SEGURANÇA DA INFORMAÇÃO NO CONTEXTO EMPRESARIAL: UMA ANÁLISE DAS LACUNAS NA APLICAÇÃO DE POLÍTICAS E TREINAMENTOS

INFORMATION SECURITY IN THE BUSINESS CONTEXT: AN ANALYSIS OF THE GAPS IN THE APPLICATION OF POLICIES AND TRAINING

Cíntia Maria da Costa Duarte
Faculdade de Tecnologia de Araraquara Prof. José Arana Varela
cintia.duarte@fatec.sp.gov.br

André Castro Rizo
Faculdade de Tecnologia de Araraquara Prof. José Arana Varela
andre.rizo@fatec.sp.gov.br

Resumo

Este trabalho analisou a influência do fator humano nas vulnerabilidades de segurança da informação em 19 empresas do interior de São Paulo, utilizando uma abordagem quantitativa. Os resultados mostraram uma grande lacuna entre o conhecimento teórico e a aplicação prática das medidas de segurança. Apesar do reconhecimento da importância da segurança da informação, muitas empresas não possuíam políticas formalizadas nem programas de treinamento eficazes. A pesquisa também apontou a falta de planos de recuperação de incidentes e a baixa conscientização sobre a Lei Geral de Proteção de Dados, expondo as organizações a riscos elevados. Conclui-se que a proteção dos ativos digitais depende do engajamento dos colaboradores e da criação de uma cultura robusta de segurança.

Palavras-chave: fator humano, segurança da informação, plano de recuperação, vulnerabilidades.

Abstract

This study analyzed the influence of the human factor on information security vulnerabilities in 19 companies in the interior of São Paulo, using a quantitative approach. The results showed a large gap between theoretical knowledge and the practical application of security measures. Despite the recognition of the importance of information security, many companies did not have formalized policies or effective training programs. The survey also pointed to a lack of incident recovery plans and low awareness of the General Data Protection Law, exposing organizations to high risks. The conclusion is that the protection of digital assets depends on employee engagement and the creation of a robust security culture.

Keywords: *human factor, information security, recovery plan, vulnerabilities.*

1. Introdução

A Segurança da Informação (SI) é um tema crucial na era digital, com a crescente dependência tecnológica da sociedade, se tornou um pilar fundamental para a proteção de dados confidenciais em todos os setores.

Gonçalves (2014), diz que a SI se refere à proteção de determinados dados, com a intenção de preservar seus valores para uma organização ou indivíduo. Ela garante que as informações estejam protegidas contra acessos não autorizados.

Apesar dos avanços tecnológicos em ferramentas como *firewalls* e criptografias, a SI não se resume apenas a essas medidas. O Fator Humano emerge como elemento fundamental neste tema e quando negligenciado, pode se tornar a principal porta de entrada para ataques.

Como reafirma Mitnick e Simon (2003 *apud* Freire *et. al*, 2017, p. 147), quando dizem que o fator humano é considerado a parte mais relevante na gestão de SI, como também o elemento mais fraco da segurança. Sendo assim, a quebra de SI, a partir das vulnerabilidades humanas, passa a ser cada vez mais presente devido ao baixo custo para implementação dos ataques.

O cuidado com a SI se tornou uma preocupação essencial em todos os âmbitos, seja no ambiente organizacional ou pessoal. Com o constante aumento da quantidade de dados digitais e a crescente dependência da tecnologia nas operações comerciais e governamentais, a proteção dessas informações se tornou crucial.

Segundo Fernandes (2018), a informação é um Ativo muito desejado e valioso tanto para uma pessoa como para uma organização, devendo obrigatoriamente estar protegido de acessos não autorizados.

Além disso, a crescente complexidade tecnológica exige uma abordagem proativa e contínua para proteger informações sensíveis. Novas ameaças e vulnerabilidades surgem constantemente, exigindo uma contínua atualização e adaptação das estratégias de segurança. Os ataques cibernéticos estão se tornando mais fortes e frequentes. Essas ameaças podem levar as empresas ao risco de não conformidade com a Lei Geral de Proteção de Dados (LGPD). Enquanto a Inteligência Artificial (IA) e o aprendizado de máquina oferecem novas oportunidades para detectar e mitigar ameaças, novas tecnologias são criadas para atacar e

invadir não só por meio de máquinas, mas, também, por meio de humanos. Sendo assim, se confirma o que o estudo de Mitnick e Simon (2003) diz, o elo mais fraco na cadeia de segurança é o fator humano. Erros, negligências, má conduta, falta de informação, podem comprometer a Integridade, a Disponibilidade e a Confidencialidade que são os principais pilares da SI.

"Proteger a informação é responsabilidade de cada pessoa na organização, independentemente de seu nível hierárquico! Do mais alto executivo ao mais novo estagiário" (Gonçalves, 2014).

Este trabalho tem como objetivo explorar a influência do fator humano nas vulnerabilidades de SI, focando em como comportamentos e atitudes impactam a segurança organizacional. Por meio de uma pesquisa quantitativa, buscamos identificar boas práticas que podem ser adotadas para mitigar esses riscos, destacando a importância de um ambiente de segurança que não dependa apenas da tecnologia, mas, que também envolva a educação e conscientização dos usuários.

2. Referencial Teórico

A metodologia de coleta de definição de termos e conceitos correlatados a SI e Fator Humano, foi a pesquisa bibliográfica em artigos, livros e periódicos especializados.

2.1 Segurança da Informação

A SI é a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação não-autorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (NBR 17999, 2003; Dias, 2000; Wadlow, 2000; Krause e Tipton, 1999).

A SI é um campo multidisciplinar que visa proteger as informações de uma organização, garantindo sua confidencialidade, integridade e disponibilidade. No contexto atual, onde a tecnologia permeia todos os aspectos da vida cotidiana e organizacional, a SI se torna um requisito indispensável para a proteção de dados críticos e sensíveis.

