CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO DE GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

BENEFICIOS NA IMPLEMENTAÇÃO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EM PEQUENAS E MÉDIAS EMPRESAS

Matheus Souza Santos – matheussouzamts10@gmail.com
Wherysson Eduardo Santana – wherysson@gmail.com

Orientador: Wdson de Oliveira – wdson.oliveira01@fatec.sp.gov.br

Araraquara
2º semestre/2024

RESUMO

A segurança da informação é essencial para proteger os ativos de informação das organizações. Este estudo analisa a criação e aplicação de uma política de segurança da informação (PSI) nas empresas, com ênfase na conformidade com a lei geral de proteção de dados (LGPD). O trabalho identifica os principais desafios enfrentados, incluindo a percepção de altos custos e a falta de conscientização sobre a LGPD. A pesquisa de campo, realizada através de formulário envolve questionários que avaliam o nível de conhecimento sobre a segurança da informação da empresa e as práticas adotadas. A análise dos dados orienta propostas de implementação de PSI adaptáveis e escaláveis, visando reduzir riscos, proteger a reputação e assegurar a continuidade dos negócios. Este estudo demonstra que a PSI não é apenas uma exigência legal, mas um investimento estratégico, garantindo benefícios a todos os envolvidos.

Palavras-chave: Segurança da Informação, LGPD, PSI, Benefícios, Conformidade Legal.

ABSTRACT

Information security is essential to protect the information assets of organizations. This study analyzes the creation and implementation of an Information Security Policy (ISP) in companies, emphasizing compliance with the General Data Protection Law (LGPD). The work identifies the main challenges faced, including the perception of high costs and the lack of awareness about the LGPD. The field research, conducted through questionnaires, evaluates the company's level of knowledge about information security and the practices adopted. The data analysis guides proposals for adaptable and scalable ISP implementation, aiming to reduce risks, protect reputation, and ensure business continuity. This study demonstrates that an ISP is not only a legal requirement but also a strategic investment, providing benefits to all stakeholders.

Keywords: Information Security, LGPD, ISP, Benefits, legal compliance.

1. INTRODUÇÃO

Atualmente a segurança da informação é crucial para qualquer corporação. Mesmo em empresas que as atividades principais não estão envolvidas com meios digitais, é absolutamente necessária uma forma de tratar e lidar com os dados para evitar incidentes e impactos negativos às mesmas. De acordo com dados da empresa de segurança cibernética EST, o Brasil ocupou a quarta posição na América Latina em número de ameaças digitais detectadas no primeiro semestre de 2024, totalizando 201 mil ocorrências. Países como Peru, México e Equador lideraram o ranking (CNN BRASIL, 2024).

A segurança da informação é uma área crucial da gestão empresarial, que visa proteger os ativos de informação dentro das organizações. A “Segurança da Informação é um conceito fundamental que envolve a proteção dos dados de propriedade das organizações e de pessoas

físicas e jurídicas, garantindo a mitigação de riscos e a continuidade das operações" (SCIENTIFIC SOCIETY, 2024). Este artigo propõe-se a analisar as melhores formas de desenvolver e implementar uma Política de Segurança da Informação (PSI) em empresas de pequeno e médio porte, muitas das quais ainda não seguem as normas e diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD). Um dos maiores desafios enfrentados por essas empresas é a percepção de que adotar tais políticas implica custos adicionais, o que pode gerar resistência.

A LGPD, criada em 2018 e em vigor desde 2020, estabeleceu normas rígidas para o tratamento de dados pessoais, incluindo sua coleta, armazenamento, compartilhamento e uso. O não cumprimento dessas normas pode resultar em multas significativas, de até 2% do faturamento da empresa, com um limite máximo de R$ 50 milhões (BRASIL, 2018).

O tratamento inadequado das informações pode ter consequências graves para as empresas, como o extravio de dados sensíveis, o que pode prejudicar sua imagem e competitividade no mercado. Além disso, tais falhas podem ser usadas de forma maliciosa, como por exemplo, para fraudes, extorsão ou quebra de sigilo comercial. Portanto, a implementação de uma PSI bem estruturada não só protege os dados, mas também assegura a integridade e a reputação da organização, evitando penalidades e danos irreparáveis (BRASIL, 2018).

A crescente importância da segurança da informação no meio corporativo está em evidência, sendo um tema cada vez mais discutido e tratado como essencial, em vez de algo desconhecido ou secundário. A PSI tem como objetivo fundamental manter a confidencialidade, integridade e disponibilidade das informações. Além disso, visa estabelecer controles de acesso, realizar análises de dados e garantir que as empresas estejam em conformidade com as leis vigentes, incluindo a LGPD.

Este artigo busca evidenciar que a implementação de uma PSI eficiente representa um investimento estratégico para as empresas, principalmente para os pequenos e médios empreendedores. Com uma PSI bem planejada, os benefícios superam os custos, proporcionando credibilidade e destaque no mercado (RODRIGUES, 2020).

Os quatro pilares da Segurança da Informação:

A elaboração de uma PSI deve seguir os 4 pilares descritos no **Decreto 9.637/2018**, sendo:

1. **Confidencialidade:** Garantir que apenas pessoas autorizadas tenham acesso às informações. O controle de acesso será realizado por meio de software especializado
2. **Integridade:** A informação deve estar correta, confiável e sem alterações. Devem ser implementados mecanismos de autenticação para garantir que as informações não sejam adulteradas.
3. **Disponibilidade**: As informações devem estar acessíveis e disponíveis para as pessoas autorizadas a utilizarem-nas.
4. **Autenticidade**: Garantir que as informações sejam provenientes de fontes confiáveis, assegurando sua integridade desde a coleta até o armazenamento.

(BRASIL, 2018).

Uma PSI eficaz tem como objetivo principal proteger os ativos de informação da empresa e minimizar os riscos de violação ou perda de dados. Ela visa garantir a confidencialidade, integridade e disponibilidade dos dados, além de mitigar os riscos associados a acessos não autorizados, uso indevido de informações e vazamentos de dados.

Objetivos da Política de Segurança da Informação (PSI):

- **Reduzir Riscos:** Mitigar as chances de perda ou dano à informação, prevenindo incidentes como vazamentos de dados e ataques cibernéticos.
- **Atender às leis e regulamentações**: Manter a conformidade com as exigências legais, como a LGPD, evitando multas e sanções.
- **Proteger a reputação**: Proteger a imagem da organização e garantir a confiança de clientes, parceiros e investidores, preservando a segurança dos dados.
- **Manter a continuidade dos negócios**: Minimizar interrupções nas operações da organização e reduzir a perda de receita em caso de incidentes de segurança.
- **Promover a conscientização**: Aumentar o conhecimento dos colaboradores sobre os riscos à segurança da informação, reduzindo a ocorrência de erros humanos, uma das principais causas de incidentes.

(BRASIL, 2018).

Implementação da Política de Segurança da Informação

As políticas de segurança da informação devem ser aplicadas tanto dentro quanto fora da corporação, sendo de responsabilidade de todos os colaboradores. O sucesso da implementação da PSI depende do comprometimento de todos os envolvidos, desde a alta gestão até os funcionários operacionais (BRASIL, 2018).

A PSI não deve ser vista como um simples “produto” a ser adquirido, mas como um **investimento estratégico** em segurança. Com o aumento dos ataques cibernéticos, a PSI é essencial para a proteção dos dados da organização, independentemente do seu porte. Ela é um conjunto de medidas e regras que orientam as práticas de proteção da informação dentro da corporação, tornando-se uma aliada fundamental na preservação da segurança dos dados (BRASIL, 2018).

O objetivo deste trabalho é desenvolver e propor uma Política de Segurança da Informação (PSI) para pequenas e médias empresas, buscando proteger os dados organizacionais e assegurar a conformidade com a Lei Geral de Proteção de Dados (LGPD).

