Universidade Federal de Pernambuco
Centro de Informática

Bacharelado em Sistemas de Informação

Avaliação da Cultura de Segurança da Informação: A Aplicação de um Survey sobre Cultura de Segurança da Informação nas Organizações

---

Trabalho de Graduação

Pedro Vinícius de Lima Santos

Recife
2020

Universidade Federal de Pernambuco

Centro de Informática

Pedro Vinícius de Lima Santos

Avaliação da Cultura de Segurança da Informação: A Aplicação de um Survey sobre Cultura de Segurança da Informação nas Organizações

Trabalho de Conclusão de Curso apresentado no curso de Bacharelado em Sistemas de Informação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientadora: *Jéssyka Flavyanne Ferreira Vilela*

Co Orientadora: *Mariana Maia Peixoto*

Recife
2020

Este trabalho é dedicado especialmente a minha mãe e minha avó que hoje não estão mais aqui, junto com meus familiares, amigos e professores sem vocês nada disso seria possível.

AGRADECIMENTOS

Agradeço especialmente a minha mãe Solange e a minha avó Marli que são pessoas que me fazem ter força todos os dias para continuar e fazer eu dar o melhor de mim e mesmo não estando aqui comigo hoje, espero que onde estiverem, estejam felizes. Mãe, sei que nunca lhe conheci, mas essa eu dedico a você. Essa conquista além de minha, é de todos aqueles que acreditaram em mim, e que quando passei por momentos difíceis, estavam lá para me apoiar.

Agradeço ao meu pai Pedro por ter me proporcionado educação desde cedo, e sei que a sua contribuição foi de extrema importância, sei um pouco das dificuldades que o senhor passou pra me dar tudo que precisei e, se não fosse o senhor, eu não estaria aqui hoje, muito obrigado pai.

Ao meu avô Luiz e minha tia Silvaneide, obrigado por terem cuidado de mim todos esses anos e por terem se importado tanto comigo sou o que sou hoje também por conta de vocês, agradeço de coração. A minha família de coração, obrigado por terem me acolhido depois daquele momento tão difícil na minha vida, saibam que vocês foram de extrema importância para não me fazer desistir, sempre que podiam estavam do meu lado, amo vocês.

Aos meus melhores amigos: Eric, esses quase cinco anos me fizeram refletir o quão vale a pena não desistir das pessoas, o quão é importante confiar em si próprio e, o mais importante de tudo, a nunca desistir, muito obrigado por estar sempre presente em toda a minha graduação e em toda a execução deste trabalho, esse trabalho finalmente saiu. Gustavo, mesmo com nossas desavenças no passado, hoje você é uma pessoa que tenho total admiração, amigo, obrigado por ter sempre ficado do meu lado me apoiando todo esse tempo, finalmente posso dizer que está acabando esse ciclo.

À minha psicóloga Thaíssa por me ajudar a manter o foco para continuar esse trabalho, você foi de extrema importância para me fazer continuar, sempre me colocando pra cima e me fazendo confiar mais em mim e no que sou capaz.

À minha orientadora Jéssyka e à minha co orientadora Mariana por terem confiado em mim e aceitado fazer este trabalho comigo, que mesmo passando por altos e baixos, acredito ter chegado ao fim. Obrigado pelo apoio, interesse, vontade e disponibilidade constante para fazer este trabalho se tornar realidade, sou eternamente grato a vocês.

Okay, I'm ready for this episode to end.
—GARNET

RESUMO

Contexto: Incidentes relacionados a vazamentos de informações sensíveis e privadas representam um grande impacto na sociedade. Um dos principais fatores que ocasionam esses vazamentos é a ação humana. O ser humano pode ser, por muitas vezes, influenciado a expor informações confidenciais por meio da conquista da confiança por terceiros, em uma prática chamada Engenharia Social. Sendo assim, para reduzir o risco desses incidentes, é necessário que as organizações possuam um forte nível de cultura de segurança da informação, para haver uma maior cautela com o manuseio e tratamento de dados sensíveis. Então, para que medidas possam ser tomadas para aprimorar as práticas de segurança da informação nas organizações, é necessário, primeiramente, fazer uma análise do estado atual da cultura para que assim seja possível identificar qual área da segurança que necessita de uma atenção maior. Objetivo: Este trabalho visa identificar métodos de avaliação de cultura de segurança da informação nas organizações, elaborar e conduzir um *survey* sobre a cultura da segurança da informação nas organizações e com os resultados, conseguir caracterizar a cultura de segurança da informação das organizações estudadas. Método: Foi construído um instrumento de avaliação que contempla setores da cultura de segurança da informação propostos na literatura. Resultados: O *survey* recebeu 75 respostas pertencentes, em sua maioria, a funcionários de instituições privadas. Nos resultados, observou-se que existe uma necessidade de capacitações dos funcionários sobre segurança da informação, existe incongruência entre conhecer, compreender e aplicar os procedimentos descritos na política de segurança de informação, além de que as organizações precisam promover mais o engajamento da segurança da informação com os seus colaboradores. Conclusões: Sendo assim, este trabalho proporcionou um entendimento do status atual da cultura de segurança da informação nas organizações cujos resultados sugerem situações que as organizações precisam tomar medidas para melhorar, além da grande aceitação dos participantes por mudanças para ajudar a garantir a segurança da informação em suas organizações e a pesquisa pode ser ampliada e utilizada em estudos futuros para melhoria das práticas de segurança nas organizações.

Palavras-chave: Cultura de Segurança da Informação, Segurança da Informação, Avaliação de Cultura de Segurança da Informação, ISCA, Questionário, Organizações.

ABSTRACT

Context: Incidents related to leaks of sensitive and private information represent a major impact on society. One of the main factors that cause these leaks is human action. The human being can often be influenced to expose confidential information by gaining trust by third parties, in a practice called Social Engineering. Therefore, in order to reduce the risk of these incidents, it is necessary that organizations have a strong level of information security culture, in order to be more careful with the handling and treatment of sensitive data. So, so that measures can be taken to improve information security practices in organizations, it is necessary, first, to make an analysis of the current state of culture so that it is possible to identify which area of security needs greater attention. Objective: This work aims to identify methods for assessing the culture of information security in organizations, to develop and conduct a survey on the culture of information security in organizations and with the results, to be able to characterize the information security culture of the organizations studied. Method: An evaluation instrument was built that includes sectors of the information security culture proposed in the literature. Results: The survey received 75 responses, mostly from employees of private institutions. In the results, it was observed that there is a need for training of employees on information security, there is incongruity between knowing, understanding and applying the procedures described in the information security policy, in addition to the fact that organizations need to further promote the engagement of information security. information with its employees. Conclusions: Therefore, this work provided an understanding of the current status of the information security culture in organizations whose results suggest situations that organizations need to take steps to improve, in addition to the great acceptance of participants for changes to help ensure information security. in their organizations and the research can be expanded and used in future studies to improve security practices in organizations.

Keywords: Information Security Culture, Information Security, Information Security Culture Assessment, ISCA, Questionnaire, Organizations.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1. Introdução

Esse capítulo possui quatro seções. A primeira seção contextualiza os temas abordados neste trabalho. A segunda descreve a motivação e a justificativa da realização dessa pesquisa. A terceira seção apresenta os objetivos. Por fim, a quarta seção discute trabalhos relacionados.

1.1 Contextualização

Com uma frequência cada vez maior, tem sido comum ouvir notícias sobre incidentes relacionados a vazamentos de dados sensíveis e privados (MACHADO et al., 2019). De fato, há um volume crescente de dados vazados nos últimos anos e que apresentam um grande impacto na sociedade (MACHADO et al., 2019). Em 2018, por exemplo, o valor relacionado a prejuízo com vazamento de dados nos Estados Unidos foi em torno de 654 bilhões de dólares e houve uma exposição de 2,8 bilhões de dados de usuários (SECURITY, 2018).

Segundo Herold (2011), um dos principais fatores de problemas em relação a incidentes com informações é a ação humana. Uma pesquisa conduzida pela PricewaterhouseCoopers (2014) descobriu que 31% dos funcionários atuais de uma empresa cometem incidentes com vazamentos de informações e 27% de antigos funcionários contribuem também para esse problema. Já outra pesquisa realizada pela Intel Security (MCAFEE, 2017) afirmou que os funcionários internos são responsáveis por 43% dos vazamentos de dados corporativos e que 21% quase metade desse percentual, são de maneira acidental. Isso pode ser considerado preocupante, pois boa parte dos vazamentos de dados ocorridos nas organizações são causados pelos próprios funcionários e pessoas que são ou já foram envolvidas com a empresa.

As pessoas podem ser influenciadas a expor informações confidenciais por meio da conquista da confiança, essa prática é conceituada como Engenharia Social (HENRIQUES, 2017). Essa técnica ocorre quando pessoas maliciosas utilizam de meios estratégicos para conseguir informações vitais de uma organização por meio de qualquer pessoa ligada à empresa, as informações podem ser conquistadas por meio de chaves de acesso ou até outras informações pessoais dos funcionários, assim como é explicado por Henriques (2017).

A motivação da execução da Engenharia Social para a coleta de informações pode vir de vários incentivos, sendo um dos mais comuns o ganho financeiro dependendo da vantagem conquistada pelo praticante (ALLEN, 2007). Com a ideia de que existem pessoas com intenções maliciosas para conseguir informações das empresas, nota-se a importância de avaliar uma forma de como mitigar os riscos de incidentes com informações.

Para minimizar os impactos sobre os vazamentos de dados, existe a segurança da informação que auxilia na proteção dos dados (HINTZBERGEN,

2018). A segurança da informação contribui para minimizar os incidentes com dados e que os princípios de confidencialidade, integridade e disponibilidade dos dados sejam seguidos (FONTES, 2017).

1.2 Motivação e Justificativa

Os princípios para que a segurança da informação seja alcançada em uma organização envolve o uso de políticas de segurança da informação como também por meio das atitudes, premissas, crenças, valores e conhecimentos que os funcionários e partes interessadas utilizam para interagir com os sistemas da organização (DA VEIGA e ELOFF, 2010) (SCHEIN, 1992). A chamada cultura de segurança da informação de uma instituição é algo de grande importância para reduzir os incidentes com vazamentos de dados (DA VEIGA e MARTINS, 2015). Johnson e Goetz (2007) reforçam o ponto de que o fator comportamental dos colaboradores e o foco da organização como um todo que é necessário para criação de uma cultura da segurança da informação são importantes dentro de uma organização.

A cultura de segurança da informação também pode ser vista como quais comportamentos de segurança da informação dentro da organização são aprovados e instigados para serem incorporados nas ações da organização (MARTINS e ELOFF, 2002).

Uma forte cultura de segurança da informação é necessária nas organizações em que a confidencialidade, o manuseio de dados sensíveis e a privacidade das informações são entendidas e tratadas (DA VEIGA e MARTINS, 2015). Além disso, uma cultura voltada para a segurança da informação auxilia a alta gerência da empresa ter ciência da existência de riscos e com isso ajudar a capacitar os funcionários para que consigam agir da maneira mais segura e consciente possível contra ameaças (ALHOGAIL e MIRZA, 2014).

Para que medidas possam ser tomadas para aprimorar as práticas de segurança da informação nas organizações, é necessário, primeiramente, fazer uma análise do estado atual da cultura (DA VEIGA e MARTINS, 2015). Para essa análise, existem alguns questionários que são aplicados nas organizações. Por exemplo, a avaliação proposta por Al-Mayahi e Sa'ad (2013) tem o objetivo analisar uma amostra de uma organização para que com o resultado deles seja consolidada uma análise sobre o estado atual da cultura de segurança da informação com o objetivo de trazer um diagnóstico e, assim, a empresa conseguir tomar medidas de melhoria.

Já outro trabalho sobre avaliação da cultura de segurança de informação que pode ser citado é o de Parsons et al. (2017). Os autores abordam o fator comportamental como o foco principal do questionário e, assim, na análise é possível conseguir um parecer da situação atual da cultura da organização.

Em resumo, para conseguir executar o diagnóstico da cultura de segurança da informação, é necessário fazer avaliações que consigam apresentar indícios nos

resultados que representem qual a situação atual com o qual a empresa se encontra (AL-MAYAHI e SA'AD, 2013).

Assim como na cultura organizacional, toda organização possui uma cultura de segurança da informação que nasce da maneira como as pessoas se comportam com as informações. Os procedimentos que os funcionários da organização realizam nos seus trabalhos diariamente podem representar o elo mais fraco quando se fala em segurança da informação, pelo fato de que é uma das formas mais arriscadas de haver algum vazamento dessa informações (DA VEIGA e ELOFF, 2002).

Uma cultura de segurança da informação robusta e bem disseminada contribui para minimizar os riscos do comportamento dos funcionários quando estão agindo e processando informações (DA VEIGA e ELOFF, 2010). Desse modo, é importante desenvolver e melhorar a cultura da segurança da informação por meio da análise e policiamento dos comportamentos dos funcionários (DA VEIGA e ELOFF, 2002).

1.3 Objetivos

O objetivo geral do trabalho é conduzir um *survey* sobre a cultura da segurança da informação nas organizações. Para atingir esse objetivo, foi elaborado um instrumento de avaliação que contempla as dimensões relacionadas à cultura de segurança da informação propostas por Martins, Da Veiga e Eloff (2007). Como objetivos específicos pretende-se:

(i) Investigar métodos de avaliação de cultura de segurança da informação nas organizações;

(ii) Elaborar um instrumento para avaliar a cultura de segurança da informação;

(iii) Aplicar o instrumento para coletar resultados para fazer uma avaliação;

(iv) Caracterizar a cultura de segurança da informação a partir dos resultados obtidos no survey.

Sendo assim, pretende-se compreender o comportamento e a opinião dos funcionários para assim obter um panorama da cultura atual das empresas. Além disso, essa pesquisa pode servir de insumo para outras pesquisas e projetos futuros que possam ser realizados com o objetivo de aprimorar as práticas da cultura de segurança da informação nas organizações.

1.4 Trabalhos relacionados

O estudo sobre a cultura de segurança da informação possui esse papel fundamental por mostrar sua devida importância na segurança de ativos da informação das organizações. Nas próximas seções são discutidos trabalhos relacionados à cultura de segurança da informação e sua relevância.

1.4.1 Avaliação de cultura nas organizações

A influência da cultura organizacional na gestão de processos de negócios, com o objetivo de entender a sua atuação, é descrito no trabalho de Arteiro (2015). O autor realizou um estudo de caso em uma instituição pública que tem o foco primário em dar suporte ao controle de gestão pública, além de funcionar como uma ferramenta de defesa do interesse social e no combate a casos de corrupção. O foco do trabalho foi entender como a cultura organizacional da empresa influencia na gestão de processo de negócios. Para isso, foi definida uma metodologia do termo em português Gerenciamento de Processos de Negócio (do inglês, *Business Process Model* (BPM)) para se alinhar aos objetivos da empresa, que com isso passaria por um processo de melhoria de quatro fases. Essas fases são: modelagem (AS-IS), análise, desenho (TO BE) e implementação de acordo com a metodologia definida no escritório de processos.

De acordo com Arteiro (2015), a pesquisa utilizou para coleta de dados entrevistas de forma semi estruturada com objetivo exploratório, observações e análise de documentos da organização. Para a coleta de dados das entrevistas, foi elaborado um roteiro que seguia algumas categorias iniciais definidas pela pesquisadora em relação a empresa que foram a Estrutura Organizacional, Política, Reação às Mudanças, Alinhamento Estratégico, Comunicação, Motivação, Comprometimento, Relacionamento, Habilidades e Competências, Política de Valorização, Melhoria Contínua, Inovação, Orientação ao Cliente e Visão Geral da Iniciativa de BPM dentro da organização.

Primeiro aconteceu o período de observação como parte do escritório de processo da empresa, e com base nessa etapa foi desenvolvido o roteiro da pesquisa. Posteriormente, foram criadas perguntas que cobriam cada uma das categorias. A coleta de dados teve a duração de um ano, de maio de 2014 a maio de 2015. Ao total foram entrevistados nove funcionários de diferentes áreas para ocorrer a diversificação e seguindo o roteiro criado anteriormente.

Após o período de análise das entrevistas e da coleta de dados, o resultado do estudo foi a fonte para construção de um modelo de diagnóstico que relaciona os valores culturais anteriormente definidos da organização aos valores CERT (Orientação ao Cliente, Excelência, Responsabilidade e Trabalho em equipe) (Schmiedel, 2013) de uma cultura BPM. Com o alinhamento dos dados obtidos, foram propostas algumas estratégias para reduzir e, em alguns casos, aprimorar a atuação dos valores e aspectos culturais que acarretam a implantação da iniciativa de Gestão de Processos de Negócio na organização.

