ANÁLISE DE VULNERABILIDADES NA INFRAESTRUTURA DA TECNOLOGIA DA INFORMAÇÃO DE UMA EMPRESA DO SETOR DE MATERIAIS DE CONSTRUÇÃO

VULNERABILITY ANALYSIS OF THE INFORMATION TECHNOLOGY INFRASTRUCTURE OF A COMPANY IN THE CONSTRUCTION MATERIALS SECTOR

Thais da Vera Sousa Brito
Fatec Santana de Parnaíba
thais.brito2@fatec.sp.gov.br

Wilson Otávio de Santos Junior
Fatec Santana de Parnaíba
thais.sousa2823@gmail.com

Irapuan Glória Junior
Fatec Santana de Parnaíba
ijunior@ndsgn.com.br

Resumo

O presente artigo analisa as vulnerabilidades existentes em uma empresa do setor de materiais de construção com o objetivo de gerar recomendações de Segurança da Informação na infraestrutura da tecnologia da informação analisada. A pesquisa utilizou a metodologia de estudo de caso único, em que foram feitas análises baseadas em dados coletados através de uma entrevista com os funcionários para localizar as vulnerabilidades. Após a análise foram identificados diversos pontos que necessitavam de melhorias e foram feitas dez recomendações envolvendo a infraestrutura física e lógica da rede, prevenção contra *Ransomware* e Segurança da Informação. A contribuição acadêmica inclui evidenciar as formas de vulnerabilidades que podem ser identificadas em empresas de pequeno porte, principalmente empresas locais. A contribuição para a prática é informar as empresas e os principais envolvidos sobre a relevância da segurança da informação e a necessidade de corrigir as vulnerabilidades.

Palavras-chave: Segurança da Informação, Infraestrutura de tecnologia da informação, *Ransomware*, Materiais de Construção.

Abstract

The present article analyzes the existing vulnerabilities in a company in the construction materials sector with the aim of generating Information Security recommendations for the analyzed information technology infrastructure. The research utilized a single case study methodology, where analyses were based on data collected through interviews with employees to identify vulnerabilities. After the analysis, several areas needing improvement

were identified, and ten recommendations were made involving the physical and logical network infrastructure, ransomware prevention, and information security. The academic contribution includes highlighting the types of vulnerabilities that can be identified in small businesses, particularly local companies. The practical contribution is to inform companies and key stakeholders about the relevance of information security and the need to address vulnerabilities.

***Keywords**: Information Security, Information Technology Infrastructure, Ransomware, Building Materials.*

1. Introdução

Com a utilização da Tecnologia da Informação (TI), as empresas vivem atualmente um cenário em que a era da informação está completamente vinculada as rotinas das operações, em que através da propagação em larga escala da TI em nível global e o avanço tecnológico cada vez mais acelerado, as empresas tornaram-se mais suscetíveis a possíveis crimes cibernéticos (LIMA; FERREIRA; PEIXOTO, 2022).

O avanço tecnológico traz consigo muitos benefícios, como: modernidade, agilidade, competitividade e inovação, mas por outro, as empresas tornaram-se mais vulneráveis, comprometendo a segurança das informações. Dentre as grandes ameaças cibernéticas que se aproveitam das vulnerabilidades das empresas se destaca o *Ransomware*, um tipo de *malware* que infecta o sistema, criptografa os dados e exige um resgate por aquelas informações (VENTURA; MARTINS, 2022).

A segurança da informação se tornou um fator primordial de sucesso nas organizações e contribui para a continuidade dos negócios independe do ramo das organizações (SILVA; SOUSA; GLÓRIA JÚNIOR, 2023). Por essa razão, é importante que as empresas estejam atentas à segurança da informação, em prol de proteger seus ativos que é tudo que gera valor para empresa. Isso incluí as organizações do setor varejista de materiais de construção, um dos pilares fundamentais da economia brasileira que apresenta um crescimento contínuo ao longo dos anos (ABECIP, 2023).

Assim, é necessário que a empresa mantenha um monitoramento contínuo da infraestrutura TI, a fim de detectar antecipadamente possíveis vulnerabilidade e a ataque ou até mesmo reduzir os impactos (SANTOS, 2023).

Diante disso, a questão de pesquisa é: "Quais são as vulnerabilidades na infraestrutura de TI no ambiente organizacional de uma empresa no setor de materiais de

construção?". Os objetivos são: (1) Identificar o ambiente de TI da empresa Alpha; e (2) Apresentar sugestões de melhorias na segurança da informação da Empresa Alpha.

2. Referencial Teórico

2.1. Segurança da informação

Diante do cenário que vivenciamos atualmente, em que a informação é um ativo valioso para as empresas, em que se tornou crucial sua preservação e proteção, de forma que sua divulgação ocorra somente de acordo com os interesses da empresa (VENTURA; MARTINS, 2022).

Nesse contexto a Segurança da Informação (SegInfo), tornou-se essencial, uma vez que busca garantir a proteção da informação contra quaisquer tipos de ameaça com intuito de garantir a sobrevivência dos negócios e a otimização do retorno sobre os investimentos (NASCIMENTO; GLÓRIA JÚNIOR, 2023).

Visando criar um ambiente de trabalho com SegInfo é necessário que a empresa adote os três pilares da informação conhecidos como Tríade CIA: confidencialidade, integridade e disponibilidade (LIMA; FERREIRA; PEIXOTO, 2022). Estes elementos estão relacionados diretamente com a informação e devem ser aplicados na prática como referência na busca de garantir a segurança da informação, esses aspectos foram introduzidos pela norma ISO 27000, que trata sobre a SegInfo (GOUVEIA, 2023)

A confidencialidade está relacionada com o fato de garantir a proteção da informação contra possíveis acessos não autorizados, restringindo o acesso para apenas indivíduos permitidos (NASCIMENTO; GLÓRIA JÚNIOR, 2023). Sendo assim, a confidencialidade é qualidade de prevenir com intuito de impedir exposições e o acesso indevido a informação, evitando seu comprometimento (GOUVEIA, 2023).

A integridade é associada com certificar que a informação esteja preservada de forma original, sem quaisquer tipos de alteração ou corrupção dos seus dados, mantendo-se intacta conforme gerada pelo seu criador (NASCIMENTO; GLÓRIA JÚNIOR, 2023).

A disponibilidade visa assegurar que a informação esteja acessível ao sistemas, sem nenhum tipo de interferências ou bloqueios de maneira que esteja no formato necessário para ser compreendida seguindo os critério de confidencialidade e integridade (GOUVEIA, 2023).

BB SegInfo abrange a proteção dos dados e informações, sendo implementada tanto por indivíduos quanto por organizações, independente se for no setor privado ou público (LIMA; FERREIRA; PEIXOTO, 2022). Como resultado, a segurança da informação passou a ser uma prática extremamente adotadas nas organizações, uma vez que ela engloba as proteções contra ameaças internas e externas, protegendo contra qualquer possível quebra de privacidade e violação da informação (GOUVEIA, 2023).

Dentro desse aspecto, pode-se relacionar a SegInfo com a elaboração de um documento que estabeleça medidas a serem adotadas para preservar as informações e os sistemas de informações (COSTA; GALVÃO, 2023). Esse documento é conhecido como Políticas de Segurança da Informação (PSI), em que é conjunto de regras e princípios que que devem ser adotados pela organização, por isso esse processo envolve a integração eficaz de processos, procedimentos, controles, melhores práticas e tecnologias, proporcionando uma direção para os procedimentos que devem ser executados pela empresa através da Gestão da Segurança da Informação. (LIMA; FERREIRA; PEIXOTO, 2022).

Dentro desse aspecto, o PSI é baseado em normas que fornecem diretrizes que contribuem para gestão da segurança da informação. Essas políticas devem ser implementas e atualizadas em conformidade, como é caso da Lei Geral de Proteção de Dados em vigor no Brasil (LIMA; FERREIRA; PEIXOTO, 2022).

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei de número 13.709, sancionada em 14 de agosto de 2018 surgiu com a finalidade de regulamentar o tratamento de dados pessoais tanto em contextos digitais quanto físicos, com o intuito de preservar os direitos fundamentais de liberdade e privacidade. Com objetivo de assegurar o cumprimento das normas estabelecidas a LGPD possui um conjunto de sanções em caso de violação e a utilização de medidas corretivas (BARBOSA et al., 2021). Desta forma a lei elenca os direitos e obrigações das empresas para a regularização da proteção e segurança dos dados.