Segundo Gonçalves (2014), a SI envolve um conjunto de práticas e políticas que buscam proteger dados contra ameaças internas e externas. Essas práticas incluem a implementação de controles técnicos, como firewalls, criptografia, e o uso de tecnologias de detecção de intrusão, além de políticas de segurança que orientam o comportamento dos colaboradores. A eficácia da SI não depende apenas da tecnologia, mas também da conscientização e educação dos usuários sobre os riscos e boas práticas de segurança.

Além disso, a ISO/IEC 27001 é uma norma internacional que fornece um quadro para a implementação de um Sistema de Gestão de SI (SGSI). Ela define requisitos para estabelecer, implementar, manter e melhorar continuamente um SGSI, garantindo que as organizações protejam suas informações de maneira sistemática e eficaz (ISO/IEC, 2013).

A crescente quantidade de dados digitais e a intensificação das ameaças cibernéticas tornam a SI ainda mais relevante. Em um estudo realizado por Anderson (2008), é destacado que a SI deve ser vista como um investimento estratégico, não apenas como um custo. A implementação de políticas e tecnologias de segurança eficazes pode prevenir perdas financeiras e danos à reputação, além de garantir a conformidade com regulamentações, como a LGPD no Brasil.

Os ataques cibernéticos estão se tornando cada vez mais sofisticados. De acordo com um relatório da *Cybersecurity & Infrastructure Security Agency* (CISA, 2020), as ameaças mais comuns incluem *phishing*, *ransomware* e ataques de negação de serviço (DDoS). Essas ameaças frequentemente exploram vulnerabilidades humanas, reforçando a ideia de que a SI deve incluir um componente educativo significativo, que envolva o treinamento e a conscientização dos colaboradores.

Em resumo, a SI é um componente crítico para a proteção de ativos informacionais em qualquer organização. Com a evolução constante do cenário de ameaças e a necessidade de adaptação a novas tecnologias, a abordagem em relação à SI deve ser proativa e contínua. É vital que as organizações adotem uma mentalidade de segurança em toda a estrutura, integrando aspectos tecnológicos, humanos e organizacionais.

2.2 Confidencialidade, Integridade e Disponibilidade

Segundo a ISO 27001, os três pilares da SI são definidos como:

Confidencialidade: Esta característica assegura que a informação é acessível apenas para aqueles que têm autorização para acessá-la. A confidencialidade é essencial para proteger dados sensíveis, como informações pessoais e segredos comerciais. Medidas comuns para garantir a confidencialidade incluem o uso de criptografia e controles de acesso que limitam o compartilhamento de informações apenas aos usuários autorizados (IT Governance, 2023).

Integridade: A integridade refere-se à precisão e consistência da informação ao longo do tempo. É crucial que os dados sejam protegidos contra alterações não autorizadas, que podem ocorrer por erros humanos ou ataques cibernéticos. A manutenção da integridade é alcançada por meio de controles como auditorias e verificações de dados (IT Security HQ, 2023).

Disponibilidade: Este princípio garante que as informações e os sistemas estejam acessíveis e operacionais quando necessário. A disponibilidade pode ser comprometida por falhas de hardware ou desastres naturais. Para garantir a disponibilidade, as organizações implementam soluções como backups regulares e planos de recuperação de desastres (IT Governance, 2023; IT Security HQ, 2023) .

2.3 Vulnerabilidade

No contexto da SI, vulnerabilidade refere-se a qualquer fraqueza em sistemas, processos ou pessoas que pode ser explorada por agentes maliciosos para comprometer a integridade, confidencialidade ou disponibilidade de dados. Segundo Tariq *et. al*, (2023), as vulnerabilidades podem surgir de falhas técnicas, como erros de codificação e configurações inadequadas, ou de fatores humanos, como falta de conhecimento e negligência. Essas falhas permitem que atacantes acessem sistemas, alterem informações ou causem interrupções em serviços essenciais. A identificação e mitigação de vulnerabilidades são etapas críticas na SI, sendo essencial para a redução de riscos (MPDI, 2022).

Além disso, Von Solms e Van Niekerk (2013) destacam que as vulnerabilidades podem ser exploradas de várias formas, desde ataques de negação de serviço até explorações complexas envolvendo redes interconectadas, como no caso da Internet das Coisas (IoT). A

segurança nesses ambientes exige uma abordagem que combine práticas técnicas, como atualizações e monitoramento contínuo, com conscientização e treinamento humano (MDPI, 2022).

2.4 Fator Humano

O termo fator humano, conforme definido por Wang (2008), refere-se aos papéis e efeitos das atividades humanas em um sistema, introduzindo forças, fraquezas e incertezas adicionais. Em sistemas de informação e Tecnologia da Informação (TI), isso implica que o ser humano, como componente principal, exerce influência direta no nível de segurança.

O estudo de Triplett (2022) destaca que a gestão dos fatores humanos é crucial para a eficácia da segurança. Os comportamentos dos indivíduos, suas interações com sistemas de informação e o contexto social em que operam são determinantes nas vulnerabilidades que as organizações enfrentam. O estudo sugere que, para mitigar riscos, é essencial implementar treinamentos e estratégias de conscientização, pois muitas vulnerabilidades surgem de erros não intencionais e comportamentos complacentes dos usuários.

Além disso, Cano (2019) reforça que, apesar de investimentos em tecnologia e processos, a natureza humana frequentemente leva a falhas de segurança. Muitas vezes, as organizações não conseguem alinhar suas expectativas de segurança com as ações reais dos funcionários, resultando em brechas de segurança (ISACA, 2019). Assim, é fundamental que as empresas desenvolvam uma cultura de segurança que reconheça e integre o fator humano como um componente vital na proteção de ativos de informação.