O trabalho de Vegro et. al. (2016) avaliou os valores e as práticas que fazem parte e definem a cultura organizacional de um hospital privado do interior de São Paulo, sendo transparecido pela visão dos funcionários que fazem parte da enfermagem. O estudo consistiu em uma pesquisa quantitativa utilizando um instrumento de avaliação de cultura organizacional brasileiro o Instrumento

Brasileiro de Avaliação da Cultura Organizacional (IBACO) (Ferreira et. al., 2002). Na pesquisa, participaram 21 enfermeiros e 62 técnicos e auxiliares de enfermagem, no período de janeiro a março de 2013.

O estudo aplicou um questionário que foi dividido em algumas fases. A primeira fez o reconhecimento de cada voluntariado, pegando suas informações gerais como sexo, escolaridade e função desenvolvida. Na segunda fase foi introduzido de fato a ferramenta principal da pesquisa, o IBACO, que foi uma ferramenta criada e validada por pesquisadores brasileiros da área de cultura organizacional e com o objetivo de fazer uma avaliação da cultura organizacional pela visão dos trabalhadores. As práticas, valores e crenças dos trabalhadores são levados completamente em consideração nessa avaliação. Essa ferramenta contempla 94 itens e um pouco mais da metade deles, 55 itens fizeram a identificação dos valores da organização, incluindo também especificamente: Valores de Profissionalismo Cooperativo (VPC), Valores de Rigidez Hierárquica (VRH), Valores de Profissionalismo Individual (VPI) e Valores de Bem-estar e Satisfação (VBE) e as últimas 39 afirmações são específicas sobre as práticas organizacionais que englobam: Práticas de Integração Externa (PIE), Práticas de Recompensa e Treinamento (PRT) e Práticas de Promoção do Relacionamento (PPR). Essas afirmativas foram espalhadas de forma aleatória na pesquisa.

O questionário foi distribuído para todas as afirmativas em escala Likert com a pontuação de 1 até 5. Após o fim da coleta de dados, as respostas foram agrupadas para que fosse possível conseguir uma análise estatística do estado atual da cultura organizacional naquele momento. Na parte de resultados, os valores e as práticas que mais se destacaram na visão dos enfermeiros foram a cooperação no ambiente de trabalho e a preferência pela qualidade e bem estar dos pacientes. Entretanto, algumas características de rigidez e até controle por conta da hierarquia e as relações de poder também puderam ser observadas.

Em resumo, o diagnóstico é que os trabalhadores apresentaram que a empresa tem uma cultura de cooperativismo e busca de satisfação e qualidade por parte dos pacientes. porém em casos de processo decisório, por exemplo, há um problema na comunicação pelo fato das cadeias de poder e hierarquização influenciarem nas opiniões desses trabalhadores, o que pode acarretar em insatisfação e desmotivação no hospital. O interessante dessa pesquisa é poder captar tantas características que na parte de resultados até parece que o pesquisador faz parte da organização.

O trabalho de Ližbetinová, Lorincová e Caha (2016) abordou a influência que a cultura organizacional tem sobre empresas do ramo de logística. O ponto central da pesquisa foi analisar a cultura organizacional nas empresas da Eslováquia, com a justificativa da cultura ser um dos fatores principais para a qualidade dos produtos e a sua competitividade no mercado. No trabalho foi utilizado como base o *Organizational Culture Assessment Instrument* (OCAI) (CAMERON e QUINN, 1999)

que é um questionário usado em várias pesquisas que possuem o objetivo de examinar a cultura organizacional e assim trazer um diagnóstico da organização.

A pesquisa teve 14 organizações participantes, 8 delas eram de pequeno porte (de 10 a 49 funcionários), 1 foi de médio porte e 5 foram de grande porte (mais de 250 funcionários) com o total de 345 voluntários que responderam a pesquisa. Os resultados da pesquisa fizeram com que fosse concluído que essas empresas da Eslováquia são focadas no suporte interno, estabilidade e controle.

1.4.2 Avaliação de práticas de segurança da informação

O trabalho de Parsons (2017) abordou a aplicação de um questionário para avaliação de comportamento humano. A conscientização sobre segurança da Informação é um dos fatores que podem ser colocados como ferramenta para evitar ameaças nas organizações. A ideia da pesquisa foi aplicar o termo português (do inglês, *Human Aspects of Information Security Questionnaire* (HAIS-Q)) que são 63 itens que avaliam sete áreas de foco: gerenciamento de senhas, uso de e-mail, uso da Internet, uso de mídias sociais, dispositivos móveis, tratamento de informações e relatórios de incidentes. O intuito é realizar uma medição do nível de conscientização nas organizações com o objetivo de evitar futuras ameaças.

A pesquisa conduziu dois estudos para validar o instrumento, sendo o primeiro um estudo empírico relacionado a *phishing* que é definida como uma ação de fraude realizada por uma entidade para obter informações confidenciais de usuários, se passando por uma outra entidade confiável (Ramzan e Zulfikar, 2010) que para entender como as pessoas reagiriam a ele. O *phishing* basicamente pedia informações sensíveis dos usuários via email. Um total de 112 universitários participaram do estudo que foi dividido em duas partes. A primeira era passar pela experiência com o *phishing* e, na segunda, os participantes foram requisitados a responder o questionário HAIS-Q. O resultado foi que os estudantes que obtiveram uma maior pontuação, também tiveram um melhor desempenho com o *phishing,* o que significou que o instrumento conseguia identificar, pelo comportamento, possíveis ameaças que poderiam ocorrer.

Além do *phishing* existem outras formas de ataque a informações confidenciais. A informação é a base de todo negócio e o tratamento adequado das informações é necessário para que haja uma garantia de que não serão violadas de distintas formas, como ataques de hackers por exemplo (SANTOS, 2014). O trabalho de Santos (2014) possui dois objetivos principais, o primeiro é a ideia de apresentar e comparar normativos mais utilizados para criação e implementação de um sistema de gestão de segurança da informação aplicado a um centro hospitalar. Já o segundo, é fazer um estudo de caso com um hospital público português utilizando um framework selecionado anteriormente na fase de comparação, para que com isso fosse possível entender como é feita a gestão de segurança da informação do hospital.

Durante a pesquisa, foi observado com a revisão bibliográfica que os normativos mais citados eram a norma internacional ISO27001, a *Information Technology Infrastructure Library* (ITIL) e o framework *Control Objectives for Information and Related Technology* (COBIT) com o COBIT5SI focado diretamente na segurança da informação (SANTOS. 2014). Com os frameworks e as normas entendidas, o estudo analisou cada uma delas para que fosse identificado diferentes visões dos componentes da gestão de segurança da informação para dar garantia que as empresas que forem colocá-las em prática tenham um sistema adequado.

O objetivo principal seguinte validou os resultados em uma organização. Para isso foi elaborada uma entrevista com um dos representantes do centro hospitalar que se ofereceu como voluntário para a pesquisa. Com essa entrevista, cobriu-se quatro facilitadores da segurança da informação, políticas e princípios, processos, estruturas organizacionais e informação. Na Tabela 1 é possível observar os tipos de informações e a resposta do entrevistado sobre a preocupação do que deve ser documentado da organização.

O trabalho demonstrou que uma possível melhoria, seria a organização investir na documentação, em princípios e novas políticas de segurança da informação para que alguns processos e preocupações existentes fossem reduzidas.

Analisar quais comportamentos despertam diferentes atitudes em jovens adultos em relação às práticas de segurança da informação é o objetivo do trabalho de Yoon, Hwang e Kim (2019). A proposta é utilizar o modelo de pesquisa da Protection Motivation Theory (PMT), que é uma teoria bem fundamentada e é baseada no conceito de trazer o medo com o comprometimento de um determinado evento. Os hábitos e comportamentos são levados completamente em consideração.

Tabela 1 - Checklist de tipos de informação de segurança da informação baseada nas recomendações do COBIT5SI.

TIPOS DE INFORMAÇÃO	C. Hospitalar
Estratégia de Segurança da Informação	±
Orçamento da Segurança da Informação	±
Plano de Segurança da Informação	±
Políticas	±
Requisitos de Segurança da Informação	±
Material de Conscienciali zação	±
Relatórios de Revisão de Segurança da Informação	√
Perfil de Risco da Informação	X
Painel de Segurança da Informação	±

√ presente | ± preocupação existente | X não existe

Fonte: Santos (2014).

Nesse estudo, a avaliação ocorreu por meio de um questionário que teve a participação de 209 estudantes voluntários de uma universidade da Coréia do Sul para testar o modelo projetado na pesquisa em que 202 responderam completamente. A universidade não possui uma política de segurança da informação explícita, nem outro procedimento.

Os resultados acabaram revelando que os estudantes se sentem mais motivados para se preocupar e agir com práticas de segurança da informação quando percebem um nível maior de severidade da informação. Foi observado também que as intenções dos estudantes não eram alteradas pela influência social, por exemplo. O estudo promove que novas descobertas da pesquisa ajudam a prever atitudes dos alunos com relação a práticas de segurança da informação e que a motivação surge pela influência da conscientização sobre segurança.

1.4.3 Avaliação de cultura de segurança da informação

Dentre trabalhos relacionados, um que abrange várias vertentes da área de segurança da informação para realizar o diagnóstico é a, no termo em português, Avaliação de Cultura de Segurança da Informação (do inglês, *Information Security Culture Assessment* (ISCA)) (DA VEIGA e MARTINS, 2015). O trabalho apresenta um questionário que utiliza os principais fatores (nomeado pelos autores como dimensões) de uma organização. Além disso, esse trabalho é base de vários outros relacionados ao assunto.

Com o resultado desse questionário do ISCA é possível obter um parecer geral da organização e de como está o seu nível de cultura de segurança da informação. Isso pode contribuir para minimizar os riscos do ponto de vista do comportamento dos funcionários como a divulgação indevida de informação sensível (DA VEIGA e MARTINS, 2015).

No trabalho de Martins e Eloff (2002c), é citado como o fator humano atuando juntamente com a tecnologia das organizações impacta diretamente na segurança da informação e como, muitas vezes, esse é o elo mais fraco da organização para incidentes com informações. O trabalho argumenta que para conseguir haver um controle sobre como as informações da organização são utilizadas, é necessário entender a cultura de segurança da informação da empresa e, assim, investir em mudanças positivas nela. O objetivo principal do trabalho é criar esse instrumento de avaliação.

Toda organização possui um determinado nível de segurança da informação e dependendo do nível, a organização pode estar aberta a ameaças. O intuito de se fazer uma avaliação da cultura é entender como está o nível atual da organização e com os resultados, adequá-lo a um nível ideal. Para fazer essa avaliação, a ferramenta utilizada é um questionário que faz esse nivelamento. Esse questionário consiste em coletar as percepções, atitudes, opiniões e ações dos funcionários da organização e com o resultado, a alta gerência da organização consiga entender

como está o seu nível de maturidade em relação a segurança da informação, e logo após isso, consiga tomar decisões do que fazer para melhorá-la.

A pesquisa foi dividida em 4 fases:

- **Desenvolvimento do questionário:** É a fase que o questionário é desenvolvido. Modelos de cultura de segurança da informação são levados em consideração e algumas particularidades da organização estudada são consideradas;
- **Processo de pesquisa:** O questionário desenvolvido na fase anterior é aplicado e um parecer atual ainda não analisado da cultura de segurança da informação é o resultado dessa etapa;
- **Análise de dados:** As informações geradas na etapa anterior são analisadas. O resultado dessa fase gera um indicador quantitativo de como está a situação atual da organização;
- **Interpretação dos dados:** Essa última fase utiliza dos dados analisados da fase anterior para fazer interpretações e recomendações sobre a cultura de segurança da informação.

Em outro trabalho de Da Veiga (2016) é feito uma análise de como os colaboradores de uma organização que leem e os que não leem a política de segurança da informação impactam na cultura de segurança da informação. Outro objetivo da pesquisa, é entender se com o passar do tempo, os funcionários que não sabiam sobre a política passarem a lê-la, se teria um impacto positivo na cultura de segurança da informação e se ela tornaria-se mais forte.

A pesquisa teve a duração de oito anos em quatro intervalos, o instrumento utilizado para fazer a avaliação da cultura de segurança da informação foi o ISCA com o resultado podendo-se fazer uma análise quantitativa. A empŕesa que foi feita de amostra do estudo foi uma empresa internacional que atua sobre 12 países. O ISCA nesse momento foi utilizado com 9 dimensões e possuía uma média de pontos que ia de 0 a 5 e as perguntas que cobriam cada uma delas foram separadas em escala Likert e perguntas de sim ou não .

Tabela 2 - Média geral da cultura de segurança da informação.

Anos de aplicação do ISCA	Respostas obtidas	Média geral de cultura de segurança da Informação	Média geral de cultura de segurança da Informação (%)
ISCA 4 - 2013	2159	4.10	83.6%
ISCA 3 - 2010	1320	3.76	75.7%
ISCA 2 - 2007	1571	4.00	81.7%

ISCA 1 - 2006	1941	3.89	75.7%

Fonte: Adaptado de Da Veiga (2016).

Como resultado final, foi observado que houve uma melhora considerável no nível de cultura de segurança da informação da organização comparado ao primeiro ano da pesquisa, como pode ser observado na Tabela 2. Os resultados forneceram base para organização saber que a sua cultura de segurança da informação estava sendo otimizada e seus colaboradores estavam se integrando com a política de segurança da informação da organização.

Não defender que o único foco da implantação de uma forte cultura de segurança da informação é no comportamento do funcionário, e sim algo mais voltado a uma maneira holística e que é necessário envolver todos da organização em conjunto são os pontos centrais do o estudo de Lim et. al. (2010). O desafio mostrado na pesquisa corresponde a dificuldade de melhorar as práticas de segurança da informação da organização ao invés de apenas mudar o comportamento dos funcionários. A pesquisa é realizada em duas empresas por meio de entrevistas, observações e análises de documentos das organizações. É utilizado um framework que faz a captação de três tipos de relacionamentos entre a cultura de segurança da informação e a cultura organizacional. Os relacionamentos são:

- A cultura de segurança da informação não faz parte da cultura organizacional;
- A cultura de segurança da informação é uma subcultura da cultura organizacional;
- A cultura de segurança da informação está completamente inserida dentro da cultura organizacional.

O framework propõe que o terceiro relacionamento depende da alta gerência envolvida na gestão das práticas de segurança da informação, aplicação das políticas, conscientização de segurança, treinamento de segurança, entre outros. Na aplicação da pesquisa, as duas empresas escolhidas foram de segmentos diferentes com características de média até alto perfil de risco. Os participantes escolhidos eram da alta gestão e os funcionários que estavam envolvidos com o processamento de informações. Os resultados da pesquisa demonstram que a cultura de segurança da informação não opera isoladamente. A atuação da alta administração e a alocação de orçamento para segurança da informação, por exemplo, podem fazer com que cada pessoa que está envolvida com a empresa, entender a importância de manter os dados da organização em segurança.

Na Tabela 3 é apresentada uma comparação entre os principais trabalhos relacionados e o trabalho proposto.

Tabela 3 - Comparação entre os trabalhos relacionados e o proposto.

Critérios	Arteiro (2015)	Parsons (2017)	Martins e Eloff (2002c)	Trabalho Proposto
Instrumentos utilizados para avaliação	Entrevistas, observações e análise de documentos	Questionário	Questionário	Questionário
Tipo de instituição	Pública	Pública	Privada	Pública e Privada
Tipo de público	Funcionários públicos	Estudantes	Funcionários da organização estudada	Funcionários de diferentes segmentos
Tipo de contribuição	Metodologia de BPM a ser integrada na organização.	Avaliação do nível de conscientização sobre segurança da informação.	Avaliação de cultura de segurança da informação em uma organização.	Avaliação de cultura de segurança da informação por meio de um survey.
Tema focal contemplado	Cultura organizacional	Segurança da Informação	Cultura de segurança da informação.	Cultura de segurança da informação.
Quantidade de participantes no estudo total	9	112	6991	75

Comparando os principais trabalhos de cada subseção mostrada, na Tabela 3 é possível observar alguns critérios que apresentam as principais semelhanças e diferenças entre esses trabalhos e a pesquisa em questão. Com essas comparações é possível observar que alguns trabalho já tiveram ideias um pouco semelhantes, no uso de ferramentas e com isso é possível identificar relevância neste trabalho proposto.

1.5 Estrutura do documento

Este documento está dividido em cinco capítulos, são eles:

- Capítulo 2 - Revisão da Literatura: apresenta os fundamentos teóricos relacionados aos temas tratados no trabalho como Segurança da Informação,

Cultura Organizacional, Cultura de Segurança da Informação, Privacidade e Engenharia Social;

- Capítulo 3 - Metodologia utilizada para a condução desta Pesquisa;
- Capítulo 4 - Apresentação dos Resultados e Discussão;
- Capítulo 5 - Conclusões e Trabalhos Futuros.