2. REFERENCIAL TEÓRICO

A segurança da informação é um elemento de suma importância para empresas de todos os portes, mas os dados coletados revelam que das pequenas e médias empresas analisadas 70% não possuem uma Política de Segurança da informação formalizada. É um assunto que deve ser altamente disseminado devido ao grande avanço tecnológico e disponibilidade de informações.

2.1 Os desafios do desenvolvimento e implementação de uma PSI em micro e pequenas empresas

Os principais desafios estão atribuídos a desafios relatados, como falta de recursos financeiros, por não ter alguém dedicado a área de TI encontramos também a falta de conhecimento técnico sobre o tema dificuldade em adaptar as políticas às necessidades organizacionais. Esses dados reforçam a necessidade de conscientização e investimentos acessíveis.

A falta de recursos financeiros é uma das barreiras mais comuns para a implementação de uma política de segurança eficaz. De acordo com a Risk Management Studio (2024), a falta de recursos impede muitas pequenas empresas de desenvolverem e implementarem soluções de segurança adequadas, o que as torna vulneráveis a ataques cibernéticos. Muitas vezes, essas empresas não podem investir em softwares de segurança avançados ou contratar profissionais especializados, o que deixa lacunas na proteção dos dados.

Além da limitação financeira, muitas PMEs enfrentam a falta de profissionais qualificados para implementar uma política de segurança da informação eficaz. Como destacado pelo The Financial Daily (2024), a escassez de conhecimento técnico dentro das pequenas empresas faz com que elas não consigam identificar vulnerabilidades, implementar protocolos de segurança ou responder rapidamente a ameaças. A falta de pessoal especializado aumenta o risco de falhas de segurança.

A adaptação de políticas de segurança genéricas para as especificidades de uma PME também é um desafio. As práticas de segurança desenvolvidas para grandes empresas frequentemente não são aplicáveis a PMEs, que têm uma estrutura mais enxuta e recursos limitados.

2.1. Necessidade da conscientização para evitar custos da insegurança

Pretende-se identificar o nível de conhecimento e aplicação de práticas de segurança da informação nessas empresas, avaliando o grau de adequação às exigências legais e mapeando suas principais vulnerabilidades e desafios. Com base nessas análises, busca-se propor soluções práticas, economicamente viáveis e escaláveis, que promovam a implementação de políticas de segurança de forma eficiente. Além disso, o trabalho visa conscientizar e capacitar os colaboradores sobre a importância da segurança da informação e do cumprimento das normativas legais, demonstrando como a aplicação de uma PSI pode reduzir riscos, proteger a reputação organizacional, garantir a continuidade dos negócios e evitar penalizações por inseguranças e despreparo.

Segundo Cook (2017), a conscientização em segurança cibernética é uma estratégia essencial para pequenas empresas, ajudando-as a identificar e mitigar vulnerabilidades antes que elas se transformem em ameaças reais. O estudo destaca que a conscientização adequada pode ser obtida por meio de treinamentos regulares e estratégias específicas, como a inclusão de testes simulados de phishing, que ajudam a preparar os colaboradores para reconhecer ataques.

Um estudo realizado na Universidade do Norte do Texas (2014) identificou que a conscientização em segurança da informação tem um impacto direto na conformidade com políticas organizacionais de segurança. O estudo revelou que colaboradores treinados apresentam maior capacidade de reconhecer e evitar armadilhas, como mensagens de phishing, reduzindo significativamente os riscos para as empresas.

Almunawar (2023) discute que a conscientização em segurança da informação não deve ser um evento único, mas sim uma prática contínua, integrada à cultura organizacional. A

implementação de workshops regulares e treinamentos personalizados pode reduzir custos associados a incidentes de segurança e aumentar a resiliência da empresa.

2.2. Desenvolver cultura de segurança dos dados aos colaboradores:

Os dados são vitalmente importantes para uma organização e o seu zelo e mantimento seguro é um dever de todos dentro da corporação, por isso se faz necessário o desenvolvimento de cultura de segurança dos dados dentro da empresa para treinamento e conscientização dos colaboradores. Uma das ideias seria uma já existente vinda da Segurança do trabalho, onde é realizado uma semana de conscientização dos colaboradores, referente aos riscos e deveres no ambiente organizacional, conhecido como Semana Interna de Prevenção de Acidentes de Trabalho (SIPAT). Uma semana por ano dedicada à reflexão e conscientização de prevenção de acidentes no trabalho e cuidados com a saúde. Nesta semana, ocorrem diversas atividades como por exemplo palestras, teatro, intervenções, exames médicos, treinamentos, entre outros. (SUPER SIPAT, 2024).

A ideia seria uma Semana Interna de Conscientização da Segurança dos Dados, onde ficaria disponível ao time de TI da organização ou empresa terceira contratada um período diário de 30 à 45 min diários no período desta semana, para conscientização dos colaboradores. De forma simples e direta mostrando as causas e consequência de vazamento de dados e informações sensíveis, da empresa, clientes ou colaboradores, através de banner e folders demonstrativos. Dentre essa semana os colaboradores estariam cientes de que seriam testados de forma velada e segura, com ferramentas de Phishing e outra ferramentas de teste em ambientes controlado.

2.3. Conformidades Legais, normas e procedimentos:

Conforme citado por Dorneles, Araújo e Costa (2024), a norma ABNT ISO/IEC 27001 estabelece diretrizes específicas para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), com foco nos princípios fundamentais de confidencialidade, integridade e disponibilidade. Esses pilares garantem que as informações sejam protegidas contra acessos não autorizados, alterações indevidas e que estejam disponíveis sempre que necessário. A norma também destaca a importância de adaptar os controles de segurança às necessidades e finalidades de cada organização.

De acordo com Novais et al. (2021), a LGPD e a ISO/IEC 27001 podem ser integradas para assegurar conformidade regulatória e proteção de dados pessoais. A norma oferece

processos estruturados para gestão de segurança, enquanto a LGPD impõe a responsabilidade legal sobre o tratamento e a proteção desses dados. Essa sinergia é essencial para minimizar riscos e evitar penalidades legais, ao mesmo tempo que promove a confiança de clientes e parceiros.

O crescimento das ameaças aos sistemas de informação exige que as organizações adotem políticas sólidas de segurança alinhadas às regulamentações. A ABNT ISO/IEC 27002, por exemplo, descreve a informação como um ativo valioso e destaca a necessidade de proteger os dados por meio de controles eficazes, principalmente em ambientes corporativos sujeitos a legislações como a LGPD (ALMEIDA et al., 2019; FERREIRA et al., 2020).

A LGPD exige que as organizações utilizem Relatórios de Impacto à Proteção de Dados (RIPD), que documentam os procedimentos adotados para mitigar riscos e garantir a conformidade com a legislação. Esses relatórios são essenciais para mapear vulnerabilidades, implementar salvaguardas apropriadas e promover maior alinhamento com as exigências legais (LIMA et al., 2020; BASTOS et al., 2019).

Com o avanço das exigências legais, como a Lei Geral de Proteção de Dados (LGPD), e o aumento dos riscos associados a ataques cibernéticos, torna-se essencial compreender os conceitos de confidencialidade, integridade, disponibilidade e autenticidade das informações. Esses pilares, descritos no Decreto 9.637/2018, são fundamentais para estruturar uma Política de Segurança da Informação (PSI) eficiente. Também temos a ISO/IEC 27001 que rege vários aspectos da segurança da informação tais como a Gestão de riscos, Controle de acesso e criptografia. As corporações que aderem a certificação da ISO/IEC 27001 demonstram a conformidade com segurança a proteção dos dados e informações. A organização deve ter ciência de todas as regulamentações internas e as leis vigentes do País, ficando em conformidade com as leis vigentes.

2.4. Um guia para a implementação da PSI

2.4.1. Avaliação de Riscos

Para a implementação da PSI, a avaliação de riscos é um passo essencial que inclui a identificação de vulnerabilidades análises de impacto e a classificação dos riscos identificados. No processo de avaliação de riscos, torna-se extremamente que sejam seguidas orientações de normas técnicas que abrangem esse tema, como a ISO/IEC 27001 que estabelece os requisitos para o gerenciamento da segurança da informação. Os Riscos de segurança da informação são a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, assim prejudicando a organização (GUIA 73, 2009) (ISO 31000, 2018). O

processo de avaliação de riscos permite identificar eventos que possam causar a perda dos ativos e mapear as ações a serem efetuadas (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011).