2.5 Engenharia Social

A engenharia social é uma técnica de manipulação psicológica utilizada para induzir indivíduos a realizar ações que comprometam a SI. Diferente de ataques diretos a sistemas, essa abordagem foca no fator humano, explorando a confiança e a vulnerabilidade das pessoas. Segundo Mitnick e Simon (2003), a engenharia social se baseia na capacidade de persuadir ou enganar um usuário, levando-o a fornecer informações confidenciais ou a realizar ações prejudiciais à segurança.

Ainda segundo Mitnick e Simon (2003, p. 4) podemos ter a seguinte afirmação sobre Engenharia Social:

> À medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar a "*firewall* humana" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo.

Os métodos utilizados para ataques de engenharia social podem ocorrer de diversas formas, como por exemplo:

Phishing: Também conhecido como pesca é a técnica mais utiliza. É um tipo de ataque que envolve o envio de mensagens fraudulentas, geralmente via e-mail ou SMS, que passam por fontes confidenciais para induzir a vítima a fornecer informações sensíveis, como senhas, documentos e outros. (Piovesan, 2019).

Pretexting: O atacante cria um cenário fictício para convencer a vítima a compartilhar informações impactantes. Um exemplo é o fraudador que passa por um profissional de suporte técnico para obter acesso a uma conta de e-mail corporativo. Estudos mostram que esse tipo de ataque é eficaz devido à tendência humana de obedecer a figuras de autoridade (Mitnick e Simon, 2003).

Baiting: envolve o uso de iscas físicas ou digitais, como pendrives infectados ou links para downloads, que ao serem acessados instalam *malware* nos dispositivos das vítimas. Essas práticas exploram a curiosidade e a ganância das pessoas, tornando-as vulneráveis ao roubo de informações e ao comprometimento de sistemas (Hadnagy, 2018).

3. Metodologia

A metodologia de coleta de definição de termos e conceitos correlatos a SI e Fator Humano, foi a pesquisa bibliográfica em artigos, livros e periódicos especializados.

A presente pesquisa tem como objetivo analisar a influência do fator humano nas vulnerabilidades de SI em empresas de diversos setores. Para tanto, foi adotada uma abordagem quantitativa, utilizando um questionário como principal instrumento de coleta de dados.

A pesquisa quantitativa foi escolhida para este estudo devido à sua capacidade de quantificar e analisar variáveis de forma estruturada e objetiva, buscando identificar padrões e

relações entre os dados coletados. Segundo Creswell (2014), esse tipo de pesquisa é caracterizado pelo uso de métodos estatísticos que auxiliam na interpretação de dados numéricos, com o propósito de explorar correlações e variáveis específicas de um específico. Gil (2008) ressalta que a pesquisa quantitativa é essencial para análises que exigem objetividade e precisão, utilizando questionários e escalas que permitem obter respostas mensuráveis e representativas. Babbie (2003) reforça a importância da pesquisa quantitativa, destacando que ela possibilita a validação de hipóteses por meio de amostras amplas e representativas, ampliando a confiabilidade

O questionário[1] aplicado de forma online abordou diversos aspectos e após a coleta dos dados, estes foram organizados para análise estatística. Participaram deste estudo 19 empresas localizadas no interior de São Paulo, abrangendo diferentes portes, como pequeno e médio. Incluindo empresas dos ramos alimentício, escolar, prestação de serviços e outros âmbitos. Essa diversidade foi essencial para garantir uma análise representativa dos desafios de SI enfrentados por organizações de perfis variados. Essa amostra permite avaliar a influência do fator humano na segurança de empresas com recursos e necessidades específicas, contribuindo para um panorama mais completo do setor empresarial na região.

A pesquisa explorou aspectos cruciais sobre o conhecimento e as práticas de SI nas empresas participantes. Foram levantadas questões sobre o entendimento dos colaboradores em relação ao conceito de SI e ameaças como a engenharia social, além de práticas institucionais, como a presença de políticas de segurança e treinamentos. Também foram abordadas as percepções sobre a importância da conscientização em segurança e a priorização do fator humano. Por fim, perguntas sobre orçamento e estratégias de recuperação indicaram a preparação dessas empresas para responder a incidentes, refletindo os desafios que enfrentarão para equilibrar recursos e conscientização.

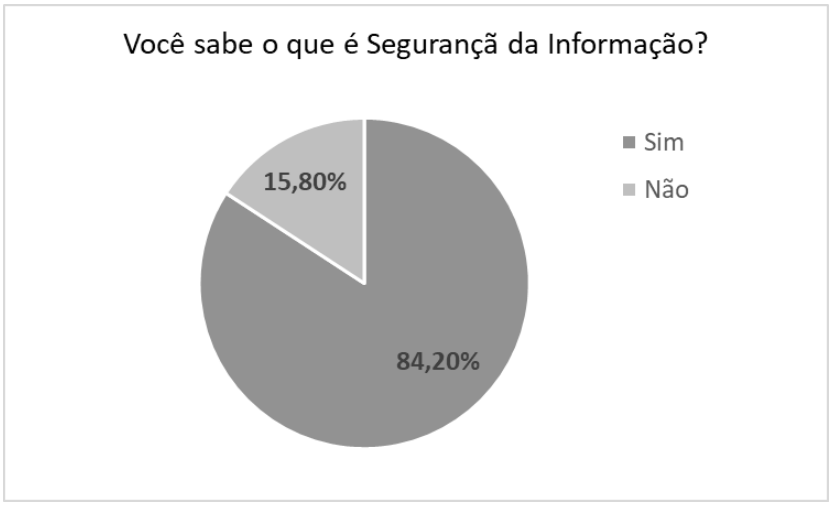
[1] Link para o questionário: https://docs.google.com/forms/d/1DZjrZDZa3tX7-M8r2p7jK5qvUN5gFW0GU2Tl262fb9M/edit?pli=1

4. Resultados e Discussões

Este capítulo apresenta a análise dos dados coletados na pesquisa, discutindo os principais achados e suas implicações para o entendimento das vulnerabilidades relacionadas ao fator humano na SI. Esta análise visa identificar padrões e discrepâncias nas respostas, buscando evidenciar como a conscientização e as políticas de segurança influenciam a postura dessas organizações frente aos riscos.