Nesse sentido, é importante salientar que com o objetivo de a empresa promover uma gestão eficiente e garantir a proteção de dados estratégicos assim preservando os valores dessas informações para a organização é necessário adotar as normas de SegInfo que estabelecem regras, normas e orientações a serem seguida pelas organizações com objetivo de garantir a confidencialidade, integridade e disponibilidade dos dados, contribuindo também para estabilidade e se segurança da gestão no âmbito empresarial (VENTURA;

MARTINS, 2022).

Pode-se observar um conjunto de boas práticas acerca da segurança da informação na Norma Internacional ISO 27000, que aborda padrões de qualidade para o gerenciamento da SI (ROMANO; ARMELIN, 2023).

A família da ISO 27.000 engloba a estrutura organizacional como um todo, contemplando processos, recursos, políticas, responsabilidades, prática, procedimentos e atividades de planejamento. Estabelecem critérios para um Sistema de Gestão da Segurança da Informação (SGSI) apresentando o mesmo como parte integrante do sistema da gestão global da empresa, considerando os riscos para estabelecer, executar, operar, vigiar, examinar, conservar e aprimorar a segurança da informação (VENTURA; MARTINS, 2022).

Por esta razão pode-se destacar que a gestão da informação é regida por normas e princípios de segurança com a finalidade de proteger a informação evitar qualquer possível corrupção na Tríade CIA (LIMA; FERREIRA; PEIXOTO, 2022).

Nesse contexto, é importante ressaltar que, com o objetivo de garantir a confidencialidade, integridade e a disponibilidade, é necessário que as empresas estejam atentas às vulnerabilidades, pois são diversos os pontos que tornam as empresas brasileiras suscetíveis a possíveis ataques, como: falta de investimentos em segurança da informação, falta de conscientização dos funcionários e falta de atualização dos sistemas (SANTOS, 2023).

Para lidar com as possíveis ameaças, é necessário primordialmente reconhecer quais são os pontos de vulnerabilidade que afetam as empresas. Muitas das vezes, a própria rede interna pode estar corrompida, facilitando possíveis invasões em bancos de dados, sistemas e até mesmo elementos básicos, como por exemplo, as vulnerabilidades em *hardware* e *software*, que acontecem devido à falta de substituição e atualização baseado em aspectos técnicos e de qualidade, uma vez que a tecnologia utilizada deve suprir as necessidades da organização. Um outro exemplo é o incorreto armazenamento de cópias de segurança (*Backup*), em locais que estão mais suscetíveis a possíveis invasões, possibilitando danos e roubos no sistema (VENTURA; MARTINS, 2022).

É importante que empresas adotem ações preventivas com intuito de evitar ataques cibernéticos como a utilização de softwares de segurança, antivírus e *firewalls*. No entanto, a conscientização dos usuários é primordial, uma vez que as ações do elo humano são essenciais para a proteção dos sistemas (SANTOS, 2023).

Diante disso, compreende-se que o fator humano representa uma vulnerabilidade dentro das organizações e mesmo que as empresas invistam fortemente na proteção das informações, os funcionários, por falta de conscientização ou até mesmo por má intenção podem causar grandes danos através da violação da segurança, como o compartilhamento de senhas, perda de dispositivos que contém algum tipo de dados sensíveis e até mesmo por meio de abertura de *e-mails* maliciosos. Sendo assim, mesmo que se invista em tecnologias de alto padrão na segurança da informação, o fator humano determina o fracasso ou sucesso da proteção dos dados (KANAGUSKU; GASETA, 2023).

Sendo assim, é necessário a conscientização e educação dos usuários para reduzir os riscos, de forma que se conheça as boas práticas, como: criar senhas complexas, evitar clicar em links suspeitos e manter os dispositivos atualizados com as correções de segurança. Além disso, a proteção dos dados deve ser uma prioridade contínua, utilizando ferramentas de criptografia e adotando as medidas determinadas no PCI (SANTOS, 2023).

2.2. Ransomware

As empresas se tornam mais vulneráveis a programas maliciosos (*malwares*) com o uso crescente da Internet, que cada vez mais tornam-se mais sofisticados e, dentro do universo do crime cibernéticos, o *Ransomware* é um programa mal-intencionado que pode causar grandes danos as organizações (CANDIDO; FLORIAN; BORGES, 2023).

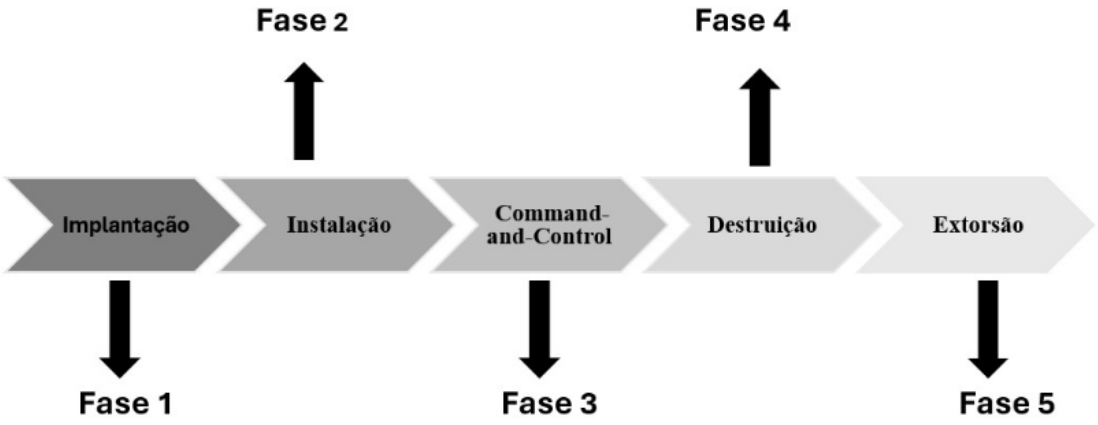
O *Ransomware* é considerado um malware que possuí alto nível de infecção com o intuito de extorquir digitalmente as vítimas, fazendo com que elas realizem um pagamento, que normalmente feito através de moeda virtual como o *bitcoin. P*or esta razão, é um dos tipos de *malwares* mais utilizados, uma vez que o objetivo é o retorno financeiro para os criminosos (FILHO; FREITAS, 2023).

O conceito de *Ransomware* está ligada com a origem da palavra inglesa *Ransom* que significa resgate, em que os criminosos injetam nos computadores um software mal-intencionado sem consentimento (CANDIDO; FLORIAN; BORGES, 2023).

Em 1989, desenvolvido por Joseph Popp, surgiu o primeiro *Ransomware*, que foi nomeado como AIDS. Após infectar o sistema, o *malware* possibilitava reiniciar o sistema por noventa vezes, ocultando os diretórios e demonstrando a criptografia de arquivo (CANDIDO; FLORIAN; BORGES, 2023). Por se tratar de um *malware*, os *Ransomwares*, mesmo sendo criados a alguns anos, continuam evoluindo e acompanhando o surgimento de novas tecnologias (FILHO; FREITAS, 2023).

Os *Ransomwares* são distribuídos normalmente através de *e-mails* por meio de táticas de engenharia social, induzindo os usuários a realizarem os downloads de arquivos com a presença do programa malicioso por meio de estratégias de convencimento, como a utilização desses e-mails falsos como se fossem de empresas verídicas, pessoas atreladas a corporação que trabalha ou algum site que o usuário possa ter algum tipo de relação (SILVA; GLÓRIA JÚNIOR, 2023).

Figura 1: Etapas do *Ransomware*



Fonte: Baseado em Pimentel (2023).

Diante disso, os ataques direcionados de *Ransomware* seguem um modelo, distribuídos em 5 fases conforme a Figura 1: Implantação (Fase 1) distribuição dos códigos infecciosos, que acontece recebimento de *e-mail* com o código malicioso; Instalação (Fase 2) após a instalação da carga com os códigos, os elementos contidos são executados automaticamente buscando controlar a máquina remotamente; *Command-and-Control* (Fase 3) acontece a partir do momento que o *malware* se conecta ao servidor e começa executar instruções; Destruição (Fase 4): Ocorre a criptografia dos arquivos e exclusão das cópias do sistema; Extorsão (Fase 5): solicitação de resgate (PIMENTEL; CABRERA; FORTE, 2021).