2.4.2. Desenvolvimento da Política

Com os riscos identificados e classificados inicia-se o desenvolvimento efetivo da PSI, que deve ser criada tendo como base a organização, se adaptando e ajustando às necessidades de cada empresa permitindo que seja abrangente a todas as áreas e atenda às prioridades de cada companhia. A criação da política é embasada na ISO/IEC 27002 que por sua vez fornece as diretrizes para a implantação de um sistema de gestão de segurança da informação. A PSI da empresa deve ser formalizada em um documento que contenha os princípios da Segurança da Informação e uma estrutura com objetivos claros, formas de controle e o comprometimento dos gestores e líderes para com a política (ABNT, 2005).

2.4.3. Implementação e monitoramento

A implementação requer amplo treinamento de todos os envolvidos, a adequação dos componentes de infraestrutura física e lógica e o monitoramento constante após a realização para que seja avaliado o desempenho e tomadas medidas corretivas caso sejam necessárias. O monitoramento deve ser realizado com auditorias e ferramentas especializadas para a detecção de intrusão e de vulnerabilidades e firewalls que podem auxiliar na filtragem e controle de acesso às informações.

2.5. Benefícios da implementação

2.5.1. Proteção de dados e ativos

A política de Segurança da Informação de como objetivo a proteção dos dados confidenciais de acesso não autorizado e vazamento dos mesmos. Tais dados podem ser tanto da organização quanto de seus funcionários ou clientes, por isso é de extrema importância que sejam protegidos evitando assim consequências legais e à imagem da empresa, contudo, políticas bem definidas garantem o cumprimento das normas vigentes e reduzem o risco de penalidades financeiras. Segundo a ISSO/IEC 27002, a proteção de dados é um elemento-chave para preservar a confidencialidade, integridade e disponibilidade de ativos da informação.

"A gestão de riscos e a proteção de dados são essenciais para garantir a continuidade operacional, pois ajudam as organizações a identificar vulnerabilidades e implementar controles adequados" (ISO/IEC 27002, 2005).

2.5.2. Melhoria da reputação

Atualmente a segurança dos dados pessoais é um tema importante mundialmente, e empresas que demonstram estarem comprometidas com tal coisa tornam-se mais confiáveis para os clientes, parceiros e investidores interessados. Com base em u estudo do Instituto Federal de Brasília, 67% das empresas que implementaram uma PSI relataram maior confiança dos stakeholders como um dos benefícios mais significativos. Uma política bem implementada traz benefícios não somente mitigando os riscos, mas também na imagem da empresa trazendo a percepção de confiança e compromisso da empresa (Unifesspa, 2024).

2.5.3. Crescimento do negócio

"Empresas que investem em segurança da informação se destacam pela capacidade de crescer e inovar em um ambiente digital competitivo e em constante evolução" (IFSC, 2023). Ao proteger seus dados e sistemas, as empresas minimizam interrupções causadas por incidentes de segurança, garantindo a continuidade dos negócios e promovendo inovação. Além disso, o alinhamento com regulamentações e boas práticas facilita parcerias comerciais e amplia a capacidade de atuação em mercados mais exigentes.

2.6. Conclusão: A segurança da Informação como um investimento estratégico para o sucesso da empresa

Assegurar a segurança da informação não é apenas uma forma de proteger a empresa e seus dados, mas também uma estratégia essencial para o sucesso e o mantenimento das organizações. Implementar uma PSI bem estruturada seguindo as recomendações das normas técnicas traz benefícios diretos na redução de riscos, fortalecimento da reputação da empresa e a continuidade de negócios em caso de desastres, incidentes ou ameaças cibernéticas.

Empresas que encaram a segurança como investimento se tornam mais aptas a se adaptar às mudanças regulatórias e tecnológicas ganhando vantagem competitiva em seus setores. De acordo com a ISSO 31000, o gerenciamento contínuo de riscos permite que organizações ajustem suas estratégias rapidamente para proteger seus ativos e explorar novas oportunidades de negócio.

"A segurança da informação é um elemento estratégico que garante resiliência organizacional, continuidade de operações e alinhamento às exigências legais e de mercado" (IFSC, 2023).

3. PROCEDIMENTOS METODOLÓGICOS

A fim de atingir os objetivos delineados para o trabalho, foi necessário realizar um levantamento bibliográfico com base no tema proposto. O levantamento bibliográfico contou com pesquisa em livros, revistas especializadas, e pesquisas na Internet.

A pesquisa de campo realizada, de cunho quantitativo, utilizou um questionário como instrumento de coleta de dados. As perguntas foram formuladas para avaliar o nível de conhecimento sobre a Lei Geral de Proteção de Dados (LGPD) e a existência de práticas relacionadas à Política de Segurança da Informação (PSI). O questionário abordou aspectos como a presença de profissionais de tecnologia da informação, a familiaridade com a LGPD, a existência de uma PSI ativa e os tipos de dados coletados e armazenados pelas empresas. Os dados coletados foram organizados em planilhas e analisados por meio de gráficos e relatórios, permitindo identificar padrões e tendências.

O desenvolvimento deste estudo foi baseado em uma **pesquisa de campo**, e teve como objetivo levantar dados de empresas localizadas em **Araraquara**. A pesquisa foi realizada por meio da aplicação de um **questionário** contendo perguntas objetivas, que visam coletar informações relevantes sobre o nível de conhecimento e as práticas de segurança da informação de aproximadamente 21 empresas de pequeno e médio porte na região de Araraquara, cidade localizada no interior do Estado de São Paulo, com ênfase especialmente no que diz respeito à **LGPD** e à **Política de Segurança da Informação (PSI)**.

A coleta de dados foi realizada com base treze perguntas divididas em cinco partes com opções de respostas pré-definidas, que abordarão tanto a **infraestrutura de TI** das empresas quanto seu nível de conformidade com a legislação vigente.

Desenvolvimento de Soluções e Propostas de Implementação

Com a coleta e análise dos dados obtidos foi possível propor um plano de ação visando os pontos fortes e fracos das empresas e o que precisa ser avaliado na implantação de uma PSI:

- **Desenvolvimento de políticas e procedimentos** de segurança adaptáveis às realidades de cada empresa.
- **Treinamento de funcionários** para aumentar a conscientização sobre a importância da segurança da informação e o cumprimento da LGPD.
- **Recomendações para a criação de controles de acesso** e autenticação, minimizando os riscos de acesso não autorizado aos dados.
- **Implementação de ferramentas e tecnologias** que garantam a integridade e a confidencialidade das informações.