Conforme Figura 1 os resultados da pesquisa revelam um alto nível de conhecimento sobre o conceito de SI entre os participantes.

Figura 1 - Você sabe o que é SI?

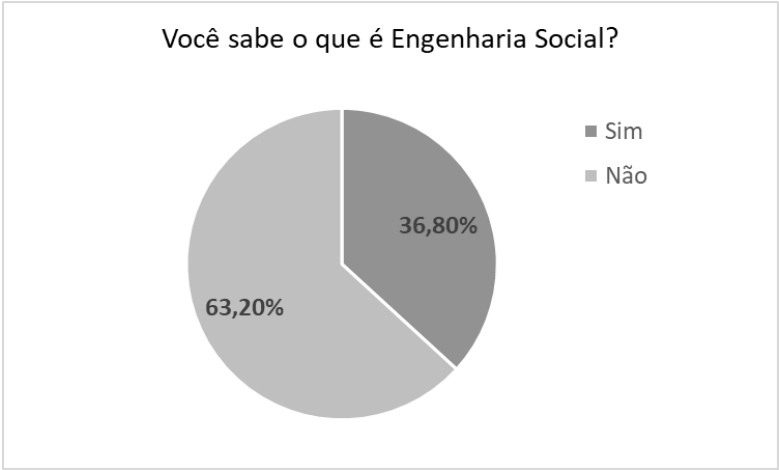


Fonte: Os Autores (2024)

Essa percepção positiva indica que as campanhas de conscientização têm sido eficazes em disseminar informações básicas sobre o tema. No entanto, é importante aprofundar a análise para verificar se esse conhecimento se traduz em práticas seguras.

Na Figura 2 por outro lado, evidencia-se uma lacuna significativa no conhecimento dos participantes sobre engenharia social, com apenas 36,6% os entrevistados afirmando estarem familiarizados com o conceito, enquanto 63,2% desconhecem essa ameaça.

Figura 2 – Você sabe o que é Engenharia Social?



Fonte: Os Autores (2024)

A engenharia social, sendo uma das táticas mais comuns e eficazes para explorar falhas humanas e obter informações úteis, representa um risco relevante para a SI. Essa carência de conhecimento indica a necessidade urgente de treinamento específico, capacitando os colaboradores a identificar e se defenderem contra essas práticas.

A Figura 3 revela que uma parte específica das empresas não possui uma política de SI formalizada, com apenas 42,1% dos participantes registrando sua existência.

Figura 3 – Porcentagem de Política de SI definida.

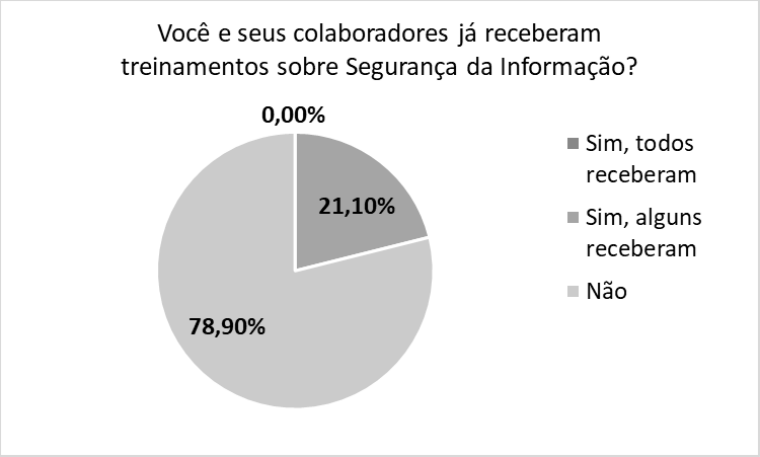
Fonte: Os Autores (2024)

A ausência de uma política clara prejudica a uniformidade das práticas de segurança e torna o ambiente mais suscetível a falhas. Além disso, a falta de clareza entre os colaboradores

sobre a presença dessa política destaca a necessidade urgente de as empresas investirem em um quadro estruturado, assim como em comunicação e conscientização mais eficazes.

Um aspecto fundamental para a SI nas empresas é o treinamento dos colaboradores. Sem essa capacitação, eles se tornam suscetíveis a erros, o que eleva a vulnerabilidade da empresa. A Figura 4 mostra algo alarmante, pois nenhuma das empresas realizou treinamento de segurança com todos os colaboradores resultando em um percentual de 0. Enquanto, 78,9% afirmam que não houve nenhum treinamento e somente 21,1% dos entrevistados garantem que pelo menos alguns dos colaboradores receberam treinamento.

Figura 4 – Treinamento.

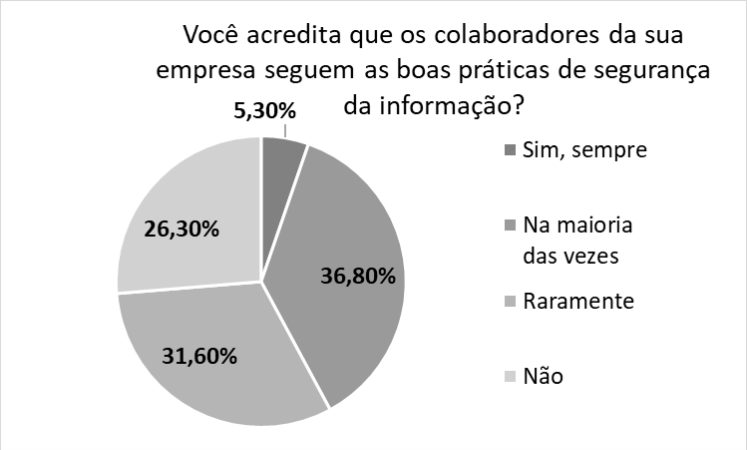


Fonte: Os Autores (2024)

A ausência de capacitação formal significa que os colaboradores estão desprovidos de habilidades e conhecimentos práticos para lidar com ameaças de segurança. Esse dado evidencia que a falta de treinamento contínuo contribui para a vulnerabilidade organizacional, pois os funcionários não têm orientações claras para proteger as informações corretamente.