2. Revisão da Literatura

Neste capítulo, serão descritos os conceitos e definições principais dos elementos teóricos deste trabalho. A Seção 2.1 descreve segurança da informação. Na Seção 2.2 é apresentado o conceito de cultura organizacional. A cultura de segurança da informação é definida na Seção 2.3. A Seção 2.4 demonstra o conceito de privacidade. E por fim, a Seção 2.5 descreve sobre a engenharia social.

2.1 Segurança da Informação

O conjunto de orientações, normas, procedimentos, políticas entre outras ações que tem a missão e objetivo de proteger informações é considerada Segurança da Informação (FONTES, 2017). Segundo Hintzbergen (2018), a Segurança da Informação pode ser vista como o caminho a se chegar ao equilíbrio entre diferentes aspectos que a compõem. A área de Segurança da Informação tem o intuito de alcançar a preservação da tríade CID (Confidencialidade, Integridade e Disponibilidade) das informações (HINTZBERGEN, 2018). Abaixo são apresentadas as definições desses termos:

- **Confidencialidade:** É descrita como uma propriedade da segurança da informação em que a informação não é disponibilizada para qualquer outra entidade que não tenha autorização. O objetivo é a prevenção da disponibilização de conteúdos de uma mensagem restrita (HINTZBERGEN, 2018);

- **Integridade:** É definida como a propriedade que protege com total exatidão o conteúdo em que ela é aplicada. Seu conceito apresenta a garantia de que sejam prevenidas modificações não autorizadas de hardware e software, e até de dados garantindo que ele continue consistente (HINTZBERGEN, 2018);

- **Disponibilidade:** Sua definição é apresentada como uma propriedade que garante que uma entidade consiga ter acesso e possa usar de um sistema que tenha autorização. Nela também, é assegurado que a entidade tenha um acesso confiável e em um tempo adequado. Em resumo, é a garantia de que os sistemas estarão funcionando sempre que necessário (HINTZBERGEN, 2018).

Além de ter como objetivo atingir a tríade CID, a área da segurança da informação busca satisfazer outras propriedades, também chamados de aspectos complementares, como a autenticidade, auditoria, não repúdio, legalidade e privacidade (HINTZBERGEN, 2018).

- **Autenticidade:** Basicamente é a propriedade que uma entidade tem de provar que é realmente quem diz ser (HINTZBERGEN, 2018). Autenticidade é a habilidade de determinar que afirmações, políticas e permissões expressadas por uma pessoa são realmente genuínas (GOODRICH; TAMASSIA, 2011);

- **Auditoria:** É a verificação realizada nas empresas para validar se a segurança da organização é condizente com a sua política de segurança da informação (BAUER, 2006);

- **Não repúdio:** É a capacidade de provar a ocorrência de algum evento e as entidades responsáveis pela ocorrência ou incidente (HINTZBERGEN, 2018);

- **Legalidade:** É a garantia de que a informação foi produzida conforme a lei, todos os ativos estão de acordo com os requisitos de conformidade (SÊMOLA, 2014);

- **Privacidade:** É o direito que todo ser humano tem a reserva de suas informações pessoais, sem que nenhuma delas seja violada (HUMANOS, 2015). A privacidade leva em consideração a cautela com a maneira com que as informações confidenciais são coletadas e também são utilizadas (TOM, 2019).

Em síntese, a segurança da informação busca a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos de negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio (HINTZBERGEN, 2018).

2.2 Cultura Organizacional

Toda sociedade humana desenvolve uma cultura com um conjunto geral de premissas, valores, crenças e linguagem que é passado de uma geração a outra, e às vezes sofre uma modificação nessa passagem. E assim como na sociedade, a medida que as empresas interagem com as pessoas, esses funcionários vão criando da mesma maneira uma cultura interna (DEAL e KENNEDY, 1982).

A definição para cultura organizacional, segundo Robbins (2012) é "*um sistema de valores compartilhados pelos membros de uma organização que a diferencia das demais*." Já de acordo com Pires e Macêdo (2006) a definição seria que a cultura organizacional, é compreendida como a "união de valores, crenças e princípios que são compartilhados pelos colaboradores de uma organização e pode sofrer influência direta do modelo de gerenciamento da alta gestão". No que essas definições entram em concordância é que a cultura organizacional é criada e

mantida pelas pessoas que fazem parte da organização e pode sofrer influências dos gestores. Todas as ações dos funcionários de uma organização fazem parte da cultura organizacional.

A cultura não é criada apenas pelos funcionários. Os maiores influenciadores de como vai ser o direcionamento dessa cultura são os fundadores e a liderança da empresa. Como são as pessoas que mais tem poder na organização, podem impor pensamentos pessoais, e seus próprios jeitos de fazer as coisas (SCHEIN, 1992).

O conceito de cultura organizacional se tornou mais popular nas últimas quatro décadas pelo fato de que algumas dessas culturas estavam trazendo um maior sucesso de negócio (ARTEIRO, 2015). A cultura organizacional é refletida como um grupo que em um tempo determinado aprende e encontra soluções para problemas relacionados aos ambientes internos e externos a eles, sendo os internos também, sua própria integração (SCHEIN, 1990).

Schein (2010) aborda que a cultura organizacional pode ser classificada em níveis distintos, em que cada um foca em um ponto de vista sobre a cultura. Dentre eles, são os artefatos, as normas e os valores e premissas.

1. **Artefatos:** Eles podem ser definidos como resultados que são visíveis e também, os processos que são desempenhados na organização (ARTEIRO, 2015). Podem ser observados de maneira fácil, mas demonstram complexidade quando se volta a sua decifragem. Entre eles, estão as linguagens tratadas dentro da organização e as suas tecnologias (ARTEIRO, 2015).

2. **Normas e valores:** São informações e pensamentos compartilhados, o nível que aborda a parte de estratégias e filosofias da organização. É o senso de que pode ser avaliado o comportamento ou pensamento correto ou não (ARTEIRO, 2015). As normas são vistas como um livro de regras das organização relacionados a comportamentos que devem ser esperados em determinados cenários. Já os valores, são uma carga de ideais abstratos que podem ser vistos como o discernimento do que é importante, e do que é correto sob as rédeas da organização (ARTEIRO, 2015).

3. **Premissas básicas:** São vistas de forma assumida e inconsciente com veracidade sobre a organização. São observadas como conceito inicial sobre quais valores e determinadas ações na empresa, vão ser baseados (ARTEIRO, 2015).

2.3 Cultura de Segurança da Informação

Assim como na cultura organizacional, toda organização possui uma cultura de segurança da informação, ela nasce da maneira como as pessoas se comportam com as informações. Os procedimentos que os funcionários da organização

realizam nos seus trabalhos diariamente podem representar o elo mais fraco quando se fala em segurança da informação, pelo fato de que é uma das formas mais arriscadas de haver algum vazamento dessas informações (DA VEIGA e ELOFF, 2002).

Desse modo, é importante desenvolver e aprimorar a cultura da segurança da informação por meio da análise e policiamento dos comportamentos dos empregados (DA VEIGA e ELOFF, 2002). O termo cultura de segurança da informação é definido por Da Veiga e Eloff (2010) como as atitudes, premissas, crenças, valores e conhecimentos que os funcionários e partes interessadas usam para interagir com os sistemas da organização e procedimentos sempre que possível. A interação resulta em comportamentos aceitáveis ou inaceitáveis evidentes em artefatos e criações que se tornam parte da maneira como os procedimentos são realizados na organização para proteger seus ativos de informação (DA VEIGA e ELOFF, 2010).

A cultura de segurança da informação no âmbito de gerenciamento, parte da ideia de que uma empresa que quiser aplicá-la tem de propor uma sub-cultura da segurança da informação. Assim, todas as atividades realizadas na organização devem ser feitas de uma forma consistente e seguindo as boas práticas de segurança da informação. Para isso, é necessário que os envolvidos tenham conhecimento como o pré-requisito para executar as atividades dentro da organização de forma segura (VAN NIEKERK e VON SOLMS, 2010).

Nesse sentido, para que a organização consiga manter esse controle sobre seus funcionários algumas ferramentas auxiliam nesse processo de avaliação da cultura como, por exemplo, o *Information Security Culture Assessment* (ISCA) que é um instrumento de diagnóstico que faz a avaliação da cultura de segurança da informação da organização para que assim se tenha um parecer do estado atual da organização. Com os resultados obtidos, possa ser colocado em prática medidas que melhorem alguns aspectos de segurança da informação na organização (DA VEIGA; MARTINS, 2015). Reduzir os riscos de comportamentos dos funcionários com o gerenciamento de informações e assim instigar uma cultura de segurança da informação com menos violações de segurança é um dos principais objetivos do ISCA (DA VEIGA e MARTINS, 2015).

O ISCA é um questionário que avalia diferentes setores da segurança da informação denominados pelos autores como dimensões (DA VEIGA e MARTINS, 2015). As dimensões são:

1. **Gerenciamento de ativos de informações:** Avalia as percepções dos funcionários sobre a proteção dos ativos de informação da organização (DA VEIGA e MARTINS, 2015);

2. **Políticas de segurança da informação:** Avalia o entendimento dos funcionários sobre a política de segurança da informação da organização (DA VEIGA e MARTINS, 2015);

3. **Gestão de mudança:** Avalia as percepções sobre mudança e a vontade dos funcionários de mudar hábitos que ajudem a manter as informações de forma segura (DA VEIGA e MARTINS, 2015);
4. **Gerenciamento de usuários:** Avalia a conscientização dos funcionários e o treinamento recebido por eles em relação aos requisitos para proteger a informação (DA VEIGA e MARTINS, 2015);

5. **Programa de segurança da informação:** Avalia a eficácia do investimento que a organização realizou nos recursos de segurança da informação (DA VEIGA e MARTINS, 2015);

6. **Liderança em segurança da informação:** Avalia as percepções dos funcionários sobre a governança da segurança da informação para minimizar os as possíveis ameaças (DA VEIGA; MARTINS, 2015);

7. **Gerenciamento de segurança da informação:** Avalia as percepções da gerência sobre a forma com que o gerenciamento da segurança da informação é realizado (DA VEIGA e MARTINS, 2015);

8. **Confiança:** Avalia as percepções dos funcionários em relação à retenção de informações privadas e sua confiança nas comunicações da organização, sejam elas por equipamentos, ou de forma direta com outros funcionários (DA VEIGA e MARTINS, 2015);

9. **Treinamento e conscientização:** Avalia a percepção dos funcionários sobre as necessidades adicionais de treinamentos em segurança da informação (DA VEIGA e MARTINS, 2015);

10. **Percepção de privacidade:** Avalia a percepção que os funcionários têm em relação aos princípios de privacidade (DA VEIGA e MARTINS, 2015).

No estudo de Nasir et. al. (2019), foi possível identificar por meio de uma revisão da literatura bem aprofundada, quais dimensões da cultura de segurança da informação eram mais tratadas nos trabalhos que ao total foram 26 dimensões que podem ser observadas na Tabela 4. A partir disso, no final do trabalho é feita uma comparação com as dimensões que são tratadas nos trabalhos que envolvem o ISCA. O resultado da pesquisa é uma tabela de comparação de quais são as

dimensões que são tratadas nos trabalhos em que o ISCA é o objeto de estudo, o resultado pode ser observado na Tabela 4.

Tabela 4 - Dimensões da Cultura de Segurança da Informação em estudos relacionados ao ISCA.

Nº	Dimensões	Estudos							Número de Ocorrências
		1	2	3	4	5,8	6	7	
1	Liderança e Governança		X	X	X	X	X		5
2	Gestão de Segurança e Operações		X						1
3	Políticas de Segurança	X	X	X	X	X	X	X	7
4	Gestão do Programa de Segurança		X	X					2
5	Programa de Segurança da Informação				X	X	X		3
6	Gerenciamento de segurança do usuário		X	X	X	X	X		5
7	Proteção e Operações de Tecnologia		X						1
8	Gestão da Mudança	X	X	X	X	X	X		6
9	Gestão de Ativos de Informação			X	X	X	X	X	5
10	Gestão de Segurança da Informação			X	X	X	X		4
11	Confiança	X		X	X	X	X		5
12	Conscientização	X							1
13	Treinamento e Conscientização				X	X			2
14	Percepção de privacidade				X				1
15	Análise de Risco	X							1
16	Avaliação Comparativa	X							1
17	Orçamento	X							1
18	Gestão	X							1
19	Conduta Ética	X							1
20	Compromisso de Segurança da Informação							X	1
21	Importância da Segurança da Informação							X	1
22	Diretivas de Segurança da Informação							X	1
23	Responsabilidade pela Segurança da Informação							X	1
24	Percepção de Monitoramento de Segurança da Informação							X	1
25	Consequências para a segurança da informação							X	1
26	Necessidade de segurança da informação							X	1
	NÚMERO DE DIMENSÕES EM CADA ESTUDO	9	7	8	10	9	8	9	
	Estudos: 1 = Martins e Eloff (2002c); Martins e Eloff (2002b), **2 =** Martins e Eloff (2010), **3 =** Da Veiga e Martins (2015), **4 =** Martins, Da Veiga e Eloff (2007), **5 =** Da Veiga e Martins (2015b), **6 =** Martins e Da Veiga (2014), **7 =** Martins e Da Veiga (2015c), **8 =** Martins e Da Veiga (2015c)								

Fonte: Adaptado de Nasir et. al. (2019)

Como discutido anteriormente, a cultura de segurança da informação existe para tentar minimizar os deslizes causados pela ação humana que é um dos fatores que podem gerar incidentes relacionados a interação dos funcionários com informações. O ISCA é uma das ferramentas que existem para tentar minimizar esses riscos e ela é a base para a realização deste trabalho.

2.4 Privacidade

Segundo o dicionário Cambridge (2020), a privacidade pode ser definida como "*O direito de alguém de manter em segredo seus assuntos e relacionamentos pessoais*". O artigo 12 da Declaração Universal dos Direitos Humanos (HUMANOS, 2015) afirma que "Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e

reputação". Comparando a definição do dicionário com a declaração pode ser observado que a privacidade é um direito que todos os seres humanos possuem.

As organizações estão o tempo todo processando informações sobre clientes, funcionários, parceiros de negócio, entre outros. Alguns incidentes no processo de manipulação e retenção desses dados podem acarretar em vazamentos. Por exemplo, no setor bancário, no ano de 2019, uma falha no sistema de informação do Banco Inter acabou provocando um vazamento de dados equivalente a 1,4 milhões de clientes diretamente na internet (PAYAO, 2019). Outro exemplo também foi o vazamento de informações de cerca de 267 milhões de usuários do Facebook em 2019, desde nomes reais a números de telefone (PRETA e SCHAEFFER, 2019).

Informações pessoais são dados específicos desde localização geográfica como endereços, até dados considerados mais sensíveis como número de cartões de crédito e saldo da conta bancária. Se essas informações forem vazadas para pessoas não autorizadas, além de violar os direitos dos donos dessas informações, a empresa pode ter prejuízos a sua imagem e reputação bem como a confiança de seus clientes (DA VEIGA e MARTINS, 2015).

Segundo Vianna (2007), a privacidade pode ser dividida em três tipos de direitos e a sua junção traz o significado da privacidade, são eles:

1. **Direito de não ser monitorado**: É basicamente o direito que o ser humano tem de não ser observado, ouvido, ou qualquer outra ação relacionada que uma outra pessoa realize (VIANNA, 2007);

2. **Direito de não ser registrado:** É o direito do ser humano de não ter imagens ou conversas gravadas por terceiros, de modo que o proprietário delas não as permitam (VIANNA, 2007) ;

3. **Direito de não ser reconhecido:** É compreendido como o direito de não ter as imagens e conversas que foram gravadas publicadas na internet ou em qualquer outro meio que tenha sido feito sem permissão (VIANNA, 2007).

Alguns países possuem regulamentos de direito relacionados a regras de privacidade. Os países da União Europeia, por exemplo, são signatários da lei chamada *General Data Protection Regulation* (GDPR) (EUROPEU, 2016). A GDPR é uma série de normas que garantem direitos sobre a privacidade e proteção de dados pessoais e regulamenta também a exportação dos dados pessoais para regiões fora da União Europeia. O objetivo da GDPR é entregar aos residentes europeus maneiras deles obterem controle sobre os seus dados pessoais (EUROPEU, 2016).

Já no Brasil, com muitos aspectos semelhantes a GDPR, foi sancionada em 14 de Agosto de 2018 a Lei Geral de Proteção de Dados (LGPD) e sua iniciação de

atuação no mês de Agosto de 2020 (BRASIL, 2020). Inspirada na GDPR, a LGPD tem o objetivo de proteção de dados pessoais de qualquer brasileiro sobre a coleta, armazenamento e manipulação de dados sobre empresas tanto públicas quanto privadas dentro do território nacional.