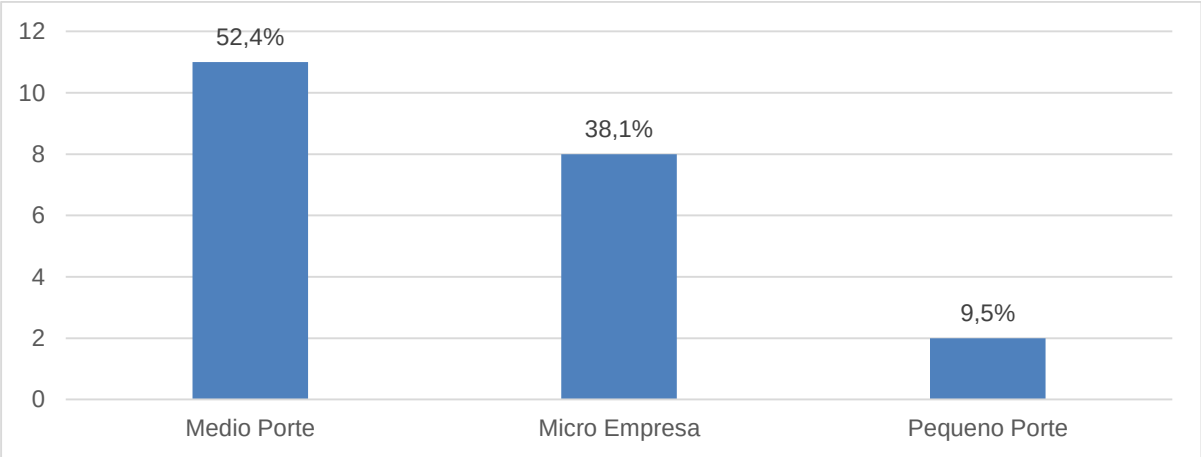
4. RESULTADOS E DISCUSSÃO

A pesquisa revela que um número significativo de empresas de pequeno e médio porte ainda não possui uma Política de Segurança da Informação (PSI) formalizada. Além disso, entre as empresas que já possuem essa política, as atualizações são pouco frequentes, o que compromete sua eficácia diante das constantes ameaças cibernéticas deixando-as totalmente vulneráveis. Os principais desafios relatados incluem falta de recursos financeiros, a não disponibilidade de um colaborador capacitado para o gerenciamento dos ativos, dificuldade de adaptação às necessidades específicas e capacitação insuficiente dos colaboradores.

Os benefícios que foram mencionados repetidamente pelas empresas que adotaram uma PSI incluem numa maior confiança dos clientes e conformidade com a legislação, passando segurança para fechamento de novas oportunidades de prestação de serviços. Entretanto, é claro que a redução de custos com incidentes de segurança foi percebida por uma minoria por ser pouco eficaz nos casos de empresas que não faz o tratamento da PSI adequadamente. Empresas maiores com um poder de investimento demonstraram maior eficácia na aplicação da PSI, com a manutenção correta, cobrindo áreas como controle de acesso e treinamento, enquanto as menores enfrentaram limitações financeiras e tecnológicas.

No gráfico 1 podemos observar que 52,4% das empresas que responderam o questionário são corporações de médio porte, já as microempresas correspondem a 38,1% das respostas do questionário e 9,5% são empresas de pequeno porte.

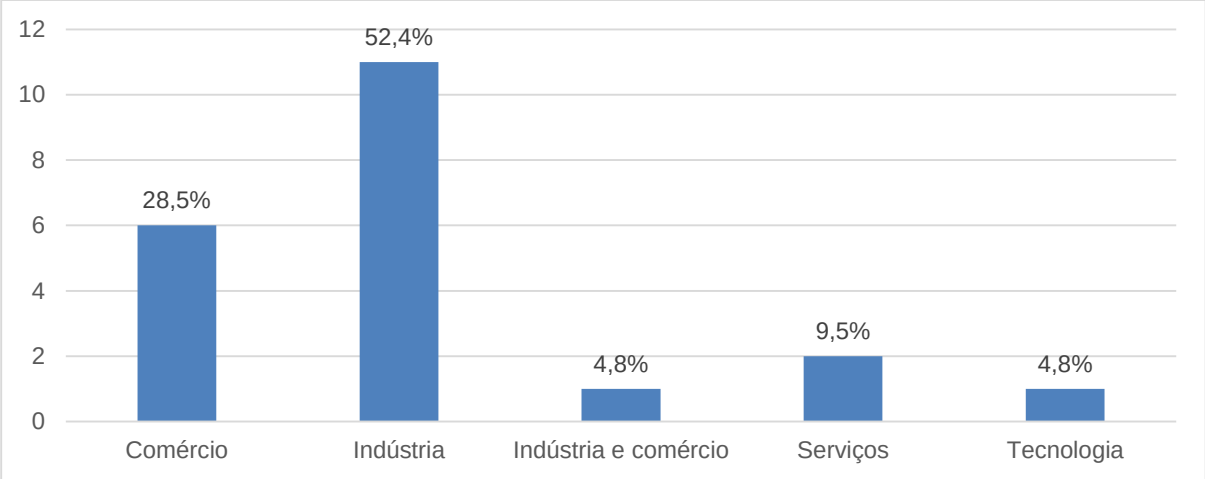
Gráfico 1: Porte das empresas que participaram do questionário.



Fonte: Elaborado pelos autores Matheus Souza e Wherysson Santana (2024)

Podemos verificar no decorrer do questionário que dentre as empresas, o setor de atuação que mais se destaca é o ramo de Indústria, seguido por Comércio e Serviços. Conforme ilustrado no gráfico 2.

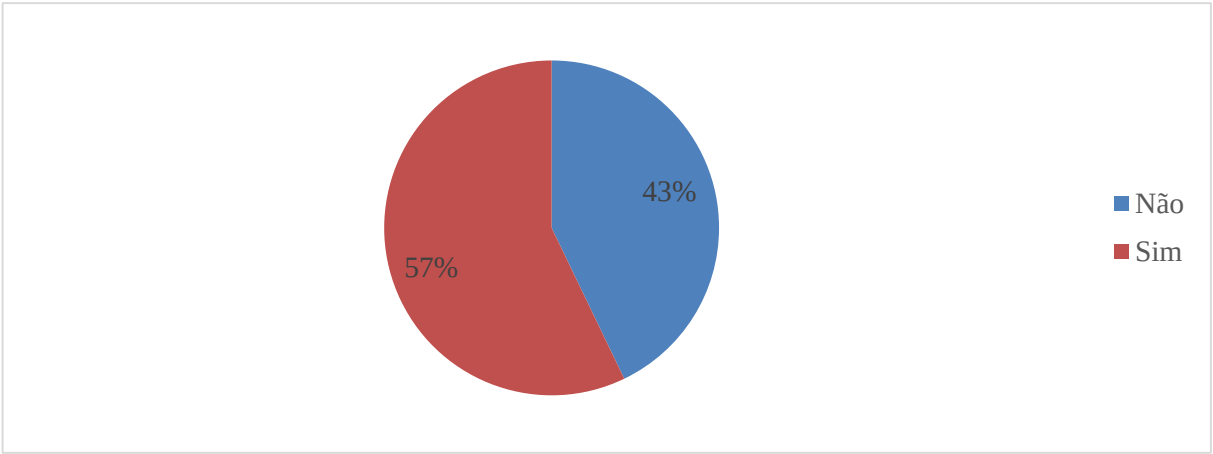
Gráfico 2: Setor de atuação das empresas.



Fonte: Elaborado pelos autores Matheus Souza e Wherysson Santana (2024)

O gráfico 3, traz a representação das empresas que possuem uma equipe de TI dedicada, e podemos verificar que dentre as empresas participantes apenas 57% possuem colaborador ou uma equipe dedicada para o desenvolvimento da tecnologia da informação das empresas.

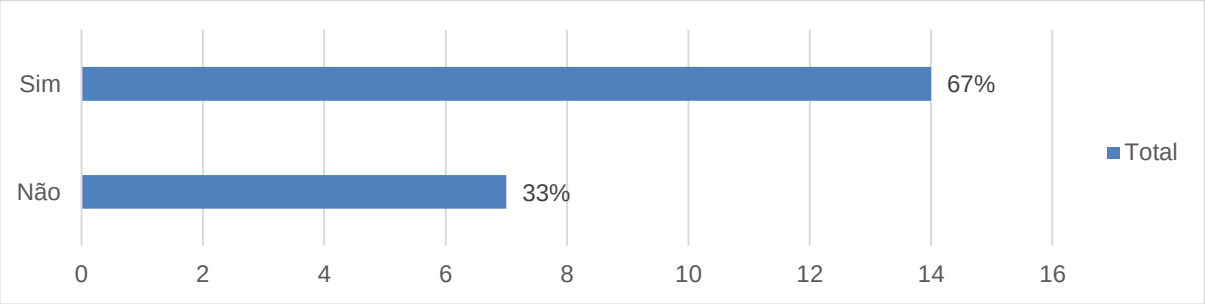
Gráfico 3: Possui uma equipe de TI dedicada?