Em relação a Figura 5 já é possível observar os impactos identificados no gráfico anterior. Isso indica que, à medida que o número de colaboradores que recebem treinamento diminui, a adesão às boas práticas também se reduz. Apenas 5,3% dos entrevistados afirmam que as boas práticas são sempre seguidas, enquanto 31,6% indicam que elas raramente são e 26,3% acreditam que não.

Figura 5 – Boas práticas dos colaboradores.

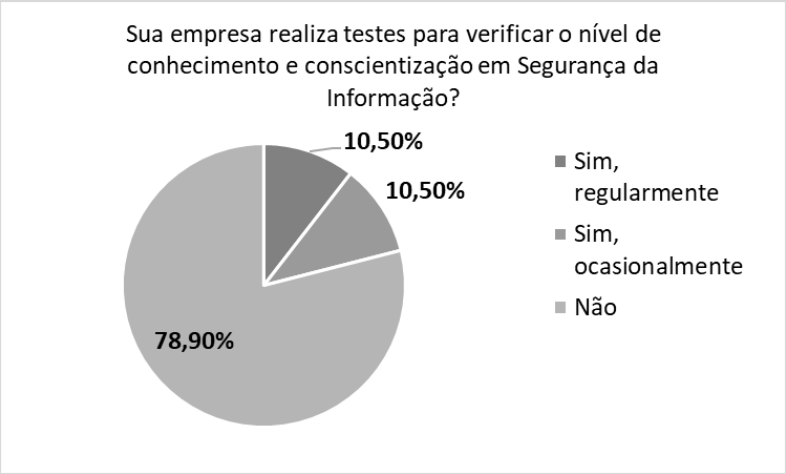


Fonte: – Os Autores (2024)

Esses dados sugerem que, mesmo que existam práticas recomendadas, elas ocasionalmente são implementadas e seguidas. Esse cenário é reflexo da falta de disciplina ou de consciência sobre a importância dessas práticas, reforçando que o comportamento humano é um ponto crítico para a SI.

Para determinar se os colaboradores estão aderindo às boas práticas que raramente são instruídas nos treinamentos, é essencial que as empresas realizem testes para avaliar o nível de conscientização de cada colaborador. E a Figura 6 mostra que, 78,9% das empresas não realizam estes testes. E apenas 10,5% realizam regularmente.

Figura 6 – Realização de testes.

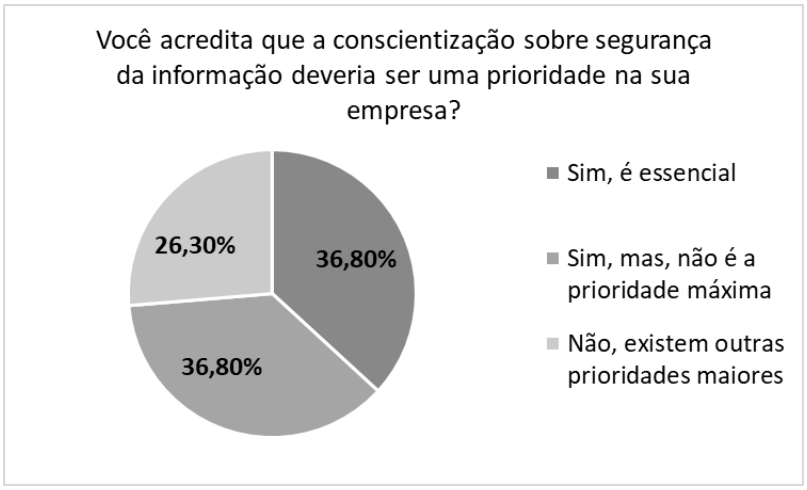


Fonte: Os Autores (2024)

Se não houver uma política claramente definida e implementada, e se as boas práticas e treinamentos não forem estabelecidos, os testes não poderão ser executados corretamente e nem poderão ter resultados positivos, pois os colaboradores não terão compreensão adequada sobre o tema. Com isto, percebe-se uma falta de acompanhamento e avaliação do conhecimento dos colaboradores sobre SI. Essa ausência de testes dificulta a identificação de lacunas no entendimento e na prática de segurança, mostrando que sem uma avaliação contínua, a vulnerabilidade ao erro humano permanece alta.

Com as informações do gráfico anterior, surge a questão sobre a conscientização em SI ser ou não uma prioridade na empresa. Surpreendentemente, como observa-se na Figura 7, 28,3% dos entrevistados acreditam que existem outras prioridades que se sobrepõem a essa questão. No entanto, a SI deve ser tratada com a mesma importância que as demais prioridades, uma vez que os impactos de sua negligência podem ser grandiosos.

Figura 7 – Prioridade de conscientização.



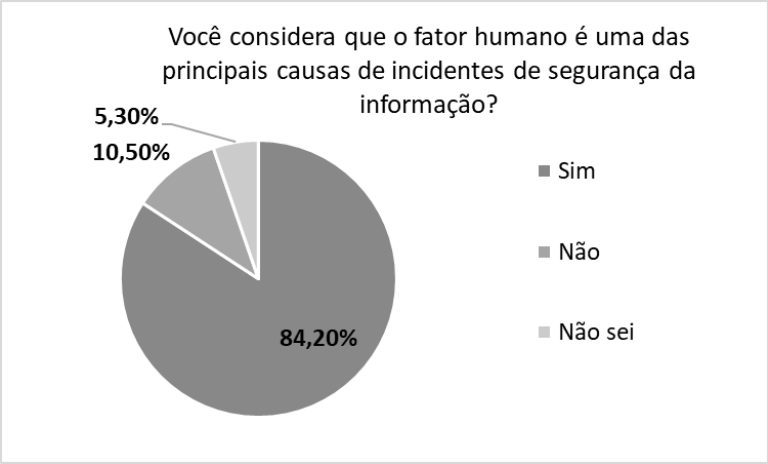
Fonte: Os Autores (2024)

Essa visão subestima os riscos de segurança, levando à falta de comprometimento com as práticas de proteção necessárias, o que aumenta a vulnerabilidade da organização.