Os *Ransomwares* são divididos em categorias, baseado em suas características e a forma de agir, entre algumas das principais está o *Crypto Ransomware* (PIMENTEL; CABRERA; FORTE, 2021), *Disk Coder* (SILVA; GLÓRIA JÚNIOR, 2023), *Locker Ransomware* (KASPERSKY, 2023) e *Pin Locker* (SILVA; GLÓRIA JÚNIOR, 2023).

O *Crypto Ransomware* tem como objetivo criptografar os dados disponíveis do computador, fazendo com que o usuário não consiga acessá-los e como muitos não realizam *backups* frequentes, ficam sujeitos a extorsão dos atacantes com base na importância dos arquivos afetados. Nesse tipo de *Ransomware*, um atributo importante é que a extração do programa malicioso do sistema operacional não restabelece os documentos afetados (PIMENTEL; CABRERA; FORTE, 2021).

Uma outra categoria é o *Disk Coder* que atua de forma em que criptografa o disco da vítima, bloqueando o acesso aos dados e um ponto crucial é que esse tipo tem capacidade de se espalhar pela rede, podendo comprometer os outros computadores conectados.

O *Locker Ransomware* tem por padrão realizar o bloqueio total do acesso do usuário ao sistema, atuando como um software malicioso que causa bloqueio das funções básicas do computador, como acessar a página inicial do computador ou tentar fazer o uso do mouse (KASPERSKY, 2023).

Diferentemente, o *Pin Locker* atua de forma que altera os códigos de acesso do usuário, bloqueando a tela do usuário através da utilização de um PIN (SILVA; GLÓRIA JÚNIOR, 2023).

Diante disso, é importante que as empresas e os usuário sigam a evolução dos crimes cibernéticos afim de mitigar as possíveis vulnerabilidades através de medidas como: realização de *backups* de arquivos importantes de forma periódica; utilização de antivírus para combate de *malware*; manter os *softwares* atualizados; tomar precauções com relação a links, para não clicar sem ter a certeza de ser autênticos; não realizar downloads de arquivos executáveis sem a certeza de serem autênticos e em caso de arquivos suspeitos desligar o computador e a internet (FILHO; FREITAS, 2023).

Além disso, é necessário que as empresas invistam em conscientização e prevenção para os usuários, de forma a ter profissionais especializados em segurança da informação é crucial para entender as novas variantes de *Ransomware*, mesmo após a mitigação da

ameaça, o *Ransomware* pode causar danos adicionais, como vazamento de dados (NASCIMENTO; GLÓRIA JÚNIOR, 2023).

2.2 Setor de Materiais de Construção

O setor de materiais de construção, no Brasil, é marcado por uma constante transformação e evolução, composto por pequenas lojas de bairros, grandes varejistas, redes internacionais, redes associativas e centrais de negócios no segmento de loja (COGNATIS, 2023).

Esse tipo de setor tem natureza comercial, com foco na venda de ferramentas, objetos e matérias primas necessárias para construções e mudanças de casas, apartamentos, edifícios residenciais ou voltados para área de comércio, sendo assim, é composto pela comercialização de materiais básicos como blocos, telhados e concretos e a parte de acabamento mais refinado como lâmpadas, fios, tintas, pisos e chuveiros, são vendidos pela indústria de materiais de construção (SEBRAE, 2023).

A indústria de materiais de construção, representa 18,3% do PIB da cadeia produtiva da construção que constitui 6,2% do PIB brasileiro, faturando aproximadamente 287 bilhões de reais por ano, empregando 759 mil pessoas em empregos diretos formais, rendendo anualmente 65,4 bilhões em arrecadação tributária (ABRAMAT, 2022).

Além disso, no Brasil existem 152 mil lojas de materiais de construção distribuídas pelo país, sendo no Sudeste (46,3%), no Norte (19,5%), no Sul (19%), Centro-Oeste (9,5%) e 5,7% no Nordeste (5,7%) (ANAMACO, 2024).

Uma característica fundamental da indústria de materiais de construção é sua estrutura de abastecimento, que geralmente opera de duas maneiras distintas, em que por um lado, a indústria fornece diretamente às construtoras envolvidas na construção e a outra forma, está relacionada com os varejistas, que são abastecidos, sendo que os de maior porte são atendidos diretamente pela indústria, enquanto os demais, em geral, são abastecidos por meio de distribuidores e atacadistas (COGNATIS, 2023).

Outra característica desse setor é que as lojas de materiais de construção são classificadas por seu porte: (1) As pequenas e médias têm como base os materiais básicos como cal, cimento, madeira, pregos, material elétrico e iluminação; e (2) As grandes são

consideradas generalistas e possuem uma gama de opção colaborando até mesmo com a tomada de decisões e surgimento de novas ideias para a construção ou reforma, deixando o comprador diante de uma maior diversidade de produtos até mesmo peças de decoração e eletrodomésticos (SEBRAE, 2023).

Por fim, o setor de materiais de construção se destaca como um segmento em ascensão e com grandes possibilidades de crescimento, cercado por novas tendências contribuindo para o aumento das vendas, além disso, o setor tem realizado investimentos em inovação tecnológica com soluções especializadas e na oferta de projetos mais eficientes utilizando materiais de qualidade superior e com alta durabilidade (FEBRAMAT, 2021).

3. Metodologia

O presente artigo adota uma abordagem metodológica de estudo de caso único (YIN, 2021), de natureza qualitativa (THEÓPHILO, 2023), pois o estudo baseia-se no funcionamento da tecnologia da informação da empresa Alpha que será analisada por meio de documentos e coleta de dados através de entrevistas (GIL, 2017). Após identificado o ambiente de Alpha, os dados adquiridos foram examinados, identificando as vulnerabilidades, para assim propor sugestões de mitigações para as ameaças encontradas. No Quadro 1, são apresentadas as características utilizadas durante a execução do estudo.

Quadro 1: Características do Estudo.

Item	Descrição	Autor(es)
Natureza	- Qualitativa	Gil (2021)
Metodologia	- Estudo de Caso Único	YIN (2021)
Coleta de Dados	- Entrevista	MARTHINS; TEÓPHILO (2023)
	- Análise Documental	MARTHINS; TEÓPHILO (2023)
Unidade de Análise	- Departamento de TI	

Fonte: Os Autores.

3.1 Processos Metodológicos

Para a construção deste estudo, foram realizadas as seguintes etapas:

Etapa 1 – Criação do Questionário: Com base no referencial teórico foi criado um questionário com intuito de identificar as possíveis vulnerabilidade dentro do ambiente da unidade de análise.

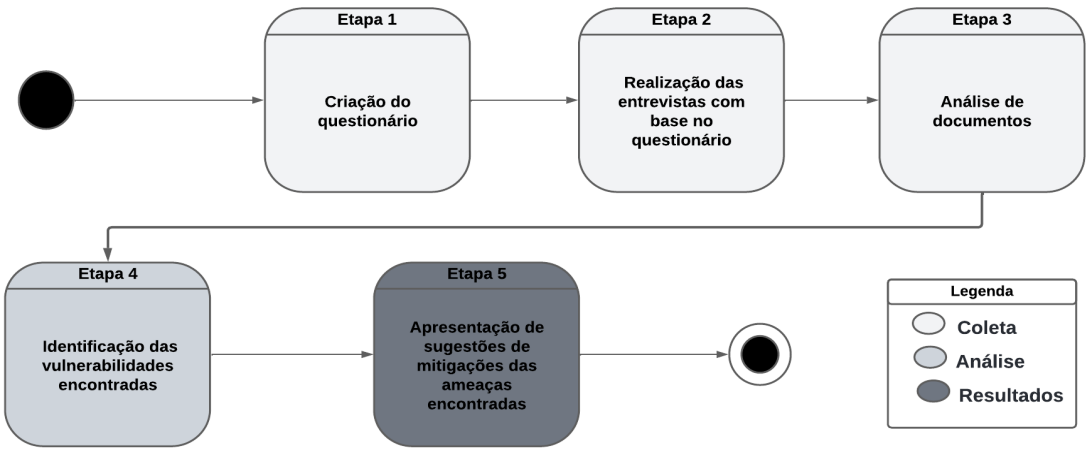
Etapa 2 – Realização das Entrevistas: Aplicação do questionário através de entrevista com o responsável de TI de Alpha.