Fonte: Elaborado pelos autores Matheus Souza e Wherysson Santana (2024)

Dentre as informações coletadas, podemos verificar que 67% das empresas que responderam o questionário, dizem ter uma Política de Segurança da informação conforme indicado no gráfico 4. E os demais 33% não possuem uma PSI ativa.

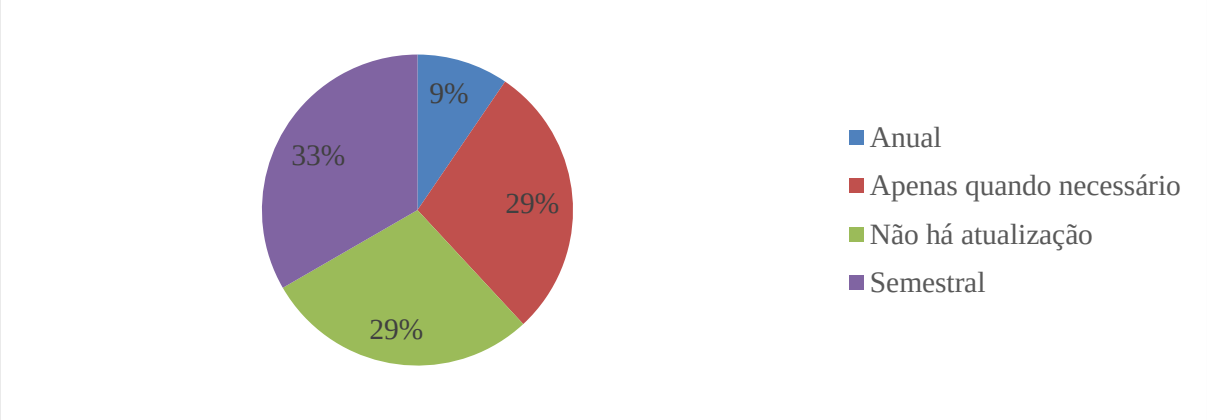
Gráfico 4: Empresa possui uma Politica de Segurança da informação?



Fonte: Elaborado pelos autores Matheus Souza e Wherysson Santana (2024)

Através das informações coletadas, podemos analisar que na grande maioria das empresas são feitas atualizações semestrais na PSI e 29% apenas quando se faz necessário. O ponto crítico nestes dados é a quantidade de empresas que não faz nenhuma atualização da PSI, sendo por não ter Política de Segurança da Informação ativa, ou por não ter recursos financeiros ou humanos, deixando assim os dados e ativos da empresa em um alto risco de vulnerabilidade. O gráfico 5 nos demonstra a frequência de atualização da política de segurança da informação nas empresas entrevistadas.

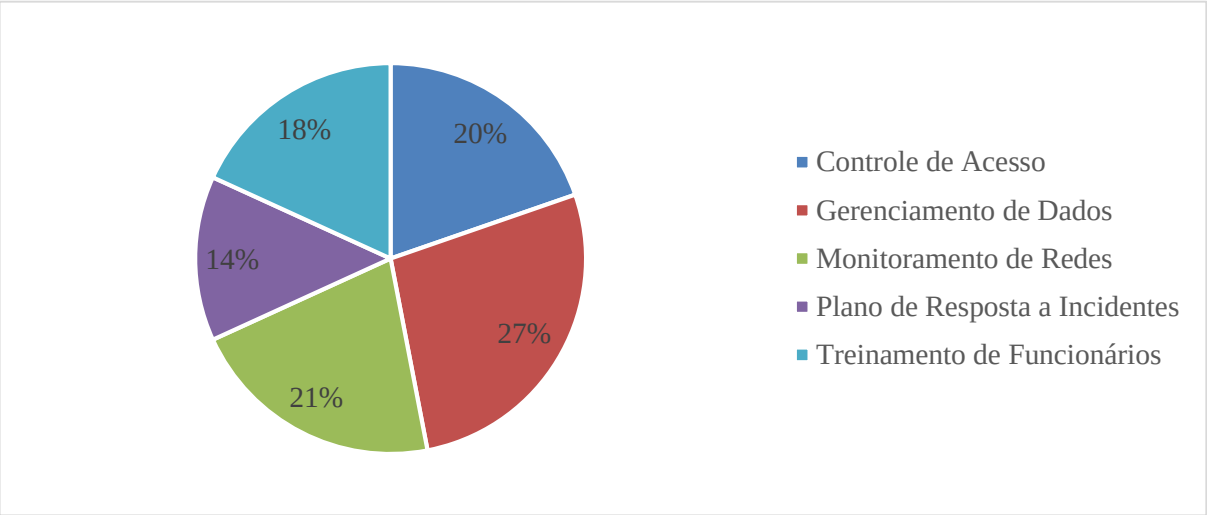
Gráfico 5: Qual a frequência de atualização da PSI.



Fonte: Elaborado pelos autores Matheus Souza e Wherysson Santana (2024)

Podemos notar gráfico 6 que dentre as análises realizadas observa-se que a principal área de abrangência das políticas é o Gerenciamento de dados, mas não exclusivamente, com ênfase também no monitoramento das redes e controle de acessos notamos que as políticas aplicadas abrangem diversas áreas da empresa o que melhora a sua efetividade.

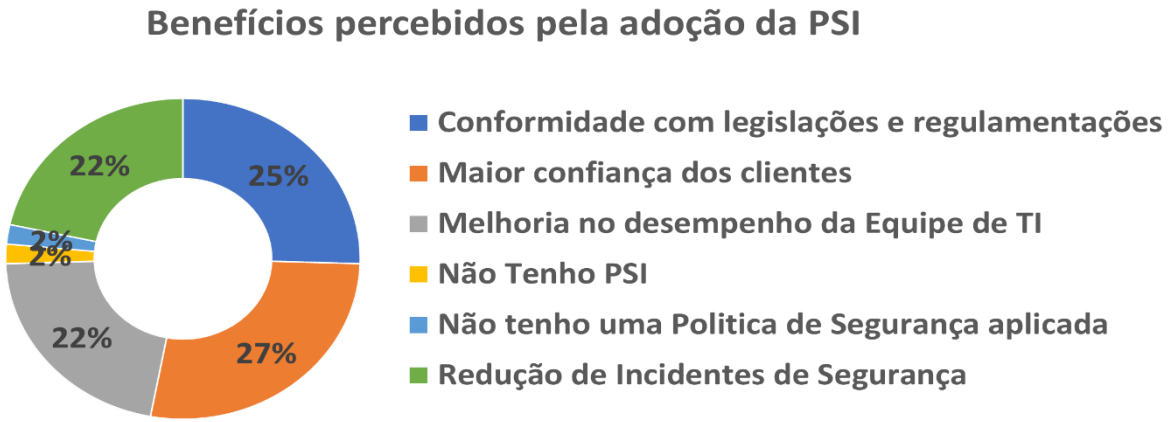
Gráfico 6: A Política de Segurança da Informação cobre quais áreas.



Fonte: Elaborado pelos autores Matheus Souza e Wherysson Santana (2024)

Podemos observar no gráfico 7 que a maioria das empresas participantes deste questionário obtiveram benefícios de uma PSI adequadamente aplicada, 27% dessas empresas tiveram uma maior confiança dos seus clientes, aumentando assim a sua credibilidade no mercado, 25% obtiveram melhores conformidade com as legislações e regulamentações, assim valorizando sua marca e criando referencias, 22% tiveram reduções significativa em incidentes de Segurança, como vazamento de dados ou ataques de phishing e outras 22% das empresas obtiveram desempenho maior na Equipe de TI.

