empresa, o trabalho em conjunto para elaborar todos os processos foi efetivo para o crescimento da organização e dos alunos participantes deste trabalho.

**7 TRABALHOS FUTUROS**

A PSI proposta neste trabalho está sendo aplicada na filial juiz-forana da empresa. No futuro, pretende-se reavaliá-la, para aprimorá-la corrigindo possíveis problemas e adicionando novos itens para suprir de fato as necessidades da organização.

Além disto, será iniciada a implantação de processos auditorias para monitorar o cumprimento da PSI, processos de gerenciamento de riscos e incidente, além de análises na continuidade do negócio, elaborando um conjunto de planos de ação para garantir que os serviços essenciais sejam devidamente identificados e conservados após a ocorrência de um desastre, e até retornar à situação inicial, ou seja, normal de funcionamento da empresa, se baseando no ciclo PDCA, que seria planejar, fazer, verificar e agir. Contudo a implantação inicial em uma das filiais for bem sucedida, será implantada em outras filiais e finalmente na matriz.

# REFERÊNCIAS

BRASIL, T. C. U. **Boas Práticas em Segurança da Informação**. 4ª. ed. Brasília, **TCU**, 2012.

FONTES, Edison. **Políticas e Normas para Segurança da Informação**. Rio de Janeiro: Brasport, 2012.

FONTES, Edison. **Praticando a Segurança da Informação**. Rio de Janeiro: Brasport, 2008.

FONTES, Edison. **Segurança da Informação: o usuário faz a diferença**. São Paulo: Saraiva, 2006.

LYRA, Maurício Rocha. **Governança da Segurança da Informação**. Brasília: Edição do Autor, 2015.

PEIXOTO, Mário César Pintaudi. **Engenharia Social & Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

SELLTIZ, C. et al. Métodos de Pesquisa das Relações Sociais. São Paulo: Herder, 1967.

SERAFIM, I. F. Segurança da Informação na Administração Pública: o caso da controladoria geral do estado da paraíba. João Pessoa, 2017. Disponível em: <<https://repositorio.ufpb.br/jspui/bitstream/123456789/1853/1/IFS29082017.pdf>>. Acesso em: 27 mar. 2019.

SOUZA, J. G. S. Análise de Tratamento da Segurança da Informação na Gestão de Riscos da Governança de Tecnologia da Informação de um Instituição de Ensino Público Federal. São Paulo, 2017. Disponível em: <<http://www.portal.cps.sp.gov.br/pos-graduacao/trabalhos-academicos/dissertacoes/gestao-e-tecnologia-em-sistemas-produtivos/2017/jackson-gomes-soares.pdf>>. Acesso em: 27 mar. 2019.

MPSP, Manual de Gestão de Projetos. São Paulo, 2017. Disponível em:<http://www.mpsp.mp.br/portal/page/portal/Centro_de_Gestao_Estrategica/ManualGestaoProjetos.pdf> Acesso em: 09 nov. 2019.

FERREIRA, Douglas. Análise SWOT. 29 jun. 2009. Disponível em: < <http://coachingsp.wordpress.com/2009/06/29/ferramentas-de-coaching-analise-swot/>>. Acesso em: 09 nov. 2019.

MAXQDA 12, Guia de Introdução. São Paulo, 2017. Disponível em: < <https://www.maxqda.com/wp/wp-content/uploads/sites/2/Getting-Started-Guide-MAXQDA12-ptbr.pdf>>. Acesso em: 09 nov. 2019.

BSI. Information Security Management. Singapore, 2019. Disponível em:<https://www.bsigroup.com/globalassets/Documents/iso-27001/resources/BSI-ISOIEC27001-Product-Guide-UK-EN.pdf>.> Acesso em 10 nov. 2019.

ABNT NBR ISO/IEC 27002. Tecnologia da informação - Técnicas de segurança - Código de prática para gestão da segurança da informação. Rio de Janeiro, 2005. Disponível em: <http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf>>. Acesso em 10 nov. 2019.

GOODRICH, Michael T.; TAMASSIA, Roberto. Introdução à segurança de computadores. Porto Alegre: Bookman, 2013.

SÊMOLA, Marcos. Gestão da segurança da informação: uma visão executiva. 2. Ed. Rio de Janeiro: Elsevier, 2014.