Etapa 3 – Análise de Documentos: Após a entrevista foi realizada a transcrição das informações, gerando um relatório com os dados importantes para análise.

Etapa 4 – Identificação das Vulnerabilidades Encontradas: Análise dos dados levantados nos processos anteriores, listando as vulnerabilidades identificadas.

Etapa 5 – Apresentação de sugestões de mitigações das ameaças encontradas: Com base na análise da Etapa 4, foram criadas propostas de mitigações contra as vulnerabilidades encontradas.

Figura 4 – Procedimento Metodológico



Fonte: Os Autores

3.2 Objeto de Estudo

Alpha é uma empresa do setor varejista que atua no Estado de São Paulo com foco na comercialização de materiais de construção, possuindo mais de 30 funcionários. Além disso, a organização é enquadrada como uma Pequena e Média Empresa (PME) devido ao seu faturamento.

3.3 Questionário

Com base no referencial teórico foi criado um questionário para realização da entrevista para levamento das informações e posterior análise, conforme exposto na Tabela 1.

Tabela 1 – Referencial teórico e Questões

Referencial Teórico	Questões
A gestão eficiente da Segurança da Informação visa garantir a proteção de dados estratégicos assim preservando os valores dessas informações para a organização é necessário adotar as normas de SI (VENTURA; MARTINS, 2022).	Como a empresa aplica a proteção da informação, considerando a crescente importância?
A informação é um ativo valioso para as empresas, em que se tornou crucial sua preservação e proteção, de forma que sua divulgação ocorra somente de acordo com os interesses da empresa (VENTURA; MARTINS, 2022).	Como são gerenciados os acessos aos sistemas e dados da empresa?
As ações preventivas nas empresas adotem medidas preventivas com intuito de evitar ataques cibernéticos como a utilização de softwares de segurança, antivírus e firewalls (SANTOS, 2023)	A empresa realiza a utilização de programas de segurança e *firewall* para evitar ataques externos em sua infraestrutura?
As Políticas de Segurança da Informação são baseadas em normas que fornecem diretrizes que contribuem para gestão da segurança da informação (LIMA; FERREIRA; PEIXOTO, 2022).	Quais são as políticas e procedimentos para lidar com dispositivos de armazenamento externo (*pen drives*, discos rígidos externos)?
Para lidar com as possíveis ameaças é necessário primordialmente reconhecer quais são os pontos de vulnerabilidades que afetam as empresas (VENTURA; MARTINS, 2022).	A empresa realiza auditorias regulares de segurança para identificar possíveis vulnerabilidades nos sistemas e na rede?
O *Ransomware* tornou-se uma grandes ameaças as organizações e por isso faz-se necessário a utilização de mecanismos de defesas úteis para prevenção e reação ao *Ransomware* (FILHO; FREITAS, 2023).	Quais as medidas de proteção aos ataques de *Ransomware* a empresa implementou ou já possuí?

Referencial Teórico	Questões
As empresas e usuários devem sempre seguir a evolução da criminologia, aprimorando seus métodos protetivos (NASCIMENTO; GLÓRIA JÚNIOR, 2023)	A empresa realiza testes de simulação de ataques de *Ransomware* para avaliar a eficácia dos seus controles de segurança?
Dentre as grandes ameaças cibernéticas que se aproveitam das vulnerabilidades das empresas se destaca o *Ransomware*, um tipo de malware que infecta o sistema, criptografa os dados e exige um resgate por aquelas informações (VENTURA; MARTINS, 2022)	Quais são os procedimentos de resposta a incidentes que a empresa possui? A empresa possuí um plano de continuidade?
É de grande importância investir em conscientização e prevenção, ter profissionais da área de segurança da informação para realizar estudos e terem mais entendimento das novas variantes de *Ransomware* (NASCIMENTO; GLÓRIA JÚNIOR, 2023).	Existe uma política de conscientização e treinamento dos funcionários em relação à segurança cibernética?
As empresas investem em tecnologias de alto padrão na segurança da informação, mas o fator humano determina o fracasso ou sucesso da proteção dos dados (KANAGUSKU; GASETA, 2023).	A empresa utiliza alguma forma de análise de comportamento de usuários ou sistemas para detectar atividades suspeitas?

Fonte: Os Autores.

4. Análise e Interpretação dos Resultados

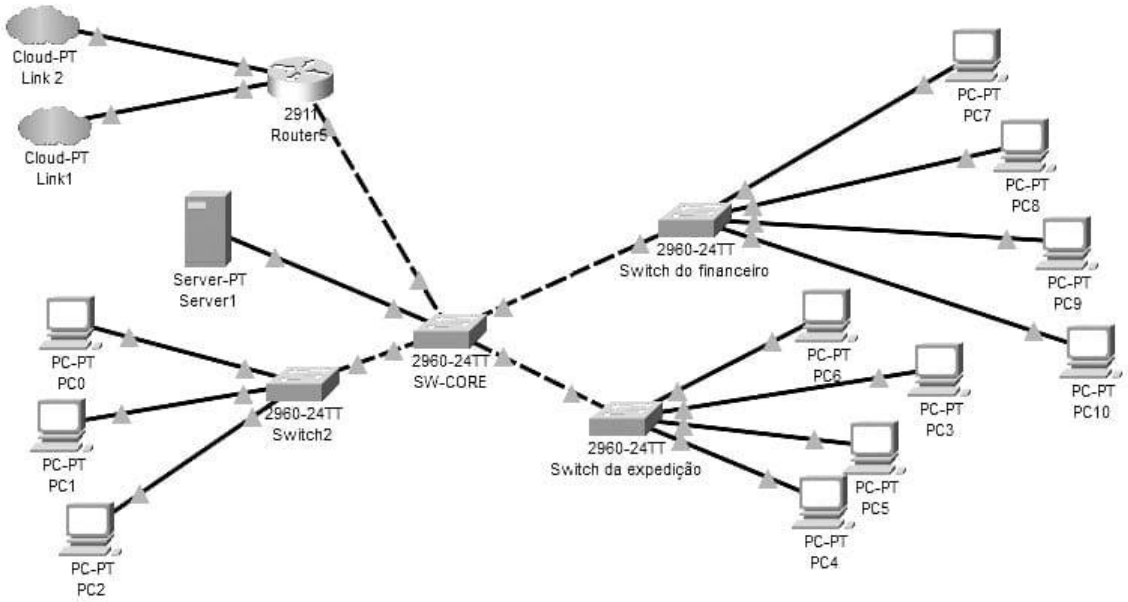
4.1. A Infraestrutura da Empresa

A infraestrutura de TI da empresa do setor de materiais carece de melhorias, uma vez que não possuí uma equipe interna de TI, conforme mencionado por R01: "A empresa possui uma empresa terceirizada responsável pelo TI que atua de forma remota e, quando necessário, diante de algum problema, faz a utilização do prestador...".

Outro fator está relacionado com a organização física que, segundo a descrição de R02, é composta por um servidor de arquivo *Linux*, que não possuí um local apropriado, pois o rack ainda não foi instalado. Além disso, há 5 switches sendo 1 switch central, 2 na área de vendas, 1 na expedição e 1 no administrativo. A empresa também possuí 16 máquinas clientes, sendo 4 delas do setor administrativo.

Dentro de sua infraestrutura, a empresa possuí dois links para todas as tarefas via Internet. No entanto, esse gerenciamento e revezamento ocorre manualmente, podendo afetar a eficiência operacional conforme afirmado por R02 que "…não é feita distribuição de tráfego da rede, não possuindo *load balancing*... A empresa possui dois links de rede, mas a operação é realizada de forma manual durante o dia." A Figura 5 demonstra o diagrama da rede da empresa elaborado conforme a entrevista realizada.

Figura 5: Diagrama de Rede



Fonte: Os Autores

Em relação aos programas de segurança há o pacote office versão 2019, *Windows 10 Home Single Language 22H2* nas máquinas clientes, mas a organização não faz a utilização de software de segurança para proteção conforme mencionado por R01: "A empresa não tem antivírus," e R02 destacou: "A empresa não utiliza antivírus, tem apenas um firewall simples e faz a utilização de um switch inteligente que realiza a entrega de pacotes para a máquina destino sem passar por todos os equipamentos...".