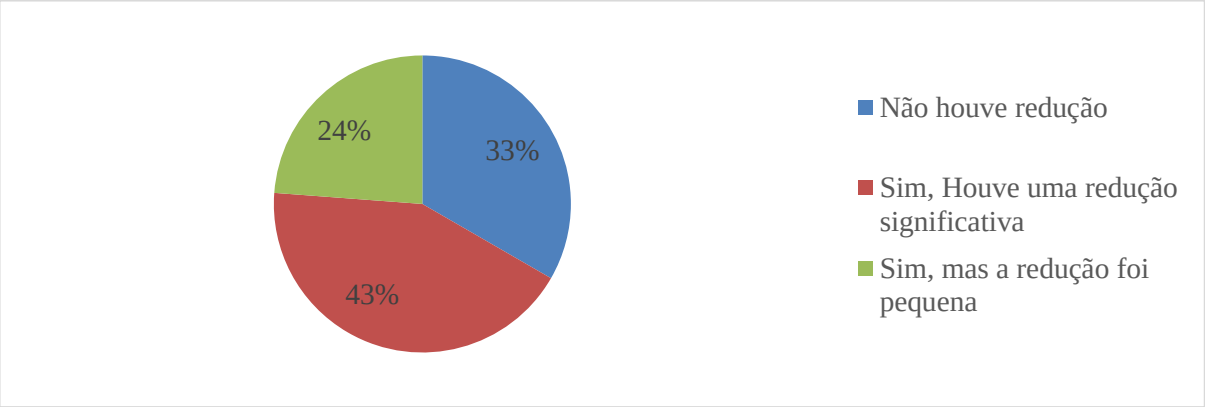
Gráfico 7: Benefícios da adoção da PSI



Fonte: Elaborado pelos autores Matheus Souza e Wherysson Santana (2024)

Podemos verificar no gráfico 8 que grande parte das empresas que aplicaram e mantem uma PSI ativa e atualizada tem uma redução significativa nos custos, porém uma quantidade considerável de 33% das empresas que participaram, porventura não possui ou não está com a PSI ativa e funcional e assim não obtiveram reduções nos custos. E ainda tivemos 24% das empresas participantes que tiveram reduções nos custos porem não de forma significativa.

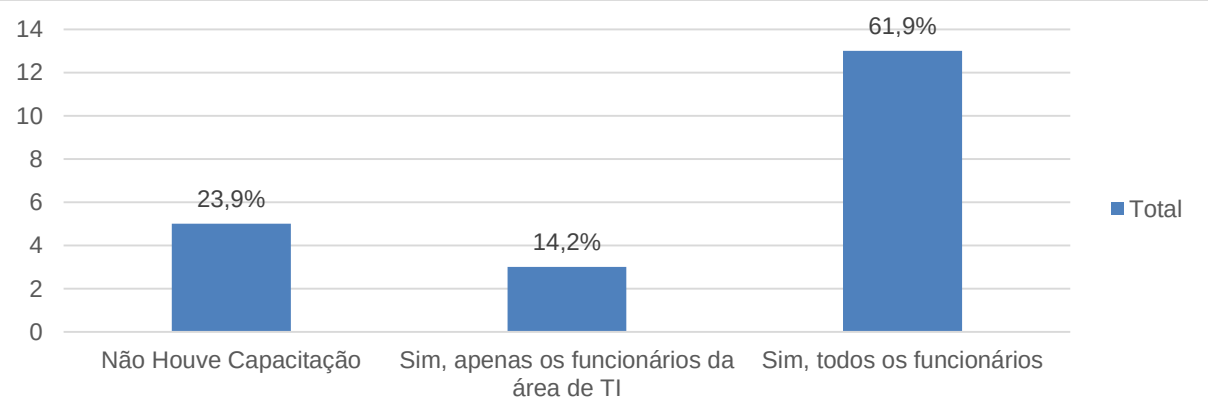
Gráfico 8: Houve reduções em custos relacionados a incidentes de segurança da informação?



Fonte: Elaborado pelos autores Matheus Souza e Wherysson Santana (2024)

Como podemos verificar no gráfico 9 as empresas que possuem PSI ativa e atualizada, prezaram pelo treinamento e conscientização de todos os colaboradores, já empresas que tem uma PSI, porém com o fluxo de atualização demasiado optou por capacitar apenas os colaboradores destinados ao TI. Dentre as 21 empresas, 5 delas ou 23,8% do geral não possuem nenhum tipo de orientação ou capacidade de aplicar as normas de uma PSI.

Gráfico 9: Os funcionários foram capacitados para entender e aplicar as normas da Política de Segurança da Informação?

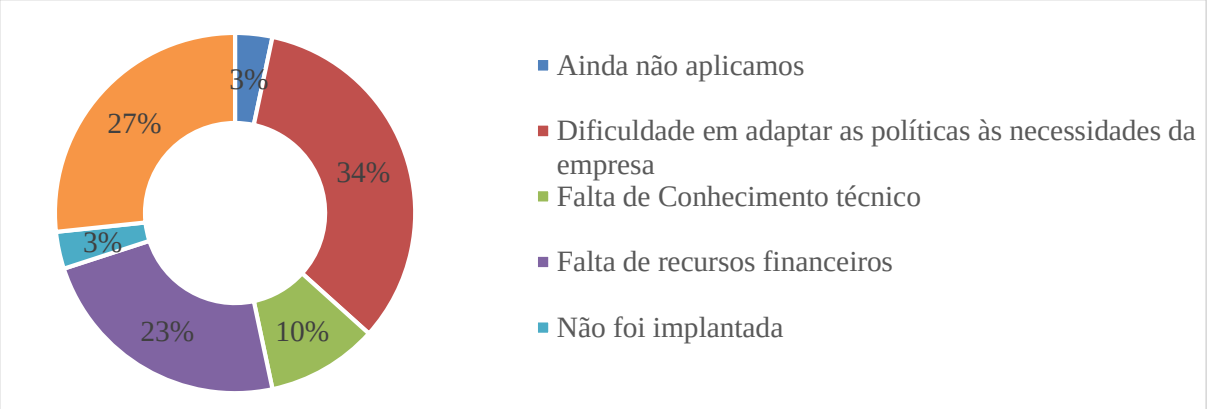


Fonte: Elaborado pelos autores Matheus Souza e Wherysson Santana (2024)

No gráfico 10 podemos observar que as principais dificuldades e desafios na implementação da PSI, 34% das empresas alegam que a dificuldade em adaptar as politicas às

necessidades das empresas e 27% afirma que o maior desafio é a resistência dos funcionários com as mudanças e novos procedimentos e normas. Dando uma ênfase que ainda 23% das empresas diz que a falta de recursos financeiros é umas das principais causas.

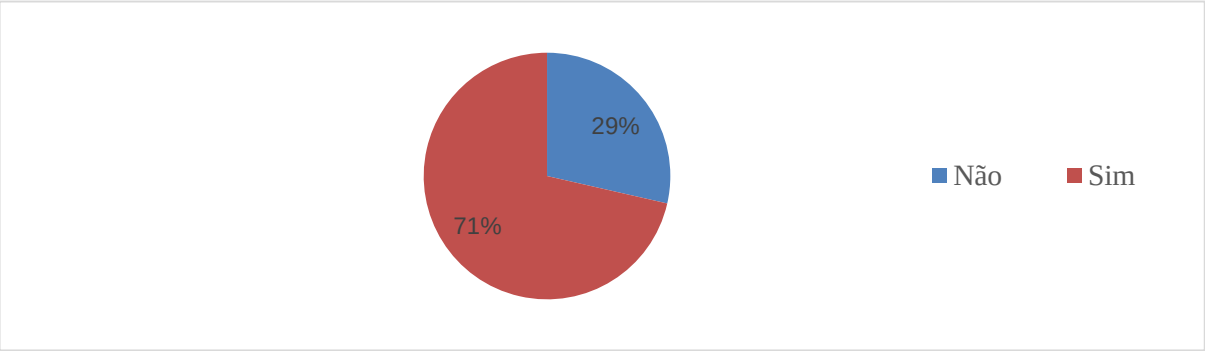
Gráfico 10: Quais foram os principais desafios na implementação da Política de Segurança da Informação.