A privacidade e a segurança das informações estão diretamente alinhadas, trazendo uma ideia única de interação. A privacidade das informações pode ser vista como “o quê” do todo, o artefato a ser protegido, a ser preservado e já a segurança da informação sendo o “como”, sendo visto como o processo e objetivo pelo qual a privacidade vai ser submetido para ficar em conformidade com a segurança (SWIRE e BERMANN, 2007).

2.5 Engenharia Social

Um do maiores desafios da segurança, e consequentemente da privacidade pelo fato de atingir diretamente os artefatos que são preservados pela privacidade, é a prática conhecida como Engenharia Social (SILVA, 2013).

Segundo Fonseca (2017), a Engenharia Social pode ser vista como uma prática utilizada por uma pessoa para se conseguir informações de seu interesse por meio de habilidades como a persuasão e a ilusão para conseguir a confiança de uma pessoa e assim fazer com que ela passe informações.

Chantler e Broadhurst (2006) afirmam que, engenharia social se caracteriza pelo manuseio de armadilhas psicológicas, a manipulação do comportamento e o uso de farsas por atacantes com intuito de ter acesso a informações de pessoas desprevenidas. O fator humano é algo bastante complexo e difícil de controlar, cada pessoa age de uma forma distinta quando está sofrendo um ataque, sendo que a maioria delas sequer percebem que estão sob ataque (FONSECA, 2017).

A engenharia social é realizada em um ciclo que segundo Mitnick e Simon (2003), é dividida em quatro etapas, que são:

1. **Obtenção de informações:** As informações são coletadas para que depois ocorra um contato com a vítima. A maior porcentagem de sucesso da engenharia social é proveniente dessa fase que ocorre de maneira bem estruturada e planejada, nesse caso existe uma maior atenção a essa etapa (HADNAGY, 2017).

2. **Desenvolvimento do relacionamento ou confiança:** Após a coleta das informações iniciais sobre a vítima, fica mais fácil determinar uma forma de abordagem. Para conseguir iniciar a conquista da confiança o engenheiro social usa informações privilegiadas sobre a pessoa, citando conhecidos dela e se passando por alguém que não é. Dessa forma, aos poucos, apresentando-se ser de confiança e com o passar do tempo desenvolver o relacionamento (MITNICK e SIMON, 2003).

3. **Exploração da confiança:** Nessa etapa, a vítima depois de ter tido a confiança conquistada pelo engenheiro social, começa a ser manipulada, para que assim comece a revelar informações e até executar alguma atividade que não ocorreria normalmente entre a vítima e um desconhecido. Essa fase o atacante tem o foco em abusar do relacionamento criado na etapa da conquista da confiança (MITNICK e SIMON, 2003).

4. **Execução objetivando a realização:** Essa fase consiste em utilizar o que foi conquistado na etapa anterior para algum benefício próprio ou para terceiros. Quando essa etapa termina, o engenheiro social tenta finalizá-la sem levantar suspeitas (MITNICK e SIMON, 2003).

Diante do que foi mencionado, pode-se resumir o conceito de engenharia social como uma arte de obter informações e/ou alguma vantagem utilizando ferramentas como a persuasão, armadilhas psicológicas, entre outras técnicas que façam proveito da vulnerabilidade do fator humano.

3. Metodologia

Neste capítulo é descrito o processo metodológico de pesquisa utilizado no decorrer do desenvolvimento do trabalho. A metodologia de pesquisa adotada neste trabalho é do processo de criação de um *survey* que é dividida em seis fases de acordo com os passos descritos em Kasunic (2005): (1) Definição da Pesquisa, (2) Caracterização do público-alvo, (3) Elaboração do questionário, (4) Condução do teste piloto, (5) Distribuição do questionário e (6) Análise dos Resultados. Os passos são ilustrados na Figura 1 e são descritos nas próximas seções com uma seção a mais comentando sobre considerações éticas.

Figura 1 - Metodologia adotada neste trabalho.

Fonte: Adaptado de Kasunic (2005).

3.1 Definição da Pesquisa

Esta etapa buscou-se entender primeiramente qual seria o objetivo da pesquisa e o que seria preciso para que ela seja realizada. Estudar o problema para saber o que existe sobre ele e entender o cenário dele foi o foco dessa etapa. O intuito da pesquisa é começar com a explicação sobre o problema e mostrar como o trabalho irá responder às perguntas do problema (KASUNIC, 2005). Nessa etapa, foi realizado uma pesquisa inicial para identificar quais problemas eram relacionados a cultura de segurança da informação e quais eram as suas possíveis soluções por meio de uma investigação no estado da arte.

O estudo foi realizado a partir de um levantamento bibliográfico sobre Segurança da Informação, Cultura de Segurança da Informação e seus métodos de avaliação. A revisão da literatura tem o objetivo de conhecer e fazer uma análise de contribuições dos estudos, tendo como exemplo a área científica, de algum assunto, tema ou problema. A motivação é conseguir apresentar um problema com o uso de referências teóricas existentes em documentos como livros e artigos científicos (CERVO e BERVIAN, 2002). A pesquisa foi conduzida utilizando várias fontes de informação como artigos publicados, livros, jornais e outras fontes secundárias como sites.

Os tipos de pesquisa podem ser classificadas pelo ponto de vista de objetivo como exploratória, descritiva e explicativa (SILVA e MENEZES, 2005). A pesquisa do tipo descritiva faz a utilização de técnicas padronizadas para coleta de dados como por exemplo o uso de questionários e observações sistemáticas. Sendo assim, o foco é realizar levantamento de informações (SILVA e MENEZES, 2005).

Esse trabalho possui características que mais se assemelham ao tipo descritivo, pois o objetivo é caracterizar as práticas relacionadas a cultura de segurança da informação das organizações por meio de um questionário. O objetivo da aplicação de um questionário é conseguir, por meio de uma amostra de um público, conseguir inferir características e comportamentos para o público em geral (GIL, 2008). Dentre as vantagens de se utilizar um questionário é o baixo custo de implementação e a possibilidade de conseguir um grande número de participantes do público-alvo (SILVA e MENEZES, 2005).

3.2 Caracterização do público-alvo

Nesta etapa o foco foi fazer o reconhecimento do público que participaria da pesquisa. Os procedimentos incluíram avaliar o entendimento das perguntas por meio do uso de termos de fácil compreensão e definir as informações que seriam coletadas desse público (KASUNIC, 2005). Após o problema definido, foi necessário refletir qual público seria incluído na pesquisa, para isso, primeiramente, o intuito foi priorizar funcionários de uma empresa, mas depois foi decidido que o escopo poderia abranger funcionários de mais organizações para que fosse possível observar resultados vindos de diferentes origens.

O público foi escolhido com base em quem pode fornecer melhor as informações que seriam necessárias para a pesquisa (KASUNIC. 2005). As pessoas que foram escolhidas para serem o público desta pesquisa foram funcionários de diferentes segmentos de empresas que entrassem em contato com a divulgação da pesquisa. Sejam de instituições públicas ou privadas, sejam empresas de tecnologia da informação ou não. O objetivo foi conseguir uma gama de diferentes perfis de funcionários para que diferentes cenários pudessem ser analisados posteriormente.

O desenvolvimento das perguntas e temas do questionário que serão interpretados pelo público é de extrema importância e os itens devem ser criados a partir da perspectiva do voluntário e não a do pesquisador (KASUNIC, 2005). Foi necessário entender que o público por ser muito abrangente, poderia acabar não entendendo alguns termos e a informação que cada uma das perguntas do questionário iria obter. Então, em vários momentos foi necessário considerar a reestruturação dos itens para que fossem de mais fácil compreensão pelos entrevistados conforme discutido na próxima seção.

3.3 Elaboração do questionário

O objetivo nessa fase foi estipular quais temas estariam no questionário e como eles poderiam ser colocados em forma de pergunta, além de pensar em formas de como facilitar a análise das respostas na parte de coleta dos dados (KASUNIC, 2005). Com um estudo prévio, foram definidos os temas que seriam contemplados no trabalho tendo como base questionários presentes na literatura.

As perguntas foram separadas em várias planilhas, e após uma análise mais profunda, foram escolhidas quais perguntas seriam incluídas no questionário.

O *survey* foi baseado em trabalhos existentes como, por exemplo, o trabalho de Martins e Da Veiga (2015) e o trabalho de Arteiro (2015). Este trabalho possui maior influência do trabalho de Da Veiga (2018) com o uso do ISCA pelo fato de dele ter sido referência para vários outros trabalhos da área de cultura de segurança da informação. Sobre as principais diferenças deste trabalho para os trabalhos existentes são que essa pesquisa pôde ser aplicada em várias organizações que diferente dos outros, o estudo era feito em uma única organização.

Além disso, uma área que não foi abordada no ISCA, mas foi contemplada neste estudo, por conta de sua relevância com a cultura de segurança da informação, foi a Engenharia Social. Nela, tiveram perguntas que avaliavam o conhecimento dos participantes desde a compreensão do termo, até percepções em situação de vulnerabilidade. Essa nova dimensão foi inserida no estudo em virtude de grande parte das vulnerabilidades presentes em uma Organização são decorrentes do fator humano conforme discutido no Capítulo 1. Foi necessário adaptar algumas perguntas de forma que fosse coletada uma visão geral da Organização e não apenas departamentos específicos como é avaliado no ISCA.

O questionário, que foi elaborado em português, foi dividido em quatro partes:

1. Questões referentes ao perfil e experiência dos participantes. Foram incluídas 10 perguntas referentes ao tipo de instituição, estado/país no qual a empresa está localizada, porte e segmento da empresa, cargo desempenhado pelo participante, tempo na organização, titulação e experiência com segurança da informação
2. 10 Questões referentes à percepção do participante sobre Segurança da Informação;
3. 10 Questões sobre Princípios de Segurança da Informação;
4. 1 Questão aberta ao final para comentários adicionais.

O questionário completo é apresentado no Apêndice A.

3.4 Condução do teste piloto

Posteriormente, foi realizado um teste piloto com dois voluntários que trabalham com informações do segmento de tecnologia da informação e na área de educação. Os participantes forneceram comentários sobre questões que continham dupla interpretação, sugeriram novas opções de resposta e outros comentários relevantes para melhorar o entendimento do questionário. A partir dos comentários recebidos no teste piloto, o questionário foi melhorado e distribuído para os participantes conforme discutido na próxima seção.

3.5 Distribuição do questionário

O questionário foi divulgado para o público-alvo selecionado definido na etapa 3 (KASUNIC, 2005) por meio do Google Forms. O trabalho foi compartilhado em vários canais de comunicação como redes sociais como Facebook, Twitter, Linkedin e Whatsapp, e convites por email, para que pessoas que pertencentes ao público da pesquisa pudessem responder. O questionário esteve disponível para respostas por quatro meses de Julho a Setembro de 2020.

A maior parte dos levantamentos existentes não é realizado com os todos os integrantes alvos em virtude do universo que pode ser grande demais (GIL, 2008). Esse é o caso do presente estudo que possui um alto número de potenciais participantes, não sendo possível determinar o valor total de possíveis respondentes.

3.6 Análise dos Resultados

As respostas foram coletadas assim como foi definido o formato de apresentação dos resultados, seja por gráficos ou relatórios. Sendo então possível obter um parecer do cenário dos resultados (KASUNIC, 2005). O questionário foi amplamente divulgado e foi recebido um total de 75 respostas cujos resultados são apresentados e discutidos no Capítulo 4.

As conclusões do trabalho foram obtidas a partir das respostas na pesquisa. Por meio da realização desse *survey* foi possível obter dos voluntários da pesquisa qual o seu grau de conhecimento e quais as suas possíveis ações em relação a situações relacionadas à segurança da informação.

3.7 Ameaças à validade e considerações éticas

A avaliação das ameaças à validade deste estudo considerou os tipos de ameaças propostos por Wohlin *et al.* (2012): Validade de Conclusão, Validade Interna, Validade de Constructo e Validade Externa. Essa seção apresenta as ameaças que foram identificadas durante a pesquisa.

3.7.1 Validade de Constructo

A relação que existe nessa validade é a de teoria e observação. Dois aspectos que devem ser assegurados é que o deve fazer uma reflexão direta da construção da causa e que o resultado externa bem a construção do resultado (Wohlin et al, 2012). As falhas podem vir do experimentador ou dos participantes.

A dificuldade de entendimento das perguntas é visto como uma ameaça deste trabalho uma vez que, dependendo da forma com a qual os participantes interpretem as perguntas, pode-se obter resultados errôneos. Para mitigar essas ameaças, o survey foi feito de maneira iterativa e foi conduzido um teste piloto com dois profissionais para avaliar a compreensão das perguntas e sua adequação ao

propósito da pesquisa. A partir do feedback recebido, o questionário foi refinado. Além disso, o instrumento que foi a base para a pesquisa, o ISCA, já foi validado por autores independentes havendo várias rodadas de discussão para obter a versão final.

3.7.2 Validade Interna

Essa validade faz a observação da relação entre o tratamento dos dados e o resultado e deve existir de fato uma relação de causa, e que não é algo que não exista um controle ou não foi medido. Em resumo, o tratamento gera o resultado (Wohlin et al, 2012). A principal ameaça dessa validade é a seleção dos participantes. Apesar do questionário ter sido divulgado em diversos canais de comunicação, os resultados podem sofrer de um potencial "viés de não resposta" (ou seja, as opiniões dos entrevistados que escolheram participar podem ser diferentes daqueles que não o fizeram). Mesmo assim, as 75 respostas recebidas fornecem uma rica fonte de dados para revelar as conclusões apresentadas neste trabalho.

3.7.3 Validade de Conclusão

Esse tipo de validade está relacionado com o tratamento e resultado dos dados para chegar em uma conclusão correta que envolve, por exemplo, a questão da confiança e se o resultado tem de fato um significado (WOHLIN et al, 2012). Neste trabalho, os resultados podem ter sido afetados por um fator externo correspondente a pandemia do COVID-19. A pesquisa foi conduzida na época da pandemia (Julho à Setembro de 2020) e vários participantes podem não estar em seu local de trabalho habitual. Sendo assim, as respostas podem refletir esse novo padrão de comportamento de alguns participantes. Finalmente, existe o risco dos dados fornecidos pelos participantes não correspondem à realidade por ser uma pesquisa baseada em opinião. Entretanto, acredita-se que esse risco é mínimo e não gera impacto impacto significante nas conclusões deste estudo.

3.7.4 Validade Externa

Essa validade tem relação com a generalização. Se existe uma relação de causa entre a construção da causa e resultado, o produto do estudo consegue ser generalizado, ou não. Existe realmente alguma relação entre o tratamento e resultado ou não (Wohlin et al, 2012). O tamanho da amostra é uma ameaça para generalização dos resultados desta pesquisa. Apesar dos esforços despendidos na divulgação e convocação de participantes, o número de respostas obtido não foi alto, no total 75. Entretanto, essa uma característica inerente a este tipo de método de pesquisa e importantes conclusões para o estado da arte e da prática já foram obtidas por meio deste método.

3.7.5 Ética

Considerando os princípios éticos na condução desse trabalho, foram adotadas medidas para não permitir a identificação dos participantes, sendo o questionário respondido de forma anônima. Além disso, antes de responder ao questionário, o termo de consentimento livre e esclarecido era apresentado aos participantes e o consentimento era solicitado. O termo possuía o conteúdo apresentado no Apêndice B.

4. Resultados e Discussão

Neste capítulo serão apresentados os resultados e a discussão sobre a aplicação do instrumento. Nas seções seguintes serão apresentados os perfis dos participantes, suas percepções sobre segurança da informação e dos princípios de segurança da informação bem como uma análise dos resultados encontrados.

4.1 Perfil dos Participantes

Esta pesquisa recebeu respostas de 75 participantes, pertencentes, em sua maioria, a instituições privadas (65,3%), seguido de instituições públicas (33,3%), conforme ilustrado na Figura 2.

Figura 2 - Tipo de instituição que os participantes estão vinculados.

As instituições estão distribuídas em diversos estados conforme apresentado na Figura 3. Observou-se uma predominância de participantes oriundos do estado de Pernambuco, o que representou um resultado um pouco esperado já que a rede de contatos do autor encontra-se no estado de Pernambuco, então mais convites foram enviados para essas pessoas. Respondentes de outros estados brasileiros conseguiram ser alcançados (12 estados). Além disso, foram obtidas duas respostas de pessoas de fora do Brasil.

Figura 3 - Localização das empresas.

As instituições estão distribuídas em diferentes portes como pode ser observado na Figura 4. Neste trabalho, foi adotada a classificação do SEBRAE (2013) de Microempresa, Pequeno, Médio e Grande porte. Apesar da maioria das respostas serem provenientes de profissionais de empresas de grande porte, mais de 25% das respostas são de profissionais de empresas de pequeno porte.

Figura 4 - Porte das empresas.