A análise das vulnerabilidades diagnosticadas na infraestrutura de TI da empresa revela possíveis vulnerabilidades nos procedimentos relacionados à segurança da informação, conforme mencionado por R01: "Apenas 3 funcionários têm acessos ao servidor da parte física, que é o próprio prestador e 2 funcionários da operação quando necessário" e acrescentado por R02, "... A empresa não possui uma política específica de proteção da informação, os funcionários do operacional recebem somente o login do sistema em particular utilizado para realização das vendas e no administrativo os funcionários possuem acesso ao sistema e aplicativos como: *NewStandard*, *Chrome*, Pacote office, *Team Viewer*, *AVG Secure Browser* e impressora".

Dentro desse cenário, o programa da AVG Secure Browser é um navegador gratuito que tem como objetivo não permitir o rastreamento do navegador e proteger a privacidade do usuário.

Um outro ponto essencial está relacionado com o fator da empresa não realizar nas auditorias de segurança, deixando a empresa exposta a diversos riscos cibernéticos conforme R01 apontou "A empresa não faz controle de segurança" e R02 confirmou que "Não são realizadas auditorias direcionadas para segurança da informação e não possui nenhuma aplicação da LGPD."

Uma outra consideração é que a empresa não possui uma política direcionada a utilização de *pendrives*, mesmo tendo a função bloqueada para utilização em alguns computadores, de acordo como foi respondido por R01: "A função está bloqueada, apenas um único computador que está liberado, mas não é utilizado durante a rotina" e confirmado por R02 "A empresa bloqueou a utilização de *pendrives*, apenas um único computador possuí que é do responsável pelo financeiro, mas também não existe nenhuma política para utilização.

A organização não possuí uma política direcionada para possíveis ataques de *Ransomware* e não realiza testes de simulação de acordo com R01 "... A empresa não realiza controles de *Ransomware*" e afirmado por R02: "A empresa não realiza testes de simulação de ataques de *Ransomware* e não sofreram nenhum ataque de *Ransomware"*. Nesse sentido, a empresa também não possuí um procedimento de respostas a incidentes e nenhum plano de continuidade conforme dito por R01 "A empresa não possuí nenhum procedimento relacionado" e confirmado por R02 "A empresa não possui procedimentos de resposta de incidentes e plano de continuidade."

Um outro levantamento efetuado é referente a falta de treinamento e conscientização em segurança cibernética, destacada por R01: "... Não possuem nenhum tipo de treinamento e os funcionários e não utilizam *e-mail*" e confirmado por R02 "…não existem políticas de conscientização e treinamento dos funcionários, eles não têm hábito de utilizar e-mail, mesmo sendo liberado a utilização."

4.2. Procedimentos de Segurança da Informação Existentes

Dentre os levantamentos realizados, foi diagnosticado que a empresa possui em suas práticas a realização de *backups* local três vezes ao dia conforme afirmado por R02 "... Os *backups* da empresa acontecem 3 vezes ao dia localmente". Essa frequência de *backup* auxilia na proteção dos dados contra perdas acidentais e falhas de sistema que possam comprometer a integridade das informações.

A realização de *backups* regulares é uma prática essencial para garantir a continuidade dos negócios e minimizar os danos em caso de incidentes que resultem na perda de dados. No entanto, é necessário que essa prática esteja integrada a um plano de recuperação de desastres assegurando que os *backups* sejam eficazes e possam ser restaurados quando necessário.

4.3. Principais Vulnerabilidades

A infraestrutura de TI da empresa do setor de materiais apresenta várias vulnerabilidades (Tabela 2) que comprometem sua segurança e eficiência operacionais.

A empresa não possui uma equipe interna de TI ou um técnico terceiro presencial, tendo que é dependente do suporte remoto (V01), podendo gerar a atrasos na resolução de problemas, prejudicando a agilidade e eficiência na resposta a incidentes.

A organização física e estrutura da rede (V02) da infraestrutura de TI não segue um padrão funcional de qualidade, podendo causar danos aos equipamentos e dificultar a manutenção. Além disso, a falta de *load balancing* para a distribuição de tráfego pode resultar em lentidão e interrupções na rede, afetando a eficiência das operações diárias.

Um outro aspecto importante, é que a empresa não utiliza antivírus e a falta da utilização do programa de segurança (V03) adicionado ao uso de um firewall básico expõem a infraestrutura a possíveis *malwares* e ataques cibernéticos, comprometendo a segurança dos sistemas e dados podendo afetar a continuidade dos negócios.

Conforme diagnosticado, a empresa não possui políticas específicas de proteção da informação (V04) e com a falta dessas políticas, a confidencialidade, integridade e disponibilidade dos dados estão em risco, aumentando a vulnerabilidade a acessos não

autorizados e perdas de informações.

Além disso, uma característica importante a ser evidenciada, com base nas respostas dos entrevistados, é o fato de que a empresa bloqueou a utilização de *pendrives* em todos os computadores, exceto no do responsável pelo financeiro, mas não existe uma política formal para a utilização desses dispositivos, então nota-se a falta de procedimentos para lidar com dispositivos de armazenamento externo (V05) oferecendo riscos de segurança, como a transferência não autorizada de dados sensíveis e até mesmo a introdução de um *malware*.

É importante também citar a questão da gestão inadequada de acessos (V06), podendo resultar em possíveis falhas como acessos não autorizados a dados sensíveis. uma vez que de acordo com a entrevista não existe um gerenciamento dos acessos dos funcionários e a empresa também não realiza auditorias de segurança. A ausência de auditorias de segurança (V07) impede a identificação e mitigação de vulnerabilidades, deixando a organização exposta a diversos riscos.

Um outro aspecto que expõe a empresa é o aumento do risco associados a segurança da informação é o fato da empresa não possuir políticas ou medidas para lidar com ataques de *Ransomware*. Apesar da empresa afirmar que nunca sofreu um ataque de *Ransomware*, a falta de mediadas contra *Ransomware* (V08) a deixa vulnerável.

A falta dessas medidas direcionadas para segurança da informação adicionados a ausência de plano de continuidade e resposta a incidentes (V09), faz com que empresa se torne vulnerável e não esteja preparada para uma resposta rápida e uma recuperação ágil sem prejudicar o desempenho do negócio podendo comprometer a estrutura da operação como todo.

Por último, a organização não tem em seu escopo políticas de conscientização e treinamento dos funcionários relacionados à segurança da informação, ficou claro durante a entrevista e a visita realizada que existe uma falta de treinamento e conscientização em segurança cibernética (V10). Diante disso, visando proteger a empresa, uma vez que está em constante crescimento, é necessário aplicar medidas de segurança.

Tabela 2 -Vulnerabilidades

#	Vulnerabilidade
V01	Dependência de Suporte Remoto
V02	Organização Física e Estrutura da Rede
V03	Ausência de Programas de Segurança
V04	Falta de Políticas de Proteção da Informação
V05	Falta de procedimentos para lidar com dispositivos de armazenamento externo
V06	Gestão Inadequada de Acessos
V07	Ausência de Auditorias de Segurança
V08	Falta de Medidas contra *Ransomware*
V09	Ausência De Plano De Continuidade E Resposta A Incidentes
V10	Falta De Treinamento E Conscientização Em Segurança Cibernética

Fonte: Autores, 2024.

4.4. Sugestões de Mitigações

Com base na infraestrutura de TI da empresa do setor de materiais foi proposto algumas sugestões de mitigações (Tabela 4) relacionado com as vulnerabilidades identificadas com objetivo de melhorar a segurança da informação colaborando para eficiência operacional e continuidade dos negócios.