A pesquisa revela que os entrevistados reconhecem e acreditam que o fator humano é uma das principais causas de incidentes de segurança com 84,2%. Como podemos observar na Figura 8. Isso demonstra a urgência de modificar os resultados apresentados anteriormente.

É fundamental que os colaboradores estejam cientes quando estão sendo alvo de tentativas de golpes de engenharia social. Ou seja, essa constatação reforça a necessidade de investir em programas de treinamento e conscientização para mitigar os riscos associados ao comportamento dos usuários.

Figura 8 – Fator humano como causa de incidentes.

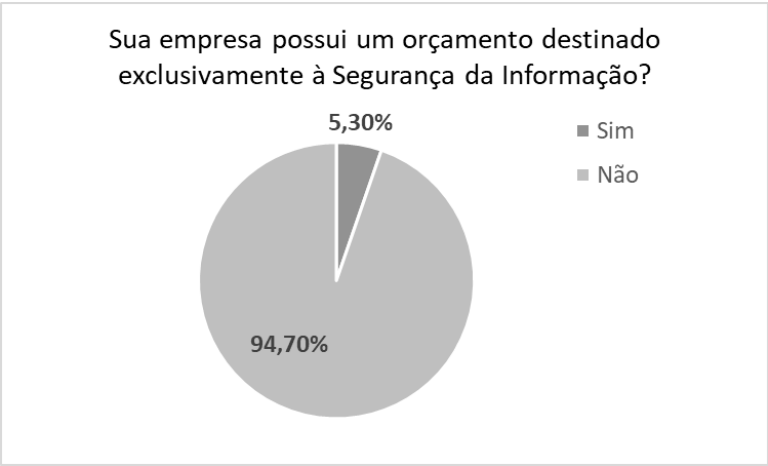


Fonte: Os Autores (2024)

Nas imagens a seguir, pode-se observar como os resultados anteriores são impactados pelos números apresentados. As empresas falham em tratar a SI com a devida prioridade, o que se traduz em investimentos inadequados para esta área.

A Figura 9 revela a esmagadora maioria de afirmantes (94,7%) que não possuem um orçamento exclusivo para SI.

Figura 9 – Orçamento exclusivo para SI.

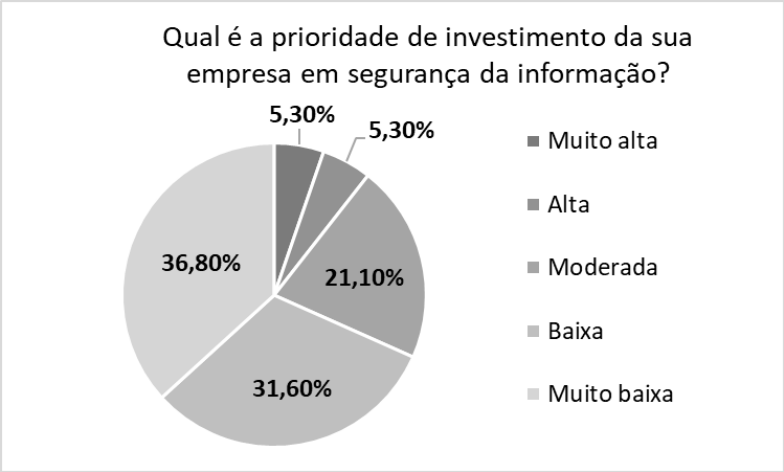


Fonte: Os Autores (2024)

A falta de recursos destinados à segurança limita a implementação de tecnologias e treinamentos que poderiam reduzir a vulnerabilidade do fator humano. Esse cenário destaca a necessidade de reavaliar a importância da segurança no orçamento organizacional.

Como consequência, a Figura 10 possibilita enxergar que a maioria das empresas realmente não trata a SI como uma das prioridades na organização e por sua vez, não possuem o orçamento exclusivo para ela, pois a prioridade de investimento é considerada muito baixa ou baixa por 68,4% dos entrevistados, evidenciando então uma priorização insuficiente.

Figura 10 – Prioridade de Investimento.



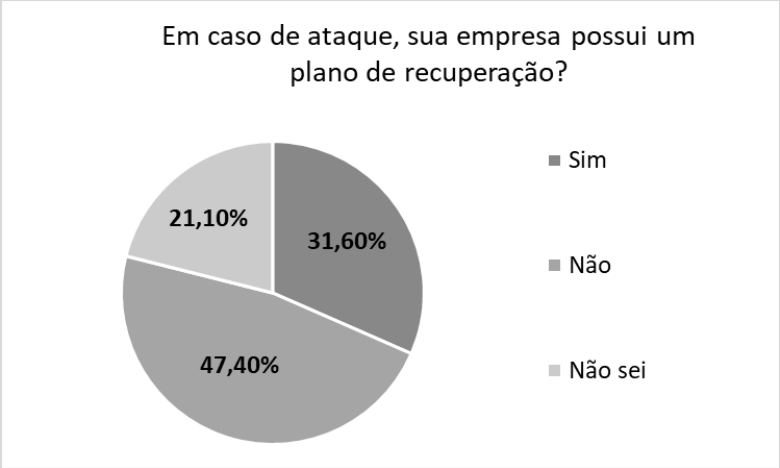
Fonte: Os Autores (2024)

Essa postura pode ser atribuída à falta de percepção do risco real, reforçando que o baixo investimento financeiro reflete uma baixa conscientização do impacto das vulnerabilidades causadas pelo fator humano.