Fonte: Elaborado pelos autores Matheus Souza e Wherysson Santana (2024)

Conforme aponta o gráfico 11 a grande maioria das empresas, utiliza ou utilizou de ferramentas tecnológicas para suporte no desenvolvimento e implementação da PSI, já 29% das empresas questionadas, alegaram não ter nenhum suporte tecnológico para o desenvolvimento e processo.

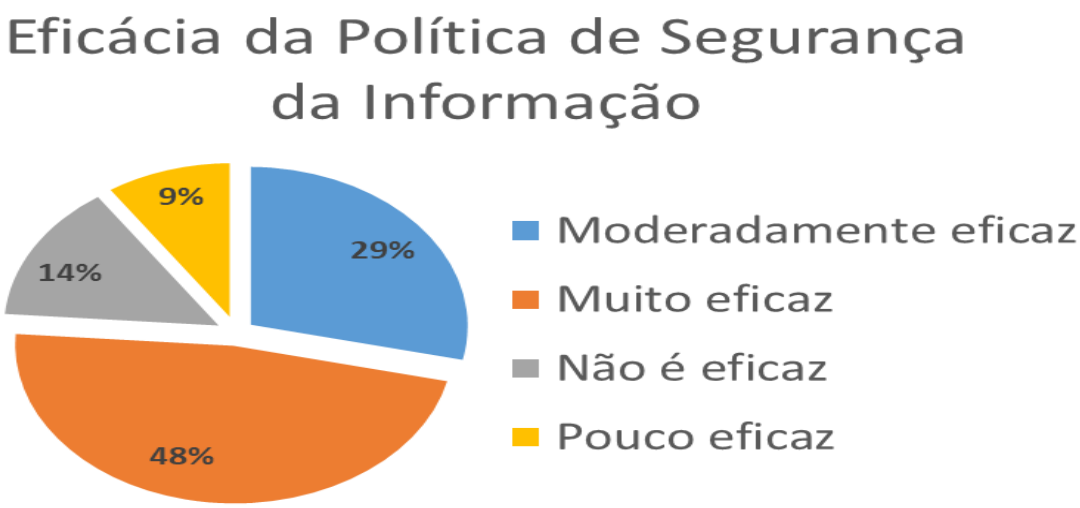
Gráfico 11: As empresas utilizam ferramentas tecnológicas para apoiar a implementação da PSI.



Fonte: Elaborado pelos autores Matheus Souza e Wherysson Santana (2024)

Podemos verificar no gráfico 12 que dentre as empresas notamos que 48% declaram como muito eficaz a aplicação da PSI em suas empresas, 29% declaram como moderadamente eficaz, 14% declaram como não eficaz e apenas 9% declararam como pouco eficaz.

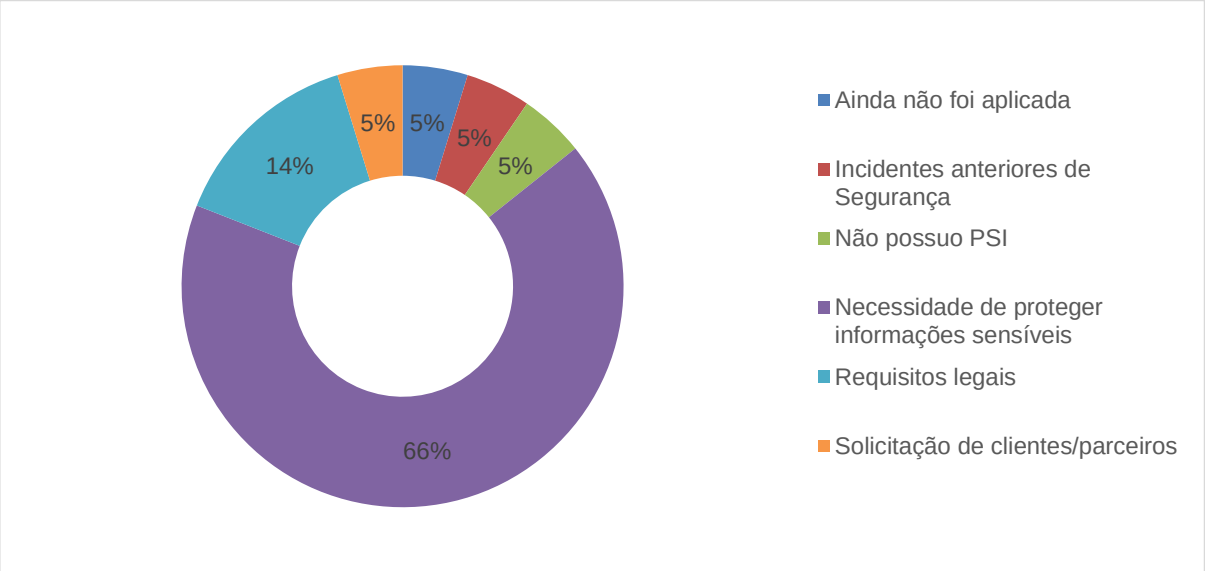
Gráfico 12: Eficácia da PSI nas empresas.



Fonte: Elaborado pelos autores Matheus Souza e Wherysson Santana (2024)

No gráfico 13 podemos notar que 66% das empresas questionadas, o principal motivo para adoção de uma PSI, é necessidade de manutenção e proteção de informações e dados sensíveis de colaboradores, clientes e parceiros. Já outros 14% buscaram a adoção da PSI para cumprimento de requisitos legais e certificações. E 5% justificam incidentes sofridos posteriormente.

Gráfico 13: Qual o motivo da adoção da PSI nas empresas?



Fonte: Elaborado pelos autores Matheus Souza e Wherysson Santana (2024)

5. CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo analisar a implementação de Políticas de Segurança da Informação (PSIs) em pequenas e médias empresas, com foco na conformidade com a LGPD. A pesquisa mostrou que, embora a segurança da informação seja reconhecida como essencial, apenas 30% das pequenas e médias empresas entrevistadas possuem uma PSI formalizada. Os principais desafios enfrentados incluem a falta de recursos financeiros, dificuldades em adaptar as políticas à realidade das empresas e o desconhecimento técnico.

As empresas que adotaram PSIs destacaram benefícios como maior confiança dos clientes e conformidade com a legislação e a pesquisa também evidenciou que empresas com PSIs atualizadas com mais frequência relatam maior eficácia na mitigação de riscos e redução de incidentes de segurança, mostrando a importância de políticas dinâmicas e em constante evolução.

Os resultados da pesquisa mostram uma diferença considerável no nível de maturidade das Políticas de Segurança da Informação (PSIs) adotadas pelas pequenas e médias empresas da região de Araraquara. Um dado preocupante é que somente 67% das empresas entrevistadas disseram ter uma PSI ativa, sendo que 29% delas só fazem atualizações quando consideram realmente necessário. Isso acaba deixando muitas empresas vulneráveis a ataques e problemas de segurança, reforçando a importância de manter essas políticas sempre atualizadas.

Por outro lado, as empresas que têm PSIs bem implementadas e atualizadas relataram benefícios importantes. Por exemplo, 27% delas perceberam um aumento na confiança dos clientes, o que impacta diretamente na imagem da empresa e na sua capacidade de fechar negócios. Já as empresas que ainda não possuem uma PSI ativa enfrentam dificuldades para reduzir custos com incidentes de segurança, como mostram os 33% que relataram não ter obtido nenhuma redução significativa. Esses dados deixam claro que implementar uma PSI eficiente pode ser uma maneira de minimizar prejuízos e melhorar a gestão de riscos.

A pesquisa também destacou alguns dos principais desafios para a implementação de uma PSI. A dificuldade de adaptação das políticas à realidade da empresa foi mencionada por 34% das organizações, enquanto 27% apontaram a resistência dos funcionários às mudanças como uma barreira importante. Esses números mostram que, além de criar as políticas, é essencial trabalhar na conscientização e no treinamento dos colaboradores para garantir que as normas sejam seguidas e que todos entendam a importância da segurança da informação.