Conforme diagnosticado na rede estrutural da empresa relacionando a dependência de suporte remoto (V01), é indicado que a organização tenha ao menos um profissional presencialmente de TI ligado diretamente à organização para resolução de problemas e possíveis incidentes que venham acontecer na empresa. Esse profissional também poderá auxiliar em todas as mitigações ligadas às demais vulnerabilidades

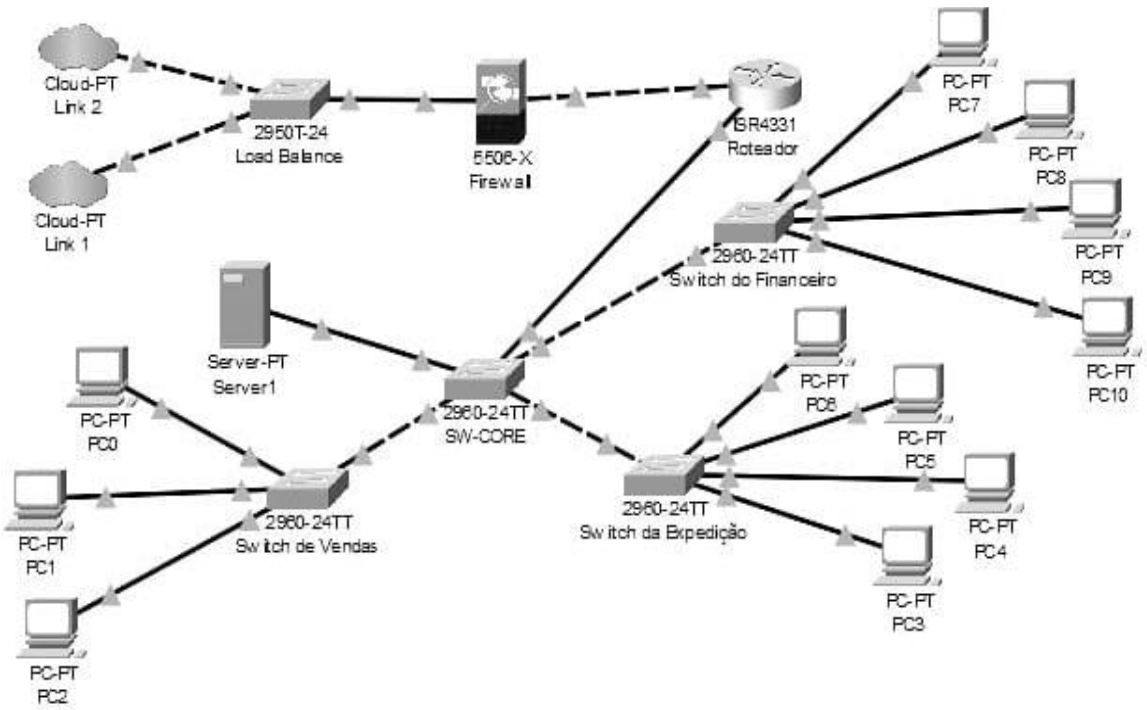
O profissional de TI será responsável por toda a organização física e estrutura de rede (V02) de TI, que de acordo com que foi identificado, é essencial a instalação de um rack para o servidor para evitar danos físicos ao equipamento e nas operações da empresa, ter um *load balance* também para distribuição de tráfego de rede (conforme identificado na

Figura 6), alterando os links de rede automaticamente sem ter que fazer isso manualmente, evitando assim interrupções nas operações.

Desse modo, como também foi identificado a ausência de programas de segurança (V03) tornando mais fácil a invasão aos sistemas, foi indicado a utilização de um antivírus nos terminais visando a proteção conforme a Tabela 3, em que são sugeridos cinco tipos de softwares de proteção com base em uma pesquisa realizada no mercado através dos sites organizacionais das empresas que oferecem antivírus para empresas de pequeno porte.

Também, é importante destacar que na rede da organização, é necessário a implantação de um *firewall* (conforme na figura 6) que melhor atenda o custo-benefício para a empresa, a fim de eliminar possíveis brechas de acessos não autorizados na rede corporativa.

Figura 6: Sugestão do Diagrama de Rede da Empresa



Fonte: Os Autores

Tabela 3: Sugestões de Antivírus

Antivírus	Característica	Investimento
Avira Antivirus Pro	O serviço bloqueia ameaças em tempo real, repara arquivos, facilita compras, navegação e acesso bancário seguros, bloqueia anúncios, protege a privacidade e realiza defesas no computador contra intrusos e ataques (AVIRA, 2024).	**R$47,99** (No Primeiro ano /Por usuário)
Kaspersky Small Office Security	O serviço oferece proteção contra ameaças em arquivos, *web* e *e-mail*, defesa contra *ransomware*, gerenciador de senhas e proteção de dispositivos móveis (KARPESKY, 2024).	**R$73,00** (Anual/Por usuário)
Avast Premium Business Security	A plataforma de gerenciamento online oferece proteção de terminais com cibersegurança premiada, defesa contra *ransomware* e *phishing*, controle *web*, VPN pessoal, e bloqueio de dispositivos USB não autorizados, permitindo gerenciar remotamente a segurança dos usuários (AVAST, 2024).	**R$129,60** (Anual/Por usuário)
Microsoft Defender Para Empresas	O antivírus oferece proteção de nível empresarial. oeferce gerenciamento simplificado e integração baseada em assistente, detecção e resposta de ameaças baseada em Inteligência Artificial (IA) gerenciamento de vulnerabilidades, correção automatizada de ameaças, relatórios mensais de segurança e proteção adicional para servidores (Microsoft, 2024).	**R$171,60** (Anual/Por usuário)
Norton Small Business.	O serviço oferece segurança de dispositivo com antivírus em tempo real e *firewall*, *backup* na nuvem para proteção de dados, navegador privado, atualizador de software, gerenciador de senhas, VPN segura e atualizador de drivers para manter os dispositivos seguros e atualizados (NORTON, 2024).	**R$199,0** (No primeiro ano/Por usuário)

Fonte: Os Autores

A falta de Políticas de Proteção da Informação (V04) também foi visto e sem isso a tríade de confidencialidade, integridade e disponibilidade se tornam inexistentes, sendo imprescindível a criação de políticas de proteção da informação pautadas na LGPD e na ISO 27001, através de um documento que reúna todas essas regras necessárias para proteção da empresa.

Observou-se também, a falta de procedimentos para lidar com dispositivos de armazenamento externos (V05), em que não se é utilizado *pendrive* em todos os computadores, exceto no do responsável pelo financeiro, mas não há política relacionado ao uso, podendo acarretar problemas em dados sensíveis sendo necessário a utilização de software de controle de dispositivos e definir políticas de uso de dispositivos de armazenamento externo, além disso, alguns antivírus citados na Tabela 3 possuem aplicação para bloquear dispositivos não autorizados.

A gestão inadequada de acesso (V06) ao sistema também se torna uma vulnerabilidade sendo necessário desenvolver um gerenciamento controlado de quais usuários podem acessar determinados recursos com a utilização do *Activity Directory*, criando políticas baseado no usuário e função.

A ausência de auditorias de segurança (V07) também foi um problema visto em que torna impossível saber quais irregularidades estão presentes na empresa e após a criação das Políticas de Segurança da informação, é de suma importância a realização de auditorias de segurança de forma regular para assim verificar se essas regras estão sendo seguidas ou se existe alguma brecha, por se tratar de uma empresa de pequeno porte, essas auditorias podem acontecer de forma anual.

Foi identificado também a falta de medidas contra *Ransomware* (V08), sendo uma vulnerabilidade de alto risco que em caso de ataque pode gerar problemas de grandes proporções, por essa razão é ideal que a organização faça a criação de políticas de segurança e realize a implantação de soluções de segurança como Sistemas de Detecção e Intrusão (IDS) e Sistema de Prevenção de Intrusão (IPS), inclusive alguns dos antivírus indicado que foram apresentados na tabela 3 possuem aplicações contra ataques de *Ransomware* auxiliando na proteção da empresa.

Com relação a ausência de um plano de continuidade e respostas a incidentes (V08), em que se torna um problema em caso de a empresa ter que agir em caso de incidentes para dar continuidade as operações, é necessário a criação de um plano de continuidade com os padrões a serem seguidos em caso de alguma situação inesperada para a recuperação seja rápida.

Por fim, é importante que após seja estabelecido as políticas de segurança da informação dentro do escopo da organização, com intuito de que estas sejam aplicadas de forma adequada e até mesmo para que os funcionários passem a conhecer, entender e aplicar, é necessário que a organização desenvolva treinamentos para funcionários sobre segurança cibernética e realize a conscientização através de palestras e minicursos.