Houveram respostas de variados segmentos de empresas, como por exemplo, empresas de educação e empresas do governo, como apresentado na Figura 5. A maior parte das respostas foi do segmento Informática seguido pelo segmento de Educação, com uma participação expressiva no total das respostas.

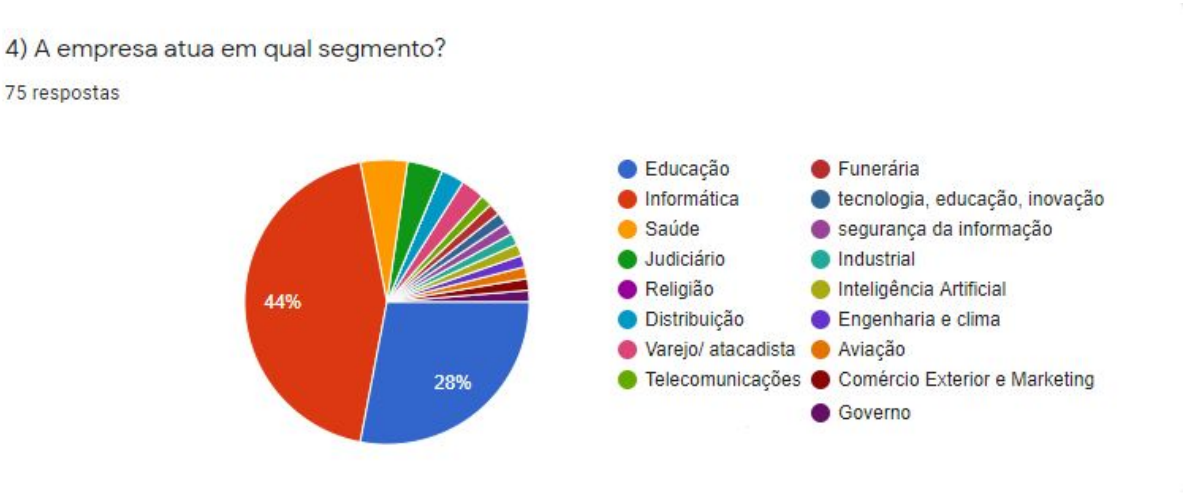

Figura 5 - Segmentos das empresas.

Os cargos ocupados pelos profissionais que responderam a pesquisa foram bem diversificados como ilustrado na Figura 6. O cargo que apresentou um número maior de respostas foi o de Analista, após agrupar os diferentes tipos (Analista de testes, Analista de TI, entre outros), representando 15% das respostas. Logo em seguida, o cargo de Professor, resultado de certa forma esperado uma vez que o questionário foi distribuído em várias redes sociais que participam professores e grupos educacionais.

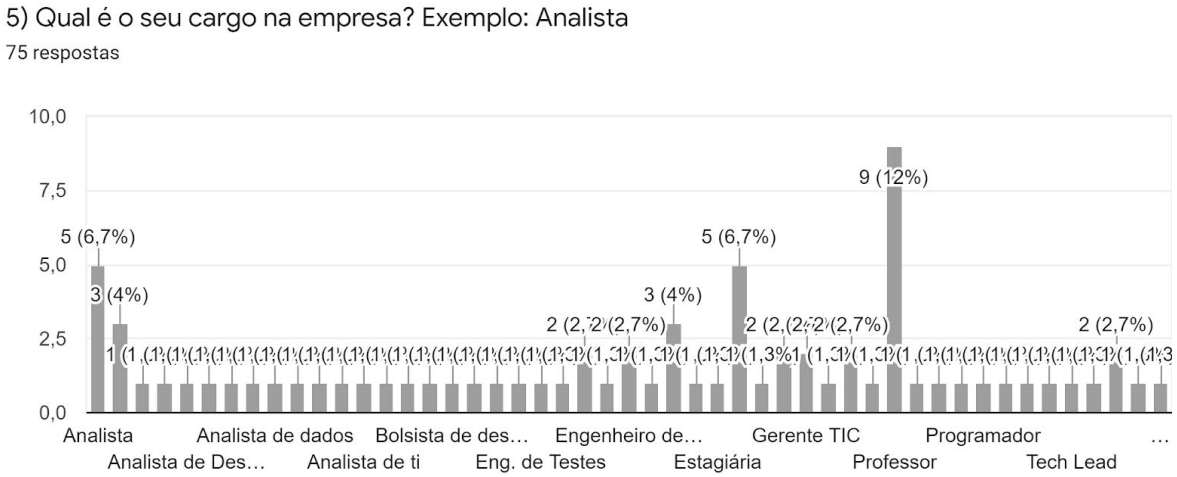

Figura 6 - Cargos nas empresas.

Na Figura 7, é possível observar que 86,7% dos voluntários estão na organização atual há menos de seis anos. Para esta pesquisa, foi importante obter perfis heterogêneos uma vez que é possível compreender como o tempo de experiência impacta na percepção de segurança do participante desta pesquisa.

Figura 7 - Tempo de trabalho nas organizações.

A distribuição da titulação dos participantes foi variada, como mostrado na Figura 8. A titulação de Ensino Médio/Técnico obteve a maior porcentagem das respostas, seguido de Graduação, Especialização, Mestrado e Doutorado. Foi importante também ter tido uma resposta da titulação de pós-doutorado, pois assim é possível coletar uma visão desse grau de titulação.

Figura 8 - Maior titulação concluída.

Apesar da maioria dos participantes não terem participado de nenhum treinamento ou capacitação sobre segurança da informação, o total foi bem dividido com apenas 10% de diferença entre os que fizeram ou não algum treinamento ou capacitação, como apresentado na Figura 9. A partir desse levantamento, foi possível entender um pouco o perfil de resposta dos dois lados, daqueles que já fizeram alguma capacitação e aqueles que também talvez nunca tenha tido contato. Essa análise é realizada na Seção 4.22.

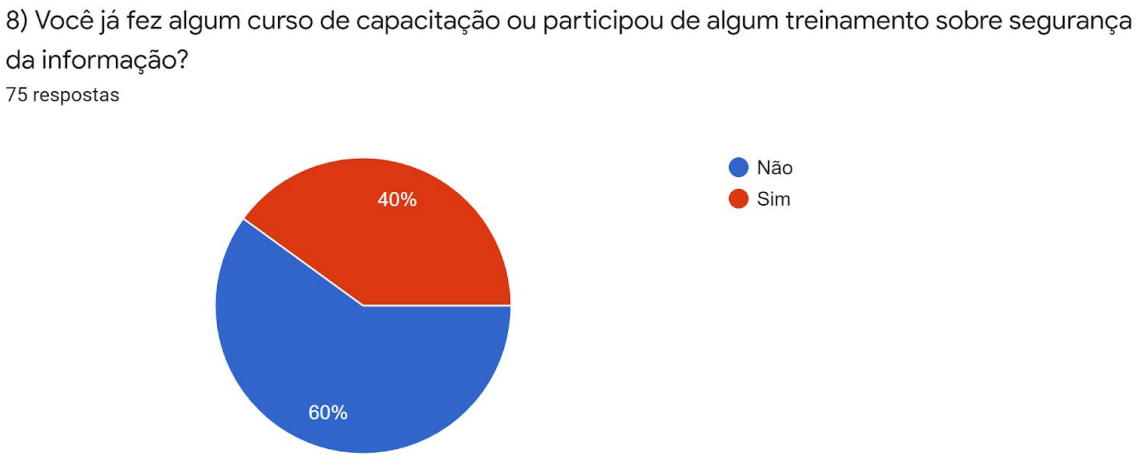

Figura 9 - Capacitações ou treinamentos praticados pelos participantes.

Caso o participante tivesse feito alguma capacitação, a próxima pergunta solicitava detalhes a respeito como, por exemplo, ano, a carga horária e os tópicos abordados. Ao total foram registradas 27 respostas.

Algumas das respostas foram:

Participante 1: *"Avaliação dos Planos Municipais de Carreira da Educação, em especial dos professores, no ano de 2017, 20h, para analisar fluxos, impactos financeiros, evolução na carreira."*

Participante 2: *"Semestralmente desde 2018. Temas abordados: cyber attacks, confidencialidade, segurança da informação"*

Participante 3: *"Diversos. Faço capacitações frequentes, sem periodicidade regular, com cargas horárias variando na faixa de 6 a 40 horas, cada."*

A pergunta final sobre o perfil dos participantes envolvia o tratamento de informações sigilosas. O intuito dessa pergunta era obter quantos participantes já haviam trabalhado com esse tipo de informação como também se eles também tinham conhecimento sobre o conceito. Boa parte, cerca de 24 participantes, especificou que nunca havia trabalhado com esse tipo de dados. 68% dos participantes já trabalharam com esse tipo de informação, algumas das respostas foram:

Participante 1: *"Sim, a atenção aumenta. Você tende a se sentir mais em alerta"*

Participante 2: *"Sim. A empresa considera qualquer informação pessoal dos usuários como sigilosa. Há um cuidado especial para não usar dados de produção*

não-ofuscados, assim como o acesso direto à base de produção é totalmente restrito. Os dados são armazenados criptografados e sempre trafegados usando https."

Participante 3: *"Sim. Trabalhei primeiramente em um projeto onde o produto final do cliente não podia ser revelado e era tranquilo manter o sigilo. Atualmente trabalho em um projeto cujas informações do cliente são todas sigilosas, inclusive o nome e os serviços prestados a ele. Utilizamos codinome e é complicado lidar com a curiosidade dos colegas de outros projetos."*

Em resumo, os participantes afirmaram que já trabalharam com informações sigilosas e afirmaram que ficam mais atentos quando estão trabalhando, pois qualquer descuido pode acabar comprometendo as informações. Os participantes responderam também que se sentem entusiasmados quando trabalham com informações sigilosas, pois indica que são de extrema relevância e os faz se sentir mais importantes.

Nas próximas seções são discutidas as respostas dos participantes sobre suas percepções relacionada a temática abordada neste trabalho. As perguntas foram estruturadas em duas seções: a primeira sobre Percepção de Segurança da Informação e a segunda seção era correspondente aos Princípios de Segurança da Informação. A maioria das respostas seguem uma escala Likert de quatro a cinco opções.

A seções estão agrupadas nas dimensões abordadas no ISCA: Gerenciamento de Usuários, Gerenciamento de Ativos da Informação, Políticas de Segurança da Informação, Programa de Segurança da Informação, Liderança em Segurança da Informação, Confiança, Gestão de Mudança, Treinamento e Conscientização e Percepção de Privacidade definidos, junto com a dimensão de Engenharia Social adicionada nesta pesquisa todos definidos no Capítulo 2.

4.2 Engenharia Social

O foco da primeira pergunta sobre Percepção de Segurança foi Engenharia Social. O objetivo da pergunta foi identificar se o participante entende o que é essa prática e sua definição. Com a análise da Figura 10, é possível concluir que cerca de 49,3% dos participantes acredita que Engenharia Social é a habilidade de coletar dados sensíveis por meio da persuasão. Esta definição foi retirada do trabalho de Henriques (2017) e é discutida no Capítulo 2.

Por outro lado, cerca de 22,6% não sabe ou não acredita que essa seria a definição correta para essa prática. Esses resultados estão alinhados com os obtidos por Henriques (2017), ainda que em proporção menor (49,3% x 86.10%), de que a maioria das respostas dos participantes convergem para concordar que essa definição está correta.Isso demonstra que é possível concluir que as pessoas

possuem a noção da existência da Engenharia Social, mesmo em diferentes segmentos de organizações.

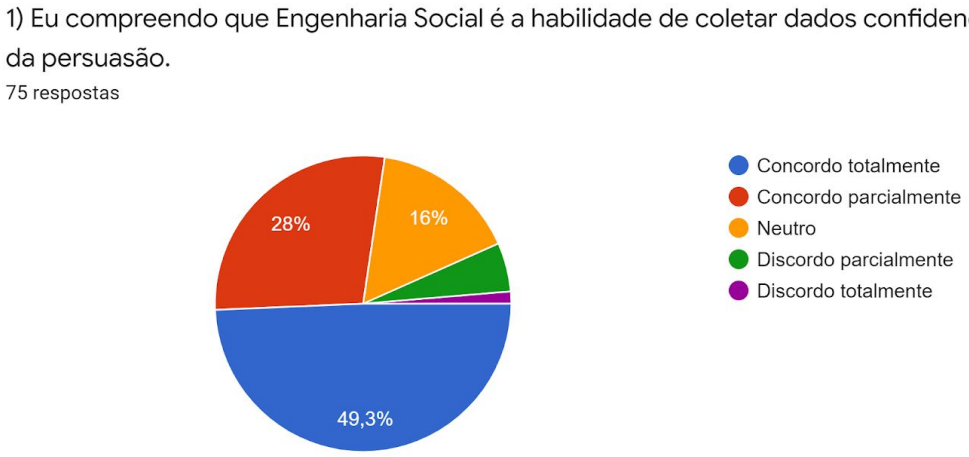

Figura 10 - Compreensão da Engenharia Social.

Observa-se na Figura 11 que 64% dos respondentes aprovam completamente que as atividades que envolvem a organização só devem ser executadas ou disponibilizadas, se a pessoa tiver permissões da organização. Cerca de 24% também acredita que é importante levar a pessoa autorizada em consideração, o que somado a porcentagem anterior apresenta a maioria dos pesquisados, cerca de 88%. Com isso, apenas 12% dos participantes representam alguma vulnerabilidade em relação a uma situação semelhante a descrita acima.

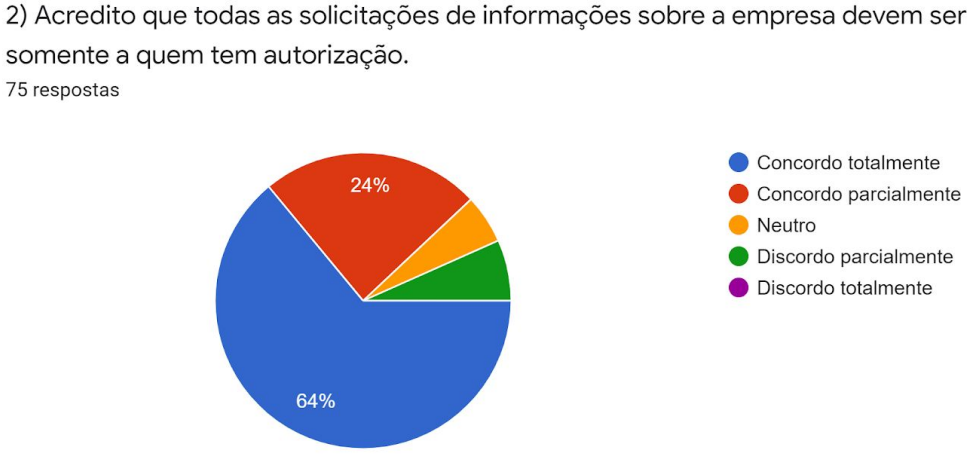

Figura 11 - Compreensão sobre compartilhamento de dados da organização.

Para informar pessoas que possuem um perfil de vulnerabilidade, de acordo com a ABNT (2013), a Política de Segurança de Informação e Comunicações das organizações devem conter os conceitos básicos da Segurança da Informação, de

uma forma que o objetivo seja ter o controle da segurança da organização para que assim seja possível reduzir possíveis ameaças.

Na Figura 12 é possível observar que a maioria dos respondentes passou por um cenário de possível roubo de informações pelo menos uma vez, cerca de 81,3%. Com relação a frequência do roubo de dados, a maioria indicou que existe uma certa frequência de Muitas ou Algumas vezes pelas quais cenários como estes de possível roubo de dados são comuns.

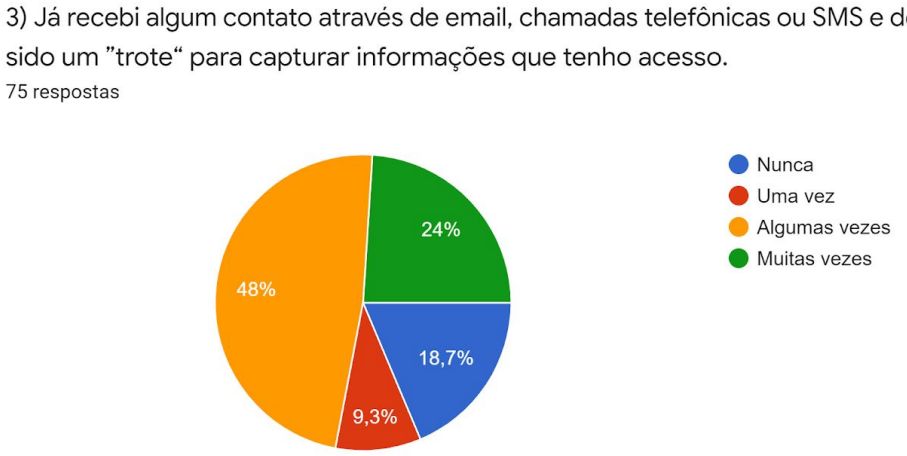

Figura 12 - Percepção de possível roubo de dados.