Por fim, a principal razão que leva as empresas a adotarem uma PSI, segundo 66% dos entrevistados, é a necessidade de proteger dados sensíveis de colaboradores, clientes e parceiros. Isso reforça que a PSI vai muito além de atender exigências legais, ela é um elemento estratégico para proteger os ativos de informação e garantir a sustentabilidade e o crescimento da empresa.

Aponta-se que a implementação de PSIs é essencial não só por uma exigência legal, mas como um investimento estratégico para a proteção de dados e competitividade. Para superar os desafios, é crucial adotar soluções acessíveis, como ferramentas escaláveis e treinamentos específicos, para facilitar a adesão das pequenas e médias empresas.

O estudo apresenta resultado com bases em amostra regional. Futuras pesquisas podem ampliar o escopo geográfico e investigar como a maturidade organizacional afeta a resiliência a incidentes cibernéticos. Além disso, explorar o uso de tecnologias emergentes, como inteligência artificial, pode aprimorar a eficácia das PSIs.

Em resumo, a política de segurança da informação deve ser vista como um pilar estratégico não só para a sustentabilidade das empresas e sim para a maturidade organizacional e qualidade nos serviços prestados, transformando uma obrigação legal em uma vantagem competitiva, onde trará segurança para o cliente ou parceiro comercial no compartilhamento dos dados e informações sensíveis, sendo assim uma chave essencial para o sucesso da empresa.

REFERÊNCIAS

MENDES, Joyce de Andrade. **Uma Abordagem sobre a Segurança da Informação no mundo atual**. 2021. 61 f. TCC (Graduação) - Curso de M Sistemas de Informação, Universidade Federal do Pará Facomp, Castanhal, 2021. Disponível em: <https://bdm.ufpa.br/handle/prefix/4401>. Acesso em: 03 abr 2024.

ANDRIETA, Caio César. **Políticas de Segurança em Tecnologias da Informação**. 2010. 36 f. Monografia (Especialização) - Curso de Curso de Análise de Sistemas e Tecnologia da Informação, Faculdade de Tecnologia de Americana, Americana, 2010. Disponível em: <http://riccps.eastus2.cloudapp.azure.com/bitstream/123456789/1648/1/20102S_ANDRIETACaioCesar_TCCPD1084.pdf>. Acesso em: 27 mar 2024.

ALEXANDRIA, João Carlos Soares de. **Uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa cientifica**. 2009. 183 f. Tese (Doutorado) - Curso de Gestão da Segurança da Informação, Autarquia Associada À Universidade de São Paulo, São Paulo, 2009. Disponível em:<http://pelicano.ipen.br/PosG30/TextoCompleto/Joao%20Carlos%20Soares%20de%20Alexandria_D.pdf>. Acesso em: 03 abr 2024.

OLIVEIRA, João Paulo de Lima Ribeira de. **Uma questão além da tecnologia**. 2012. 57 f. Monografia (Especialização) - Curso de Segurança da Informação, Universidade Presbiteriana Mackenzie, São Paulo, 2012. Disponível em:<https://adelpha-api.mackenzie.br/server/api/core/bitstreams/8554cd9f-a9e7-4cc1-8dff-49bfa4f12398/content>. Acesso em: 28 mar 2024.

DOS SANTOS, Fernando Cristaldo et al. **Segurança da informação: Sua importância dentro das organizações**. Revista das Faculdades Santa Cruz, v. 10, n. 1, 2019. Disponível em: <https://periodicos.unisantacruz.edu.br/index.php/revusc/article/view/36>. Acesso em: 28 mar 2024.

CNN BRASIL. **Brasil é o 4º país da América Latina com mais ameaças digitais no primeiro semestre de 2024, diz pesquisa**. Disponível em: <https://www.cnnbrasil.com.br/economia/macroeconomia/brasil-e-o-4o-pais-da-america-latina-com-mais-ameacas-digitais-no-primeiro-semestre-de-2024-diz-pesquisa/>. Acesso em: 13 dez. 2024.

CTIC – UNIFESSPA. **Plano de Gestão de Riscos da Tecnologia da Informação e Comunicação.** Disponível em: <https://governancadigital.unifesspa.edu.br/images/Plano_de_gest%C3%A3o_de_riscos_de_TIC.pdf>. Acesso em: 14 dez. 2024.

ABNT- Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 – **Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, ABNT, 2005.

ABNT- Associação Brasileira de Normas Técnicas. NBR ISO/IEC 31000 – **Gestão de Riscos – Princípios e Diretrizes**. Rio de Janeiro, ABNT, 2005.

IFSC – Instituto Federal de Santa Catarina. **Repositório Institucional – Estudos sobre gestão de riscos e segurança da informação**. Disponível em: < https://repositorio.ifsc.edu.br/bitstream/handle/123456789/1668/Analise%20da%20implanta%C3%A7%C3%A3o%20da%20gest%C3%A3o%20de%20riscos%20na%20tecnologia%20da%20informa%C3%A7%C3%A3o%20-%20um%20estudo%20de%20caso.pdf?sequence=1>. Acesso em: 14 dez. 2024.

PORTAL IFB – Instituto Federal de Brasília. **Políticas de segurança da informação: diretrizes e implementação**. Disponível em: < https://ifb.edu.br/attachments/article/3285/POSIC..pdf> Acesso em: 14 dez. 2024.

IFS – Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais. **Benefícios e desafios da segurança da informação em PMEs**. Disponível em: < https://portal.ifs.ifsuldeminas.edu.br/arquivos/paginas/menu_institucional/departamentos/Biblioteca/tcc/TCC_-_Raul_Aparecido_Franco_Simionato.pdf>. Acesso em: 14 dez. 2024.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD). Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 dez. 2024.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm. Acesso em: 15 dez. 2024.

RISK MANAGEMENT STUDIO. **Information Security Challenges in SMEs**. Disponível em: <https://www.riskmanagementstudio.com/information-security-challenges-in-smes/>. Acesso em: 15 dez. 2024.

THE FINANCIAL DAILY. **Cybersecurity challenges for Small and Medium-Sized Businesses (SMBs)**. Disponível em: <https://thefinancialdaily.com/cybersecurity-challenges-for-small-and-medium-sized-businesses-smbs/>. Acesso em: 15 dez. 2024.

DEMANDTEQ. **Key Cybersecurity Challenges Facing Small Businesses**. Disponível em: <https://demandteq.com/key-cybersecurity-challenges-facing-small-businesses/>. Acesso em: 15 dez. 2024.

ALMEIDA, J. R.; CUNHA, P. A.; MELO, T. F. **A importância da conformidade com a ISO/IEC 27002 nas organizações**. Revista de Gestão e Tecnologia, v. 13, n. 6, p. 45-60. DOI: 10.9876/rgt.2019.013.

FERREIRA, J. F.; RIBEIRO, D. A.; COSTA, R. B. **O papel da ISO 27002 na proteção de dados em conformidade com a LGPD**. Revista Brasileira de Segurança da Informação, v. 7, n. 1, p. 22-37. DOI: 10.3456/rbsi.2020.007.

LIMA, F. A.; OLIVEIRA, R. L.; CARDOSO, M. T. **Relatórios de impacto à proteção de dados na LGPD: implicações práticas para as empresas**. Revista de Direito e Proteção de Dados, v. 5, n. 4, p. 110-125. DOI: 10.3456/rdpd.2020.005.

BASTOS, A. J.; SANTOS, P. C.; MEDEIROS, C. D. **Governança de dados e conformidade com a LGPD: um estudo sobre os Relatórios de Impacto**. Revista de Proteção de Dados e Privacidade, v. 6, n. 3, p. 60-75. DOI: 10.4321/rpd.2019.006.

SIPAT. (2023). **Qual é a diferença entre CIPA e SIPAT?** SuperSIPAT. Disponível em: <https://supersipat.com.br/qual-e-a-diferenca-entre-cipa-e-sipat/#:~:text=Concluindo%3A%20a%20diferen%C3%A7a%20entre%20SIPAT,encarregada%20em%20organizar%20a%20SIPAT>. Acesso em: 15 dez. 2024