Tabela 4: Sugestões de Mitigações de Vulnerabilidades Identificadas

#	Vulnerabilidade	Mitigação
V01	Dependência de Suporte Remoto	Contratação de um profissional ou alteração de contrato para uma pessoa presencial.
V02	Organização Física e Estrutura da Rede	Organização da infraestrutura física mapeando a rede e avaliando os riscos.
V03	Ausência de Programas de Segurança	Instalação de programas de segurança como antívirus e *firewall* disponíveis no mercado.
V04	Falta de Políticas de Proteção da Informação	Criação de políticas bem definidas baseadas na LGPD e ISO 27001
V05	Falta de procedimentos para lidar com dispositivos de armazenamento externo	Definir procedimentos como implantação de software de controle de dispositivos e políticas de uso de dispositivos de armazenamento externo.
V06	Gestão Inadequada de Acessos	Criação de políticas baseado no usuário e função com o uso de *Active Directory*.
V07	Ausência de Auditorias de Segurança	Realizar auditorias de maneira regular para identificação de inconformidades.
V08	Falta de Medidas Contra *Ransomware*	Criação de políticas de segurança e de soluções como implantação de IDS/IPS.
V09	Ausência de Plano de Continuidade e Resposta a Incidentes	Criar e desenvolver um plano de continuidade e resposta a incidentes.
V10	Falta de Treinamento e Conscientização em Segurança Cibernética	Desenvolver treinamento para funcionários sobre segurança cibernética e conscientizá-los através de palestras e minicursos.

Fonte: Os Autores

Para realização das propostas de mitigações é necessário que os departamentos da empresa estejam envolvidos e colaborem para aplicação. No entanto, é necessário determinar as atividades de cada um dos envolvidos, para isso, foi elencado os responsáveis pelas melhorias sugeridas conforme a Tabela 5 e demonstrada a relação da quantidade de responsabilidade de cada departamento com base na Figura 6. Para V01, é necessário que o administrativo com a aprovação do financeiro realize a contratação de um profissional ou

alteração de contrato para uma pessoa presencial.

Em V02 e V03, é importante que o profissional de TI atue nas ações propostas e que o financeiro aprove a questão relacionado ao investimento realizado com relação ao programa de antivírus, o mesmo deve ocorrer em V05 com aprovação do software para controle de dispositivos.

Com base em V04, o administrativo é responsável por criar e definir as políticas com apoio do TI para orientá-los conforme as necessidades da organização e em V06, V08 e V09 é necessária atuação do TI, mas é importante que seja levado em consideração as políticas de segurança definidas. Para V07, é importante que estejam envolvidos nas auditorias o administrativo com apoio do TI para verificar e eficiência das políticas definidas e em V10, o administrativo deve programar os treinamentos, no entanto cabe a empresa como todo (Financeiro, Equipe de Vendas, Expedição, TI) adotar as boas práticas.

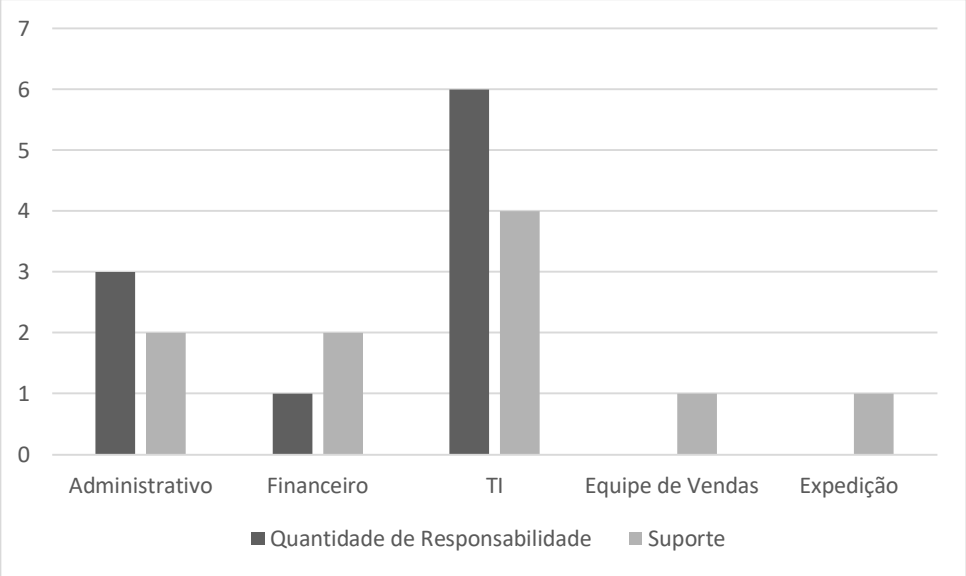
Tabela 5 – Atribuição de Responsabilidade Através das Melhorias Sugeridas

Vulnerabilidade	Mitigação	Departamento Responsável	Suporte do Departamento
V01 - Dependência de Suporte Remoto	Contratação de um profissional ou alteração de contrato para uma pessoa presencial.	Administrativo e Financeiro	-
V02 - Organização Física e Estrutura da Rede	Organização da infraestrutura física mapeando a rede e avaliando os riscos.	TI	-
V03 - Ausência de Programas de Segurança	Instalação de programas de segurança como antivírus e firewall disponíveis no mercado.	TI	Financeiro
V04 - Falta de Políticas de Proteção da Informação	Criação de políticas bem definidas baseadas na LGPD e ISO 27001.	Administrativo	TI
V05 - Falta de Procedimentos para Dispositivos Externos	Definir procedimentos como implantação de software de controle de dispositivos e políticas de uso de dispositivos de armazenamento externo.	TI	Financeiro
V06 - Gestão Inadequada de Acessos	Criação de políticas baseadas no usuário e função com o uso de *Active Directory*.	TI	-
V07 - Ausência de Auditorias de Segurança	Realizar auditorias de maneira regular para identificação de inconformidades.	Administrativo	TI
V08 - Falta de Medidas Contra Ransomware	Criação de políticas de segurança e de soluções como implantação de IDS/IPS.	TI	-

Vulnerabilidade	Mitigação	Departamento Responsável	Suporte do Departamento
V09 - Ausência de Plano de Continuidade e Resposta a Incidentes	Criar e desenvolver um plano de continuidade e resposta a incidentes.	TI	-
V10 - Falta de Treinamento em Segurança Cibernética	Desenvolver treinamento para funcionários sobre segurança cibernética e conscientizá-los através de palestras e minicursos.	Administrativo	TI, Equipe de Vendas, Expedição e Financeiro.

Fonte: Os Autores, 2024.

Figura 6: Relação de Quantidade de Responsabilidade por Departamento



Fonte: As Autores.

4.5 Discussão

A empresa faz parte do setor de varejo de materiais de construção. Apesar de ser de pequeno porte e já ser bem estabelecida em sua região, observou-se uma carência na disponibilização dos recursos voltados para segurança da informação.

A análise revelou diversas vulnerabilidades que precisam ser tratadas para garantir a segurança e a continuidade dos negócios. Inicialmente, observou a necessidade de ser implantado o básico na infraestrutura de TI a fim de melhorar a eficiência operacional e contribuir para a proteção da empresa e dos equipamentos e a criação de políticas de segurança da informação que será o pilar para a mitigação das demais vulnerabilidades identificadas.

Dessa forma, a implementação das ações proposta será uma base sólida de SegInfo

contribuindo para a proteção dos dados e operações da empresa como um todo. Ao adotar medidas de segurança sugeridas juntamente com a conscientização dos funcionários, a empresa não só se protegerá contra possíveis ameaças, mas também estará em conformidade de acordo com as regulamentações vigentes (LGPD e ISO 27001).

5. Conclusões

A empresa está inserida no setor de materiais de construção que está em constante crescimento e desenvolvimento, no entanto mesmo a empresa não seja específica de TI, a tecnologia da informação se tornou algo necessário compondo todos os processos dentro de uma organização, sendo importante os cuidados relacionados a infraestrutura para que seja aproveitada no máximo de sua eficiência e tornando-se indispensável a aplicação de proteções para preservar e resguardar a empresa com relação a possíveis vulnerabilidades relacionadas a tecnologia e segurança da informação.

Durante a pesquisa, foi identificado as necessidades da empresa relacionado com as vulnerabilidades encontradas e demonstrando a importância de definir medidas para mitigar os riscos encontrados, porque a falta dessas, não somente acarretam problemas no setor de TI como todo, mas também oferece risco a continuidade dos negócios.