De acordo com Hadnagy (2011), a Engenharia Social é descrita como o ato de manipulação de uma pessoa para que ela execute ações que não eram de seu interesse ou objetivo. Com base nessa definição, 18,3% dos participantes afirmaram que nunca passaram por essa situação. Esse resultado pode indicar que essas pessoas talvez nunca tenham passado por essa situação ou pode ser uma brecha na percepção de segurança dessas pessoas, pois esses participantes podem já ter passado por esse tipo de situação e nunca terem entendido de fato a ameaça que poderiam estar correndo. Já podem ter executado ações, ou passado informações e de fato, no momento, poderiam não ter percebido.

4.3 Gerenciamento de Usuários

É possível observar na Figura 13, que a maior parte dos participantes, cerca de 72%, afirmaram ter conhecimento a respeito dos procedimentos de segurança da informação da sua respectiva organização. Isso representa dois pontos de vista, o primeiro que as organizações estão se preocupando em divulgar de uma forma mais adequada, por meio de comunicados diretos, por exemplo, para que os seus colaboradores saibam o que é necessário que eles façam para evitar futuros incidentes. E o segundo é que como as pessoas, de alguma forma, conhecem os procedimentos segurança da organização, elas acabam atribuindo maior importância para esta área.

Estes resultados estão alinhados com os obtidos por Da Veiga e Martins (2015), em que os autores investigam, em uma organização, a evolução da cultura da segurança da informação em dois diferentes anos. No trabalho deles, os resultados sobre a percepção de Política de Segurança da Informação na visão dos colaboradores apresentou além de uma melhora de um ano para outro como também a maioria demonstrou conhecimento sobre esse ponto com 82,5% de aceitação.

Do total de 75 respondentes, 10,7% acabaram afirmando que não possuem conhecimento sobre os procedimentos de segurança da informação da sua organização. Esse dado indica que as organizações precisam melhorar as campanhas de conscientização de seus colaboradores Isso não implica dizer que as empresas desses respondentes não se preocupam com a segurança da informação ou que ela não possua uma Política de Segurança da Informação, porém precisam aprimorar sua divulgação e clareza.

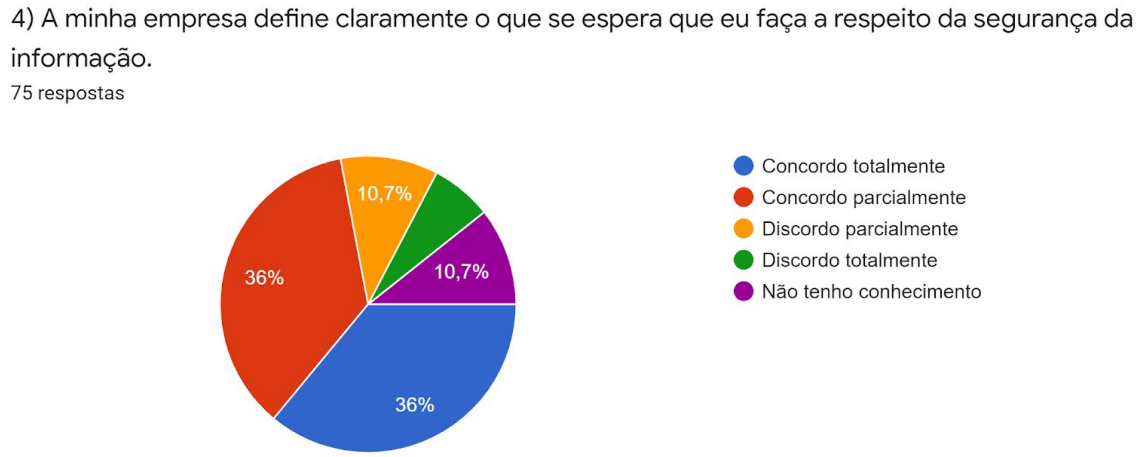

Figura 13 - Conhecimento dos participantes sobre a segurança da informação da organização.

Observa-se na Figura 14 que 32% dos participantes discordam que o departamento de Tecnologia da Informação (TI) é o responsável pela segurança da informação na organização. Em contrapartida, 64% concordam que é responsabilidade deste departamento a gestão da segurança da informação. Esses dados podem significar duas possibilidades: a primeira é que os entrevistados acreditam que apenas esse departamento é que deve se preocupar com a segurança da informação da empresa; a segunda pode ser os entrevistados acreditem que o departamento de TI tem um papel fundamental na segurança da informação da organização.

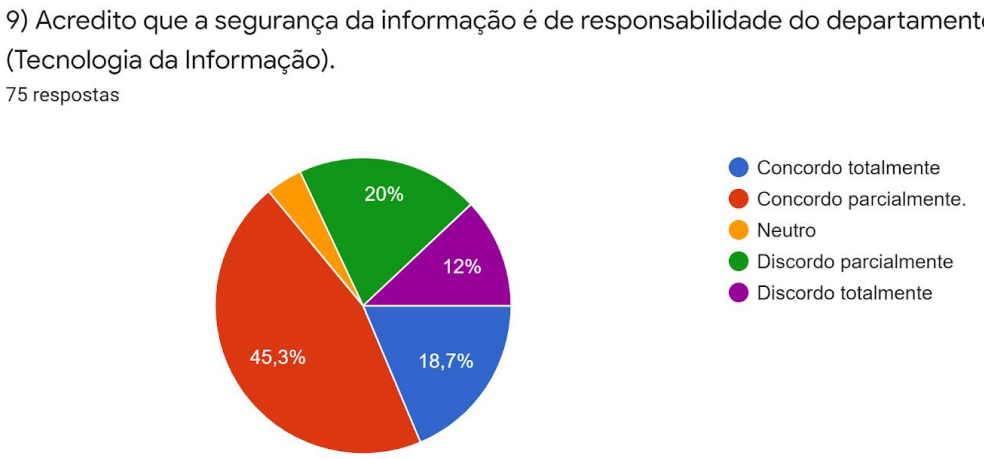

Figura 14 - Participantes que acreditam na responsabilidade do departamento de TI.

Na Figura 15, é possível observar que 88% dos participantes concordam que penalidades devem ser aplicadas aos colaboradores que não respeitarem as políticas de segurança da informação da organização. Isso implica afirmar que os participantes acreditam que a política de segurança da informação da organização é algo a ser respeitado, e que se a política for desrespeitada , é necessário que a organização aplique uma punição adequada.

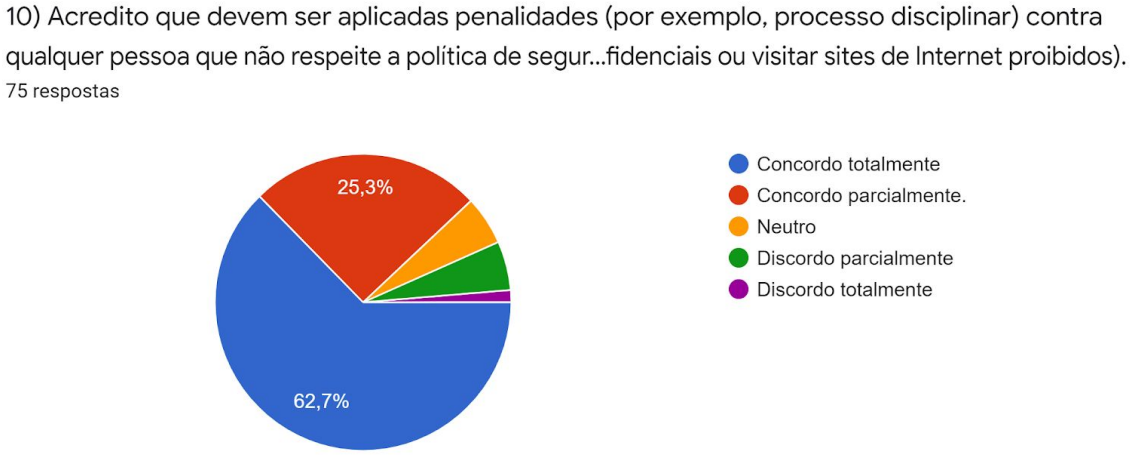

Figura 15 - Participantes que acreditam que penalidades devem ser aplicadas àqueles que não respeitam a política da organização.

Ao comparar com o trabalho de Martins e Da Veiga (2014), nota-se que no tópico que aborda as políticas de segurança da informação da empresa, os participantes apresentaram uma taxa de concordância de 72,6% no primeiro ano da aplicação do ISCA em 2006 e 82,5% no último ano da aplicação em 2013. Estes dados reforçam a importância de investir na conscientização dos colaboradores da empresa como forma de reduzir as vulnerabilidades. Além disso, observa-se uma

taxa de similar neste trabalho com os resultados obtidos em Martins e Da Veiga (2014).

4.4 Gerenciamento de Ativos da Informação

Na Figura 16 é destacado, em 98,7% das respostas, que os ativos de informação físicos e eletrônicos da organização devem ter uma atenção dedicada e devem ser protegidos. Isso implica em afirmar que os participantes acreditam que, de certa forma, os ativos da organização representam um bem importante e que precisam ser preservados. Ainda houve uma resposta sobre o participante não ter conhecimento, mas comparado a maioria das outras respostas, essa resposta pode ser considerada como uma exceção.

Comparado ao trabalho de Da Veiga e Martins (2015), os resultados discorrem de maneira semelhante, se realizada uma análise de acordo com a dimensão que aborda esse tema de ativos da informação. Os funcionários da organização do estudo de Da Veiga e Martins responderam com um grau de aceitação de 91,2% no último ano da aplicação do ISCA nessa organização. De maneira geral, observa-se ampla aceitação dos participantes.

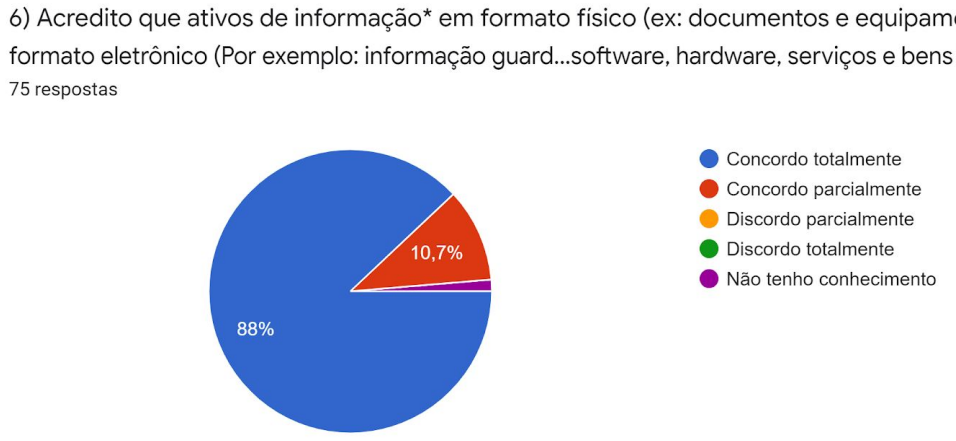

Figura 16 - Proteção da organização sobre os ativos da informação na visão dos colaboradores.

É possível observar na Figura 17 que 78,7% dos participantes afirmaram que a organização em que eles trabalham oferece atenção a proteção dos ativos físicos da organização. Esse resultado demonstra que na visão dos empregados, as organizações apresentam cautela para proteger esses tipos de ativos. Em contrapartida, cerca de 12% informaram que sua respectiva organização não gerencia seus ativos físicos.

Uma cultura de segurança da informação bem aplicada minimiza os riscos aos ativos de segurança da informação, reduzindo o mau comportamento em relação às práticas de segurança da informação dos funcionários, consequentemente diminuir o número de incidentes (DA VEIGA e ELOFF, 2010).

Nesse caso, a probabilidade da empresa obter prejuízos por conta dessas brechas é algo a ser discutido.

Figura 17 - Proteção da organização sobre os ativos da informação físicos na visão dos colaboradores.

Na Figura 18, semelhante à pergunta anterior, a maioria dos participantes, cerca de 86,6%, acredita que a organização oferece um bom nível de proteção para os seus ativos da informação no formato eletrônico. Isso demonstra que as organizações se preocupam como os seus dados salvos em plataformas eletrônicas estão armazenados.

Figura 18 - Proteção da organização sobre os ativos da informação eletrônicos na visão dos colaboradores.

4.5 Políticas de Segurança da Informação

Na Figura 19, observa-se que as respostas foram diversificadas quanto ao nível de dificuldade de compreensão da política de segurança da informação da organização. Apenas 3,9% dos participantes afirmaram que possuem facilidade em entender a política da organização. Essa conclusão, de certa forma, foi uma

surpresa, pois uma organização, que quer diminuir os riscos relacionados a incidentes com informações, deve ter uma política de segurança da informação clara e objetiva (DA VEIGA e MARTINS, 2015).

Outra observação é que 30,7% dos participantes não conhecem a política de segurança das suas respectivas organizações. Uma possível consequência dessa situação é que os funcionários podem acabar cometendo infrações sem que percebam por não possuírem o conhecimento necessário. Além disso, ataques de Engenharia Social podem acontecer com mais facilidade, pois a organização não oferece o suporte aos seus colaboradores sobre informações que são necessárias para conformidade com a segurança da informação. Assim, a empresa pode ter um perfil de funcionários com uma brecha para incidentes.

Também é notório que, 14,7% afirmam que conhecem a política de segurança da informação das suas organizações, porém acreditam que elas sejam de difícil compreensão. Isso pode ser visto como algo negativo, pois também pode abrir brechas para vazamentos de dados ou outros incidentes, caso os colaboradores não compreendam de forma clara qual a ação correta a se fazer. Portanto, é necessário que as empresas destinem esforços para tornar a política clara e realizar treinamentos contínuos para seus colaboradores.

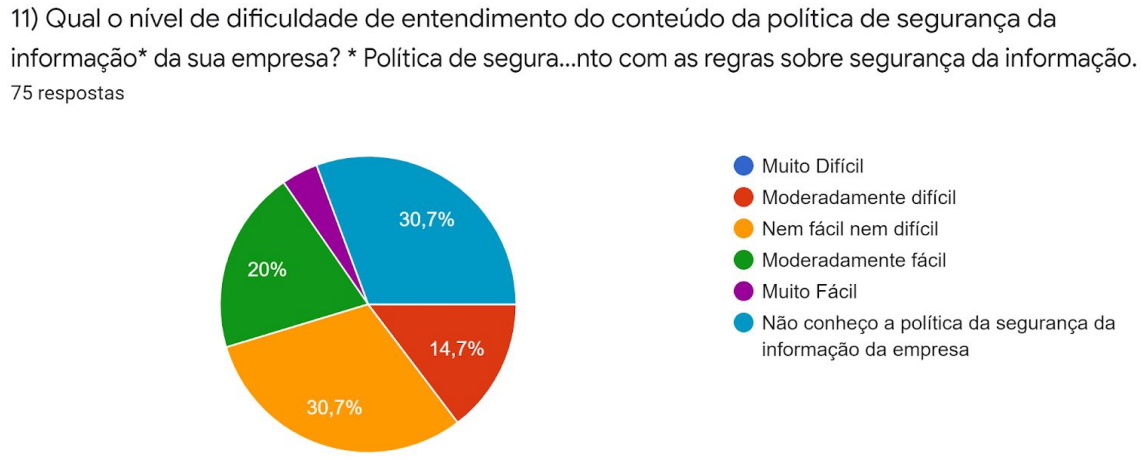

Figura 19 - Nível de dificuldade de compreensão dos participantes.

Pode-se observar que, na Figura 20, 84% dos respondentes afirmam ser comprometidos com a política de segurança da informação de suas respectivas organizações, sendo que 56% confirmam com certeza que a segue completamente. Comparado com a pergunta anterior, é possível concluir que existe uma incongruência entre o que os participantes sabem sobre a política de segurança da organização e o que de fato eles acreditam que seguem. Se cerca de 30,7%, na Figura 19, afirmam que não compreendem a política de sua organização, uma possível explicação para estes resultados é que os participantes conseguem supor

os procedimentos contidos na política da empresa, mas não tem clareza do que seja.