As próximas imagens irão demonstrar que, apesar de as empresas estarem cientes do que é SI, muitas não compreendem o impacto potencial de um incidente. O vazamento de dados sensíveis por exemplo, é uma questão extremamente complexa que viola a LGPD e pode acarretar severos problemas.

Pode-se observar na Figura 11 que menos de um terço das empresas possui um plano de recuperação, enquanto 47,4% não têm esse recurso e 21,1% desconhecem a existência dele. Esses dados demonstram a falta de preparação para lidar com incidentes de segurança e gravidade de seus impactos.

Figura 11 – Plano de Recuperação.

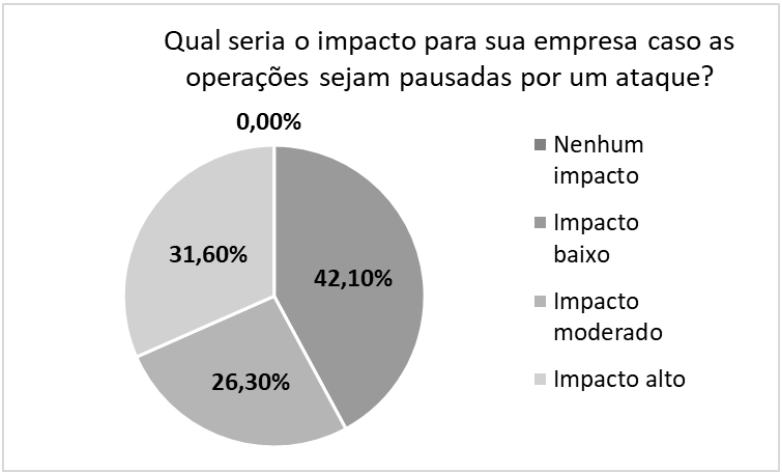


Fonte: Os Autores (2024)

A ausência de um plano de recuperação bem definido aumenta o tempo de resposta em caso de ataques, o que pode levar a perdas financeiras e reputacionais preocupantes.

A Figura 12 evidencia que os participantes não têm plena clareza sobre o que constitui um incidente de segurança. Apesar de lidarem com informações sensíveis, especialmente relacionadas a menores de idade, e dados confidenciais de clientes em diversos setores, a maioria (70,4%) ainda considera que o impacto de tais incidentes seria baixo ou moderado enquanto somente 31,6% considera este impacto como alto.

Figura 12 – Nível de Impacto.



Fonte: Os Autores (2024)

Esse reconhecimento sobre o impacto de interrupções aponta para a importância de medidas preventivas e conscientização urgentes. No entanto, o fato de muitos considerarem o impacto baixo pode indicar um subestimado entendimento sobre o que realmente causaria um ataque e paralização de seus serviços.

A análise dos dados revela uma discrepância significativa entre o conhecimento teórico dos colaboradores sobre SI e a aplicação prática de boas práticas de segurança no ambiente corporativo. Embora a maioria dos respondentes afirme saber o que é SI, menos de metade possui familiaridade com conceitos críticos, como a engenharia social, e uma proporção ainda menor adota práticas de segurança com regularidade. Esses achados evidenciam uma lacuna entre conhecimento e comportamento, o que contribui para a persistência do fator humano como uma das principais vulnerabilidades na segurança informacional das empresas.

5. Considerações Finais

A pesquisa realizada sobre a SI nas empresas revelou um cenário preocupante. Apesar do conhecimento geral sobre o tema, as práticas e os investimentos nesta área ainda são insuficientes. A falta de políticas de segurança formalizadas, a escassez de treinamento e a baixa prioridade dada à SI expõem as organizações a riscos significativos.

O fator humano se destaca como um dos principais desafios para a SI. Embora seja reconhecida a importância do tema, nem sempre são adotadas as práticas recomendadas. A falta de conscientização e o acesso a informações proporcionam a deficiência de proteção adicional para a ocorrência de incidentes. Além disso, muitas empresas não possuem um plano de recuperação para incidentes de segurança, tornando-as ainda mais vulneráveis. A ausência de um plano de resposta a incidentes pode resultar em perdas financeiras e danos à confiança dos clientes.

Um aspecto crítico que se deve considerar é o risco associado à falta de entendimento das empresas sobre a importância da proteção de dados, especialmente em relação à LGPD. Caso ocorra um vazamento, elas podem sofrer prejuízos graves, além de consequências legais e de imagem. Para reverter este cenário, é fundamental que as empresas invistam na SI.

A implementação de políticas de segurança claras e abrangentes, a realização de treinamentos regulares para os colaboradores, a aquisição de ferramentas e soluções de

segurança e o desenvolvimento de planos de recuperação para incidentes são medidas essenciais para proteger os ativos digitais das organizações.

Em suma, a SI é um desafio complexo que exige uma abordagem multifacetada. As empresas que investem na SI serão as mais preparadas para enfrentar os desafios do mundo digital, proteger seus negócios e garantir a conformidade com a LGPD, evitando assim riscos legais e financeiros.

Como sugestão para trabalhos futuros, propõe-se uma pesquisa voltada para a avaliação do impacto da inteligência artificial (IA) na Segurança da Informação. A IA, com sua capacidade de automatizar processos e identificar padrões em grandes volumes de dados, oferece novas oportunidades para fortalecer sistemas de defesa cibernética, melhorando a detecção de ameaças e a resposta a incidentes. No entanto, seu uso também traz riscos significativos, como a possibilidade de algoritmos maliciosos sendo empregados em ataques cibernéticos, além do desafio de garantir a segurança e a ética na aplicação dessas tecnologias. Esse estudo poderia explorar tanto os benefícios quanto as vulnerabilidades associadas à adoção da IA em ambientes de segurança digital.