A empresa precisa estar atenta ao fato de que, ao mesmo tempo que a tecnologia avança surgem formas de pessoas maliciosas se aproveitarem de vulnerabilidades para o ganho pessoal. Além disso, a organização tem uma base de clientes, sendo fundamental que esteja atenta aos malwares que vem surgindo na atualidade, inclusive o *Ransomware* que foi citado durante o estudo.

A contribuição para a teoria está em apresentar vulnerabilidades que podem ser encontradas em empresas de pequeno porte, principalmente se tratando de empresas locais. A contribuição para a prática é informar as empresas e os principais envolvidos a importância da segurança da informação e a necessidade de se mitigar as vulnerabilidades.

Referências Bibliográficas

ABECIP. **ABECIP**. Disponível em: <https://www.abecip.org.br/imprensa/noticias/varejo-de-materiais-elevou-faturamento-em-2022-valor-economico>. Acesso em: 2 maio. 2024.

ABRAMAT. **Home Abramat**. Disponível em: <https://abramat.org.br/>. Acesso em: 30 abr. 2024.

ANAMACO. **Brasil tem 152 mil lojas de materiais de construção, aponta levantamento do Instituto ANAMACO**. **ANAMACO**, 2024. Disponível em: <https://www.anamaco.com.br/post/brasil-tem-152-mil-lojas-de-materiais-de-construcao-aponta-levantamento-do-instituto-anamaco/>. Acesso em: 2 maio. 2024

ANTONIO CARLOS GIL. **Como elaborar projetos de pesquisa**. 6ª ed. [s.l.] Editora Atlas Ltda, 2017.

BARBOSA, J. S. et al. A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. **Research, Society and Development**, v. 10, n. 2, p. e40510212557–e40510212557, 20 fev. 2021.

CANDIDO, J. W.; FLORIAN, F.; BORGES, J. H. G. SEGURANÇA DA INFORMAÇÃO COM FOCO NA PROPAGAÇÃO IMINENTE DE RANSOMWARE NAS CORPORAÇÕES. **REVISTA FOCO**, v. 16, n. 5, p. e1766–e1766, 5 maio 2023.

COGNATIS. **Material de Construção: Um Mercado de Destaque na Economia Nacional**. **Cognatis**, 2023. Disponível em: <https://cognatis.com.br/o-mercado-de-materiais-de-construcao-no-brasil/>. Acesso em: 30 abr. 2024

COSTA, E. S. DA; GALVÃO, W. C. Segurança da Informação e Proteção dos Dados: Aplicação Web. **Journal of Technology & Information (JTnI)**, v. 3, n. 1, 8 jun. 2023.

FEBRAMAT. **Tendências do varejo de materiais de construção para 2022 que vão aumentar suas vendas**. **Febramat**, 6 dez. 2021. Disponível em: <https://febramat.com.br/2021/12/06/tendencias-do-varejo-de-materiais-de-construcao-para-2022-que-vao-aumentar-suas-vendas/>. Acesso em: 4 jun. 2024

FILHO, N. P. R.; FREITAS, D. P. DE. Ransomware: origens, consequências e prevenção. **STUDIES IN ENGINEERING AND EXACT SCIENCES**, v. 4, n. 1, p. 427–438, 28 dez. 2023.

GIL, Antonio Carlos. **Como Elaborar Projetos de Pesquisa**. 6. ed. São Paulo: Atlas Ltda., 2017. 1. Pesquisa 2. Pesquisa – Metodologia I. Título. ISBN 978-85-97-01292-7. Disponível em: https://edisciplinas.usp.br/pluginfile.php/7237624/mod_resource/content/1/Ant%C3%B4nio%20C.%20Gil_Como%20Elaborar%20Projetos%20de%20Pesquisa.pdf. Acesso em: 15 abr. 2024.

GOUVEIA, L. B. Desafios da segurança da informação: uma reflexão no contexto da ciência da informação. **Arade, Revista do Arquivo Municipal de Lagoa**, v. 2, n. 2, p. 233–247, nov. 2023.

KANAGUSKU, A. R. A.; GASETA, E. FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO: DESMISTIFICANDO O ELO MAIS FRACO. **FatecSeg - Congresso de Segurança da Informação**, 22 out. 2023.

KASPERSKY. **Ransomware: definição, prevenção e remoção**. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/ransomware>. Acesso em: 8 mar. 2024.

LIMA, P. R. S.; FERREIRA, L. M. M.; PEIXOTO, A. L. V. DE A. Gestão da segurança da informação: análise de políticas de defesa cibernética e estratégias para a proteção

de dados e informações da administração pública brasileira. **P2P E INOVAÇÃO**, v. 9, n. 1, p. 206–221, 29 set. 2022.

NASCIMENTO, S.; GLÓRIA JÚNIOR, I. O Plano de Continuidade de Negócios Aplicado a Ransomware em Empresas Multinacionais. **Journal of Technology & Information (JTnI)**, v. 4, n. 1, 2023.

PIMENTEL, J. E. DE S.; CABRERA, D. A.; FORTE, C. E. Ransomware: do surgimento aos ataques "as a service". **FatecSeg - Congresso de Segurança da Informação**, 21 out. 2021.

ROMANO, M. R.; ARMELIN, S. R. Ameaças Cibernéticas em ascensão: Os Ataques Hackers no Mundo. **Prospectus (ISSN: 2674-8576)**, v. 5, n. 2, p. 187–200, 12 dez. 2023.

SANTOS, J. V. F. DOS. CIBERSEGURANÇA E A IMPORTÂNCIA DO DIREITO DIGITAL. **Revista Multidisciplinar do Nordeste Mineiro**, v. 12, n. 1, 30 out. 2023.

SEBRAE. **Como montar uma loja de material de construção - Sebrae**. Disponível em: <https://sebrae.com.br/sites/PortalSebrae/ideias/como-montar-uma-loja-de-material-de-construcao,45287a51b9105410VgnVCM1000003b74010aRCRD>. Acesso em: 4 jun. 2024.

SILVA, E. V. F.; SOUSA, L. C.; GLÓRIA JÚNIOR, I. PRINCIPAIS ATAQUES EM EMPRESAS UTILIZANDO A ENGENHARIA SOCIAL. **FatecSeg - Congresso de Segurança da Informação**, 22 out. 2023.

SILVA, S.; GLÓRIA JÚNIOR, I. Ransomware: A Evolução Dos Ataques Na Contemporaneidade e Seus Desafios para a Segurança Digital. **Journal of Technology & Information (JTnI)**, v. 3, n. 2, 7 jul. 2023.

THEÓPHILO, C. R. Integração das abordagens quantitativa e qualitativa: ensaio sobre métodos mistos na pesquisa em Contabilidade. **Revista de Contabilidade e Organizações**, v. 17, p. e221846–e221846, 31 dez. 2023.

VENTURA, J. H.; MARTINS, D. M. S. Controle e Acesso Seguro aos Sistemas Operacionais Empresariais. **Caderno de Estudos em Sistemas de Informação**, v. 6, n. 1, 3 set. 2022.

APÊNDICE – Questionário

Conteúdo: Políticas e Procedimentos de Segurança da Informação

1) Como a empresa aplica a proteção da informação, considerando a crescente importância?
2) Como são gerenciados os acessos aos sistemas e dados da empresa?
3) Quais são as políticas e procedimentos para lidar com dispositivos de armazenamento externo (pen drives, discos rígidos externos)?
4) A empresa realiza auditorias regulares de segurança para identificar possíveis vulnerabilidades nos sistemas e na rede?
5) A empresa realiza a utilização de programas de segurança e firewall para evitar ataques

externos em sua infraestrutura?

Conteúdo: Medidas de Proteção contra Ameaças Cibernéticas

6) Quais as medidas de proteção aos ataques de Ransomware a empresa implementou ou já possui?
7) Quais são os procedimentos de resposta a incidentes que a empresa possui? A empresa possuí um plano de continuidade?
8) A empresa realiza testes de simulação de ataques de Ransomware para avaliar a eficácia dos seus controles de segurança ?

Conteúdo: Conscientização de Funcionários

9) Existe uma política de conscientização e treinamento dos funcionários em relação à segurança cibernética?
10) A empresa utiliza alguma forma de análise de comportamento de usuários ou sistemas para detectar atividades suspeitas?