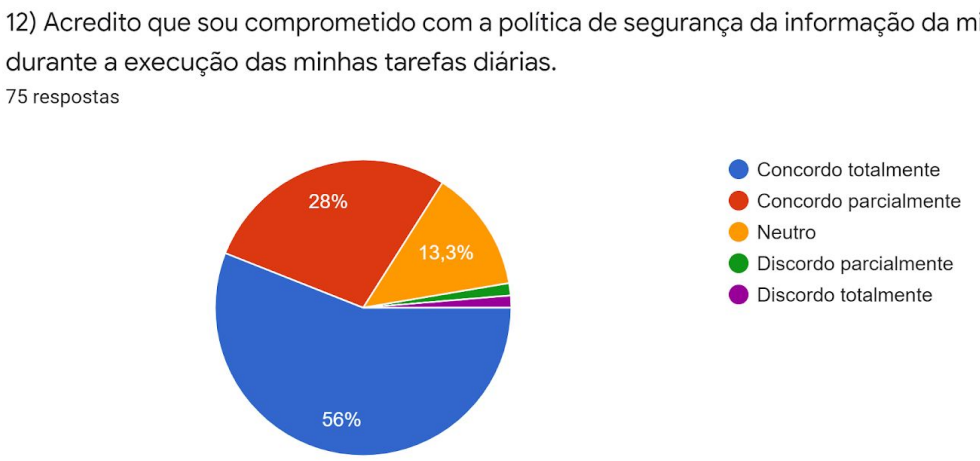

Figura 20 - Comprometimento dos participantes com a política da organização.

4.6 Programa de Segurança da Informação

Na Figura 21, é possível visualizar a diversidade da distribuição das respostas quanto ao engajamento em segurança da informação que as organizações promovem aos seus colaboradores. Foi uma surpresa desta pesquisa, pelo fato da Figura 19 ter apresentado que 30,7% dos participantes nem sequer conheciam sobre a política de segurança da informação da organização, observar que proporcionalmente os resultados foram semelhantes.

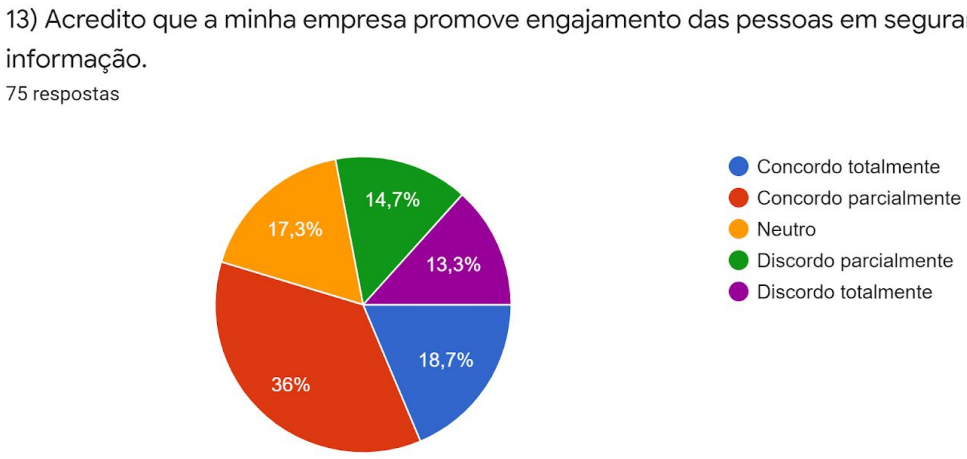

Figura 21 - Engajamento das pessoas com a segurança da informação pela empresa.

Levando em consideração os que responderam que as empresas promovem engajamento, cerca de 54,7%, ou seja, um pouco mais da metade, afirmaram que as suas organizações demonstram algum grau de preocupação em relação a

segurança da informação com seus colaboradores. Isso de certa forma é um pouco preocupante, pois, em contrapartida, 28% dos participantes responderam que as suas organizações não demonstram esse engajamento.

Essa falta de engajamento pode fazer com que seus colaboradores possam acabar não se informando sobre os riscos que a empresa pode correr se seus funcionários não demonstrarem entendimento boas práticas de segurança da informação. Sendo assim, observa-se um certo nível de vulnerabilidade no fator humano da organização.

4.7 Liderança em Segurança da Informação

Observa-se que 65,4% dos participantes, na Figura 22, afirmam que os seus colegas de trabalho demonstram comprometimento com a segurança da informação das suas empresas. Já 26,6% responderam que seus colegas não apresentam comprometimento e 8% afirmaram não ter ciência. Isso é resultado preocupante pelo fato de que uma boa parcela dos participantes entende que seus colegas de trabalho acabam deixando algumas brechas que podem ser exploradas por pessoas má intencionadas.

Além disso, 8% afirmaram não possuir conhecimento. É possível, portanto, destacar, que ou o colaborador não tem conhecimento sobre ações relacionadas a segurança da informação ou não têm conhecimento sobre práticas de seus colegas.

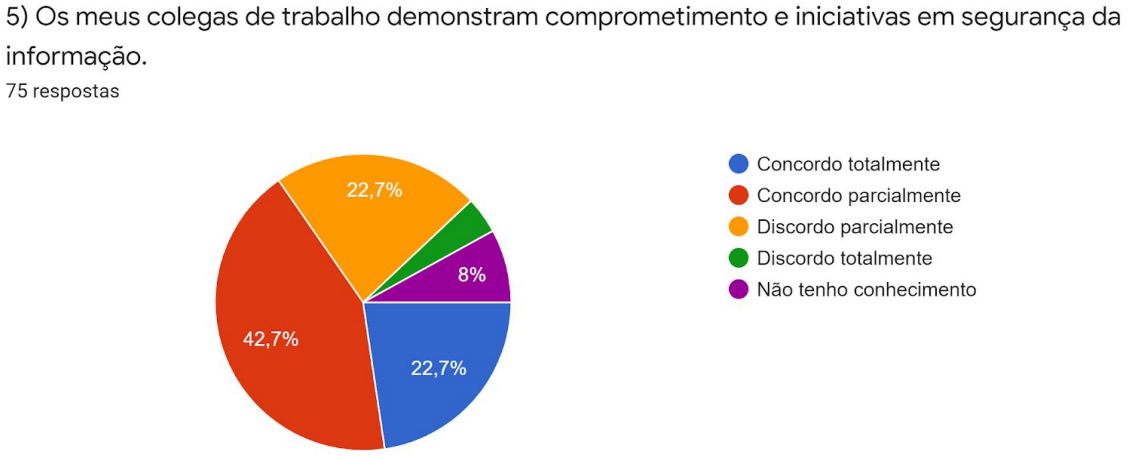

Figura 22 - Conhecimento dos participantes sobre as práticas de segurança da informação de seus colegas de trabalho.

A Figura 23 demonstra que as opiniões foram diversificadas. 30,7% dos participantes responderam que estão neutros quanto aos prestadores de serviço. É possível interpretar esses resultados de duas maneiras: a primeira é que a organização não é transparente para seus funcionários sobre se os seus prestadores de serviço implementam cuidados necessários. A segunda é que os

participantes deste estudo podem não conseguir ter acesso a essa visão diretamente das prestadoras pelo fato delas não agirem de forma transparente em relação a esta temática.

Em contrapartida, 50,6% concordam que os prestadores demonstram essa preocupação em preservar de forma confidencial, as informações que elas possuem sobre as organizações. Como essa opção acabou apresentando metade das respostas (50,6%), é possível concluir que boa parte das prestadoras de serviço demonstram esse tipo de comprometimento, mas que precisam melhorar na questão de transparência em relação aos demais colaboradores.

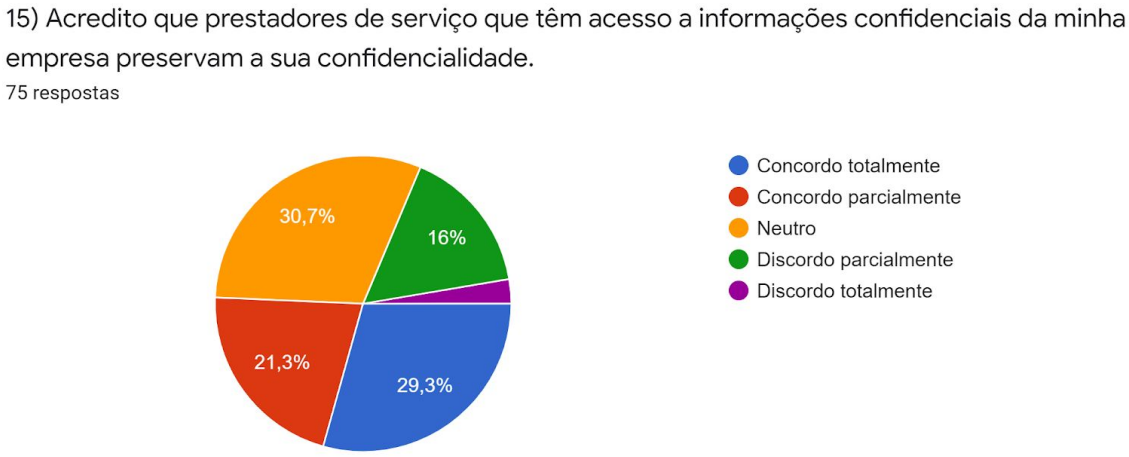

Figura 23 - Opinião dos participantes quanto aos prestadores de serviço da sua organização.

4.8 Confiança

É possível observar na Figura 24 que 70,7%, a maioria, acredita que a organização é comprometida em proteger suas informações pessoais dos seus colaboradores. Isso indica que as organizações, na visão dos participantes, acabam não apresentando problemas com vazamentos de suas informações pessoais para outras organizações ou outras pessoas má intencionadas. Por outro lado, 13,3% afirmam que não sabem e 14,7% discordam que as empresas preservam seus dados pessoais.

Esse último dado indica que existem casos, ainda que possivelmente a minoria, nos quais as organizações não tratam adequadamente os dados que possuem sobre seus funcionários. Portanto, as empresas precisam melhorar suas práticas uma vez que são controladoras de dados pessoais e serão responsabilizadas em caso de vazamento ou roubo de informações.

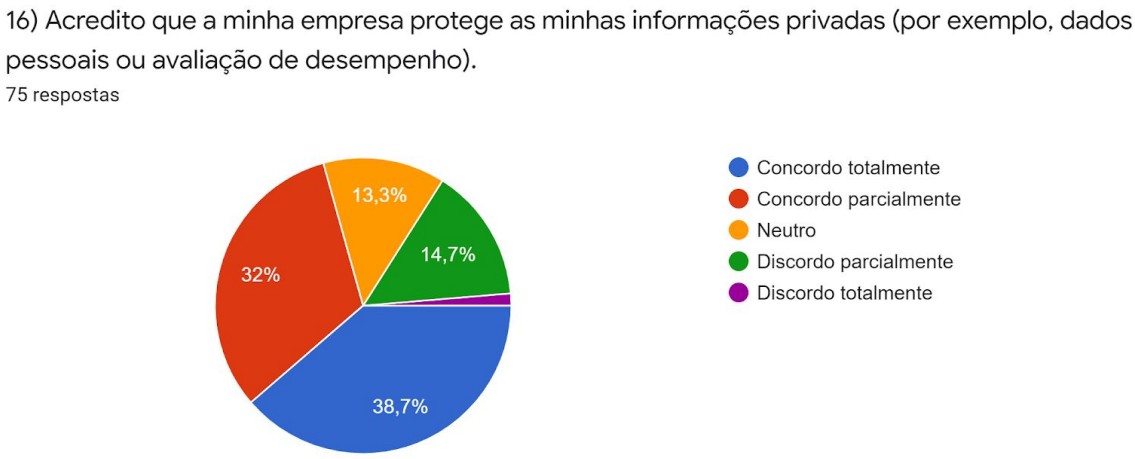

Figura 24 - Proteção de informações privadas.

4.9 Gestão de Mudança

Observa-se, na Figura 25, que cerca de 92% dos participantes aceitam mudanças de práticas que são solicitadas pela organização para ajudar a garantir a segurança da informação. Esse resultado indica que a maioria dos participantes está aberta para mudanças e para os procedimentos que a organização propor para que a segurança dos ativos seja alcançada.

Nesse contexto, a organização possui uma maior liberdade de implantar novas práticas que auxiliem na proteção dos ativos, sem a resistência de seus colaboradores. Em comparação com a Figura 20, o resultado se assemelha pelo fato de que, a grande maioria (84%) respondeu que era comprometido com a política de segurança da informação da empresa.

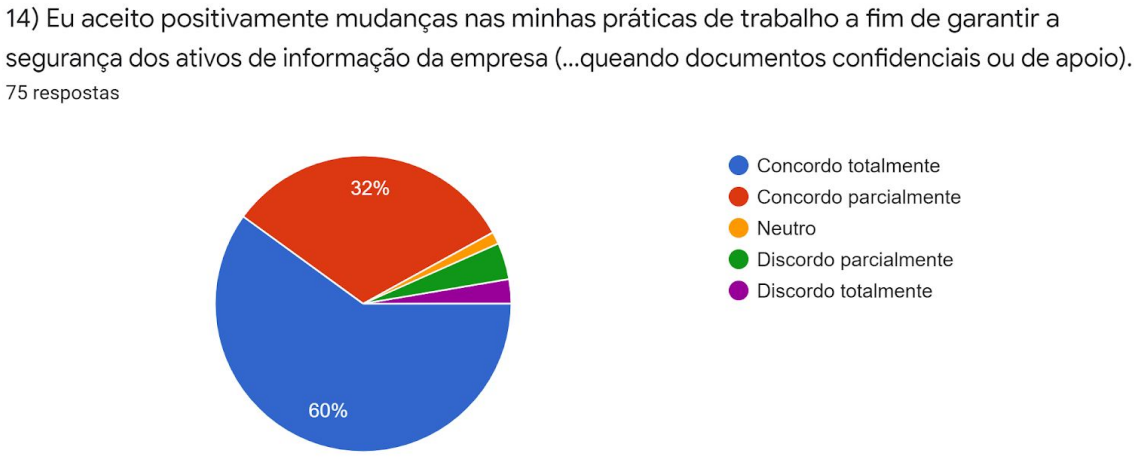

Figura 25 - Mudanças de práticas dos participantes pela organização.

4.10 Treinamento e Conscientização

Na Figura 26 é possível observar que a grande maioria, cerca de 89,3% acredita que é necessário haver treinamentos sobre segurança da informação, e assim, para ajudar a proteger as informações tratadas pela organização. Essa percepção da necessidade de treinamentos indica que há uma carência por parte das empresas de tratarem de forma adequada essa área, além de aumentarem os riscos de sofrerem algum tipo de ataque e estarem mais vulneráveis.

Figura 26 - Necessidade de treinamentos dos participantes.

Observa-se, na Figura 27, que 84% dos participantes acreditam que treinamentos, campanhas e cursos de capacitação para segurança da informação são eficazes. Isso pode indicar que a maioria dos participantes acredita que realizar essas ações possuem efeito positivo possivelmente devido a experiências passadas.

Entretanto, apesar dos participantes acreditarem que é necessário investir em capacitações e que estas proporcionam efeitos positivos em relação a segurança da informação, no levantamento do perfil dos participantes, observou-se que apenas 40% dos participantes afirmaram ter participado de algum treinamento ou capacitação como ilustrado na Figura 9. Estes dados reforçam a carência de treinamento e a necessidade de realizá-los por parte das empresas. .

Figura 27 - Eficiência de treinamentos.

4.11 Percepção de Privacidade

Observa-se na Figura 28 que 90,7% dos participantes concordam que as atividades da empresa devem abordar a privacidade na fase de planejamento. Este resultado pode indicar que os respondentes estão abertos a utilizar as práticas necessárias para manter a privacidade desde o começo dos projetos desenvolvidos pelas empresas.

Figura 28 - Privacidade nas atividades da organização.

Na Figura 29, observa-se que cerca de 88% dos participantes, sendo que 72% totalmente, concordam que deve existir uma limitação na coleta e compartilhamento de informações pessoais sensíveis. É possível inferir desses dados que os participantes não se sentem confortáveis em ter seus dados pessoais coletados e divulgados com terceiros. Com a LGPD em vigor e com as empresas se adequando aos requisitos da lei, é possível que os participantes se sintam mais confortáveis pelo fato da lei garantir acesso aos seus dados armazenados pelas

organizações, além de poder deletá-los e ter controle deles a qualquer momento (BRASIL, 2020).

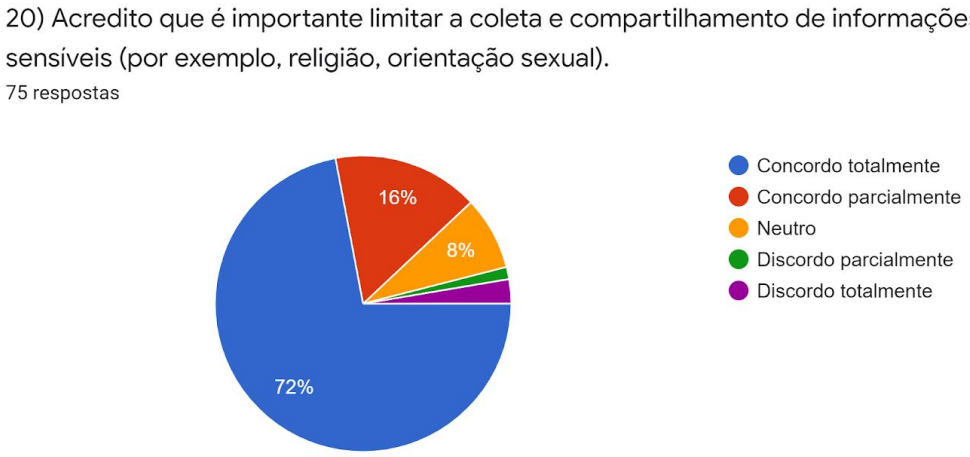

Figura 29 - Limitação de coleta de informações.