Referências

ANDERSON, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 2. ed. Wiley, 2008.

CANO, J. J. The Human Factor in Information Security. ISACA Journal, v. 5, p. 1-7, 2019. Disponível em: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2019/volume-5/the-human-factor-in-information-security_joa_eng_1019.pdf. Acesso em: 10 abr. 2024.

FREIRE, Rodolfo Francisco Paz; SILVA, Humberto Caetano Cardoso da; QUEIROZ, Ricardo Gomes de; BATISTA, Amélia Acácia de Miranda. O fator humano como uma vulnerabilidade em segurança da informação. Revista Brasileira de Administração Científica, v. 8, n. 3, p. 146-157, 2017. Disponível em: https://www.sustenere.inf.br/index.php/rbadm/article/view/SPC2179-684X.2017.003.0012/1259.

GONÇALVES, E. Segurança da Informação: Princípios e Práticas. Rio de Janeiro: Editora Ciência Moderna, 2014.

GONÇALVES, Wilson José. Termos Técnicos Fundamentais – Teoria e Prática. Campo Grande-MS: UFMS, 2014. Disponível em:

https://d1wqtxts1xzle7.cloudfront.net/34613700/Termos_Tecnicos_Fundamentais_-_2014-A-libre.pdf?1409727357=&response-content-disposition=inline%3B+filename%3DTermos_Tecnicos_Fundamentais_2014_A.pdf&Expires=1713646494&Signature=OLY5jcGF7MB3jkWURsw2ZMJWGTrzymir0nLdxhL3LNtD1z~87MCyFcJrXJVB9TTVfdnZ0kE7LQYA0W~xMu-VkcBgOdQzMk4SiQt1Xe7ufdntQMA129UM7fuj66LWa8Uc1nP0IdL0jMtJc7LpzUImA6XhjFOip7SLPyM2KiiYiLzNpn8mrQXDRKIYyit9miWeYm0bMCMDWUf14MheBf86v6y~tMinLFJd2WY286B~DdhDH8344UZmtAkGImjf7cIHoFMvrYfap7aLWjTdlqoIcJhupG-Wcy0HXzNaFnfLSjZdn5wx-lBzTDTx2QtEIiUQv9p2clIucnY-dzw7OLBIWQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=76. Acesso em: 15 abr. 2024.

HADNAGY, Christopher. Social engineering: The art of human hacking. John Wiley & Sons, 2018. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=9LpawpklYogC&oi=fnd&pg=PT7&dq=2.%09HADNAGY,+C.+(2018).+Social+Engineering:+The+Science+of+Human+Hacking.&ots=vdhsJWc6NR&sig=VTqgTE4XEQo6-IAtVgNf1IdSMIU#v=onepage&q&f=false. Acesso em 15 jun. 2024.

ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. Disponível em: https://cdn.standards.iteh.ai/samples/82875/726bcf58250e43d9a666b4d929c8fbdb/ISO-IEC-27001-2022.pdf. Acesso em: 30 jul. 2024.

MITNICK, K. D.; SIMON, W. L. A arte de enganar. São Paulo: Pearson Makron Books, 2003.

PEIXOTO, M. C. P. Engenharia social e segurança da informação na gestão corporativa. Rio de Janeiro: Brasport, 2006.

PIOVESAN, Leonardo Gubert; SILVA, Edilmárcio Reis Costa; SOUSA, Jackson Ferreira de; TURIBUS, Sérgio Noleto ENGENHARIA SOCIAL: Uma abordagem sobre Phishing. REVISTA CIENTÍFICA UNIBALSAS, v. 10, n. 1, p. 45-59, 2019. Disponível em: https://revista.unibalsas.edu.br/index.php/unibalsas/article/view/94/87. Acesso em 15 jun. 2024.

TRIPLETT, W. J. Addressing Human Factors in Cybersecurity Leadership. Journal of Cybersecurity and Privacy, v. 2, n. 3, p. 573-586, 2022. Disponível em: https://www.mdpi.com/2624-800X/2/3/29. Acesso em: 30 jul. 2024.

VIDAL, M. T. V. L. Segurança em redes. Niterói: UFF, 2006.

WANG, Yingxu. On Cognitive Properties of Human Factors and Error Models in Engineering and Socialization. International Journal of Cognitive Informatics and Natural Intelligence, v. 2, n. 4, p. 70–84, 2008. DOI: 10.4018/jcini.2008100106. Disponível em: https://www.igi-global.com/article/cognitive-properties-human-factors-error/www.igiglobal.com/article/cognitive-properties-human-factors-error/1576. Acesso em: 30 jul. 2024.

Agradecimentos

Agradeço, primeiramente, a Deus e a Nossa Senhora, por me guiarem e me darem forças durante toda a caminhada acadêmica. A fé e a esperança foram companheiras indispensáveis ao longo dessa jornada, sustentando-me nos momentos de desafios e inspirando-me a continuar em busca dos meus objetivos.

A Gabriela e minha mãe, por todo o apoio, compreensão e incentivos constantes. A presença de vocês foi essencial para que eu mantivesse o foco e a motivação, mesmo nas fases mais difíceis. A vocês, minha eterna gratidão por sempre acreditarem e estarem ao meu lado. Obrigada pelo amor e paciência ao longo deste processo.

Ao meu orientador, por compartilhar seus conhecimentos, orientações e conselhos valiosos, os quais foram fundamentais para a realização deste trabalho. Sou grata por sua paciência, empenho, amizade e pela valiosa oportunidade de crescer e aprender com suas lições.

E ao coordenador do curso, pelo apoio e dedicação em promover um ambiente acadêmico de excelência, que nos permitiu aprofundar conhecimentos e desenvolver nossas habilidades. Agradeço pela orientação e pela constante busca por oferecer as melhores condições para nossa formação.

A todos, o meu sincero agradecimento e reconhecimento pela contribuição indispensável na realização deste trabalho.