4.12 Discussão

Nesta seção é apresentada uma discussão sobre os resultados obtidos. Por meio de uma análise dos das respostas obtidas, é possível inferir conclusões por meio do cruzamento dos dados coletados.

4.12.1 Perfil de instituição

De modo geral, os participantes da pesquisa atuam em instituições de três diferentes domínios: Privado, Público e Jurídico. Foram obtidas 49 respostas de colaboradores do setor Privado, 25 respostas do setor público e 1 resposta do setor Jurídico. Analisando o tipo de instituição, foi possível observar alguns padrões:

- **Tempo de atuação na organização:** A maioria dos participantes de instituições privadas trabalham em suas respectivas organizações no período de 1 a 5 anos (65,3%). Nas empresas de domínio público, 48% atuam entre 1 a 5 anos. O respondente do setor Jurídico afirmou atuar entre 1 a 5 anos na organização. Isso indica que as respostas foram de pessoas com mesma faixa de experiência, porém com pouco tempo de atuação. Os resultados podem ser observados na Figura 30.

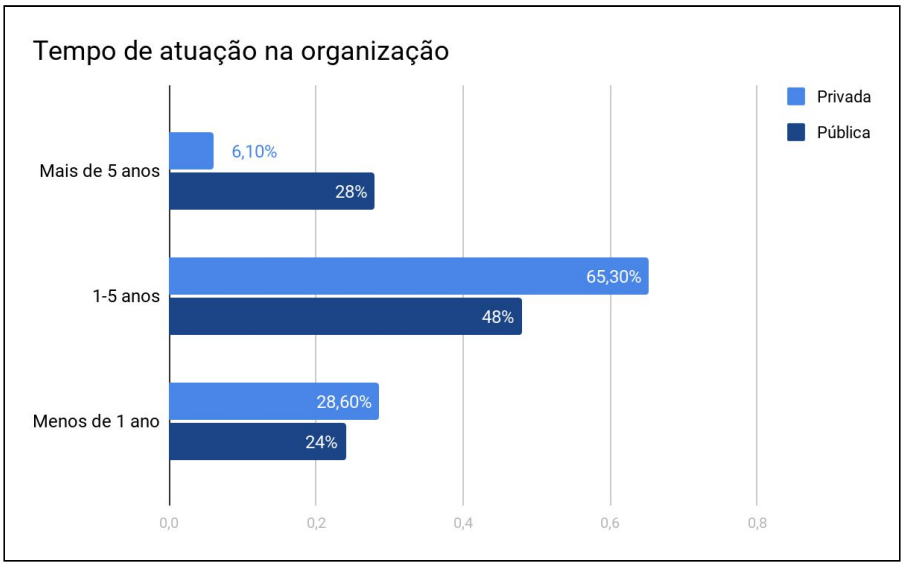

Figura 30 - Tempo de atuação dos participantes nas organizações.

- **Participação em treinamentos:** Nas respostas dos participantes do setor Privado, a maioria (59,2%) afirmou que nunca havia participado de treinamentos ou capacitações sobre segurança da informação. Já no setor Público a resposta foi semelhante, na qual 60% dos participantes afirmaram nunca ter participado de nenhum treinamento ou capacitação como visto na Figura 31. O respondente do setor Jurídico afirmou que também nunca participou de treinamentos ou capacitações. Esses dados podem sugerir que o domínio da organização não influencia na capacitação dos colaboradores e que existe a necessidade de mais treinamentos e capacitações nas organizações.

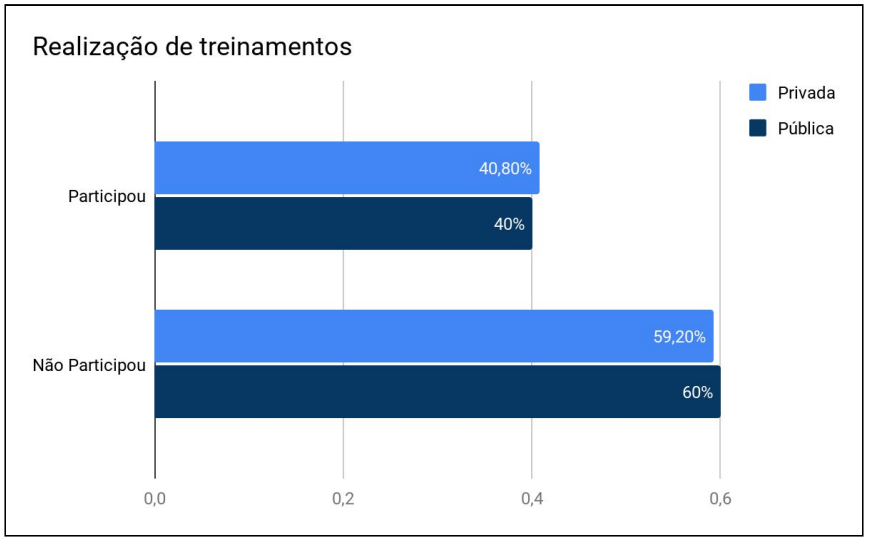

Figura 31 - Realização de Treinamentos e Capacitações.

- **Tratamento de informações sigilosas:** Como observado na Figura 32, dos respondentes do setor Privado, a maioria (77,6%) afirmou que trabalhou ou

trabalha com informações consideradas sigilosas. Já no setor Público, esse percentual é pouco menos da metade (48%). Já o respondente do setor Jurídico afirmou ter trabalhado com informações sigilosas. Esses resultados sugerem que a maioria dos participantes da pesquisa do setor Privado possuem uma experiência maior em lidar com informações sigilosas.

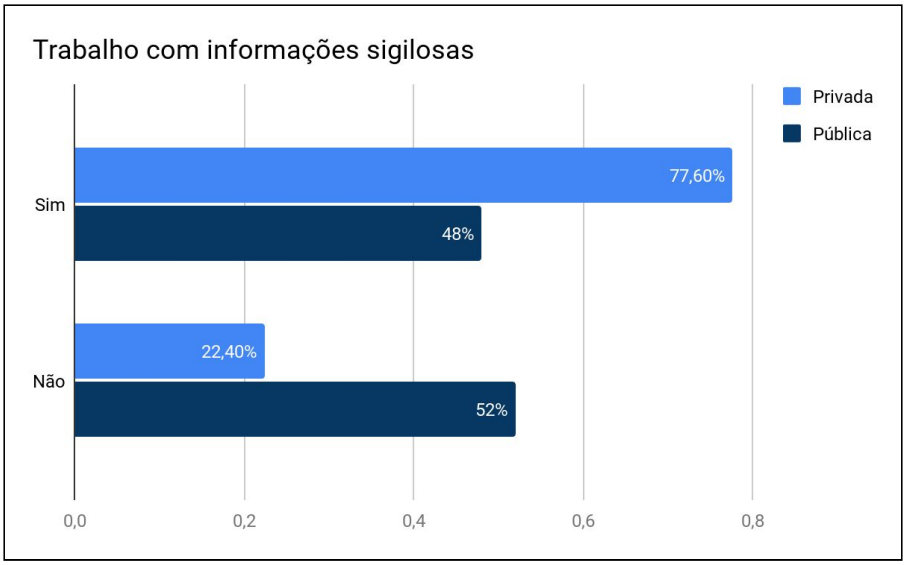

Figura 32 - Trabalho com informações sigilosas por parte dos participantes.

- **Entendimento sobre Engenharia Social:** Do total de respostas, foi possível observar que 22,6% dos participantes demonstraram que não entendem de forma clara qual a definição de Engenharia Social. Como base nesses 22,6%, a maioria das respostas foram de colaboradores do setor Privado com 10 respostas (58,8%). Logo em seguida, o setor Público com 6 respostas (35,3%), e por fim a resposta do setor Jurídico (5,9%), como pode ser observado na Figura 33. Dessa forma, obteve-se indícios que os participantes do setor Privado tem um entendimento menor sobre a definição de Engenharia Social. Esse fato pode resultar em uma vulnerabilidade maior, comparado aos participantes do setor Público.

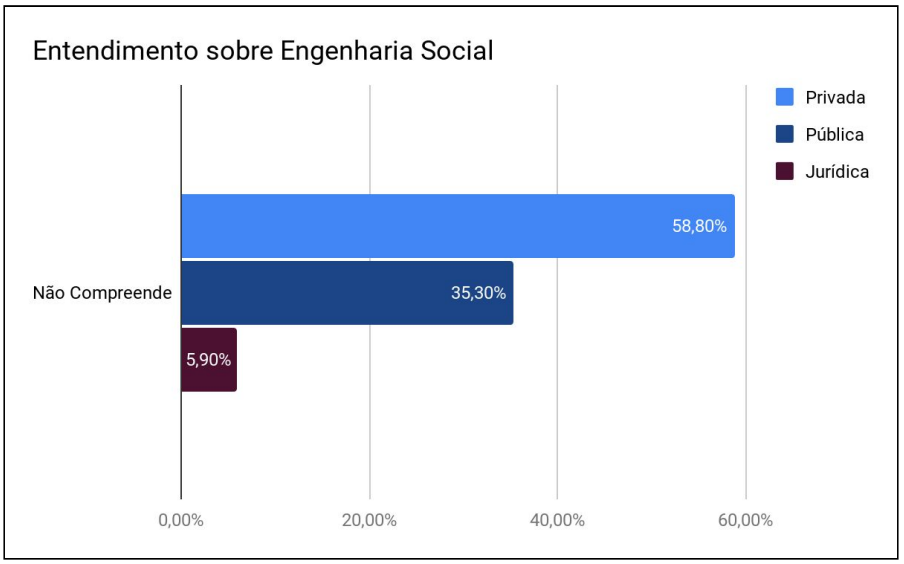

Figura 33 - Entendimento sobre a definição de Engenharia Social pelos participantes.

- **Clareza da organização sobre a segurança da informação:** Na Figura 34, foi possível observar que a maioria dos respondentes que atuam no setor Privado (85,7%) possuem conhecimento dos procedimentos que a empresa espera deles em relação a segurança da informação. Diferentemente, no setor Público, 44% possuem conhecimento sobre segurança da informação repassado e esperado pela organização. Sendo assim, é possível concluir que as instituições de domínio Privado possuem uma maior preocupação e clareza sobre a segurança da informação da organização.

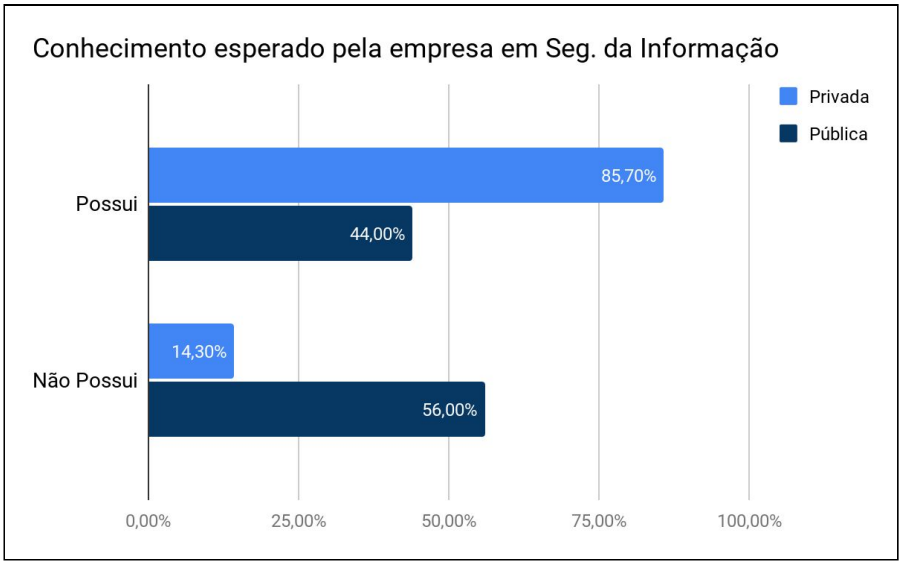

Figura 34 - Conhecimento de Segurança da Informação esperado pela empresa dos participantes.

4.12.2 Porte da Organização

Os participantes da pesquisa atuam em instituições de quatro diferentes portes: Microempresa (até 9 empregados), Pequeno (10 a 49 empregados), Médio

(50 a 99 empregados) e Grande (A partir de 100 empregados). Foram obtidas 56 respostas, representando a maioria, de colaboradores de organizações do porte Grande, 6 respostas do porte Médio, 6 respostas do porte Pequeno e 7 respostas do porte microempresa. De modo geral, é possível observar alguns padrões analisando pela ótica desse perfil:

- **Participação em treinamentos:** Do total de respostas, 45 dos respondentes afirmaram nunca ter realizado nenhum tipo de treinamento ou capacitação sobre segurança da informação. Especificamente as respostas dos participantes das empresas de grande porte, cerca de 53,6% responderam que nunca fizeram treinamento. Já os resultados das empresas de médio porte, todos os respondentes afirmaram nunca ter feito treinamento ou capacitação em segurança da informação. Nas respostas de empresas de pequeno porte, cerca de 50% afirmaram ter feito algum treinamento ou capacitação. Por último, nas microempresas, cerca de 85,7% responderam que nunca fizeram nenhum tipo de capacitação como observado na Figura 35. Com isso, é possível observar que os participantes de empresas de pequeno e grande porte demonstraram resultados próximos e apresentaram estar mais capacitados sobre segurança da informação comparados aos respondentes de organizações de portes médio e microempresas, que, por sua vez, precisam de urgentes capacitações em segurança da informação. Mesmo com resultados melhores, os participantes de empresas de grande e pequeno porte também precisam de melhores capacitações para evitarem futuras possíveis incidentes com informações em suas organizações.

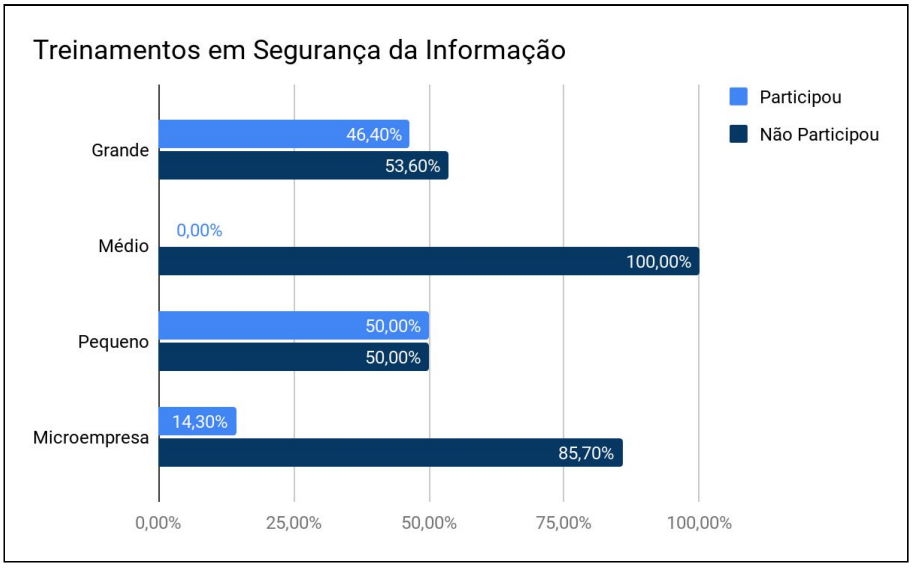

Figura 35 - Treinamentos e capacitações em Segurança da Informação.

- **Entendimento sobre Engenharia Social:** Dos participantes de instituições de grande porte 16,1% demonstraram que não compreendem de forma clara o que significa a Engenharia Social. Já, próximo ao dobro do resultado

anterior, os respondentes de organizações de médio porte, foi observado que 33,4% não entendem de forma clara o termo Engenharia Social. Logo em seguida, os participantes de microempresas apresentaram o maior índice de respostas neutras sobre o tema com 42,9%, seguidos de 28,6% de discordância com a definição da Engenharia Social. Por fim, apenas 16,7% dos respondentes de pequenas empresas demonstraram não ter opinião sobre a definição de Engenharia Social, como observado na Figura 36. Isso pode indicar, por exemplo, que os participantes da pesquisa de micro empresas podem estar com uma maior vulnerabilidade a ataques quando comparados aos outros respondentes de organizações de outros portes, por não terem clareza quanto à Engenharia Social;

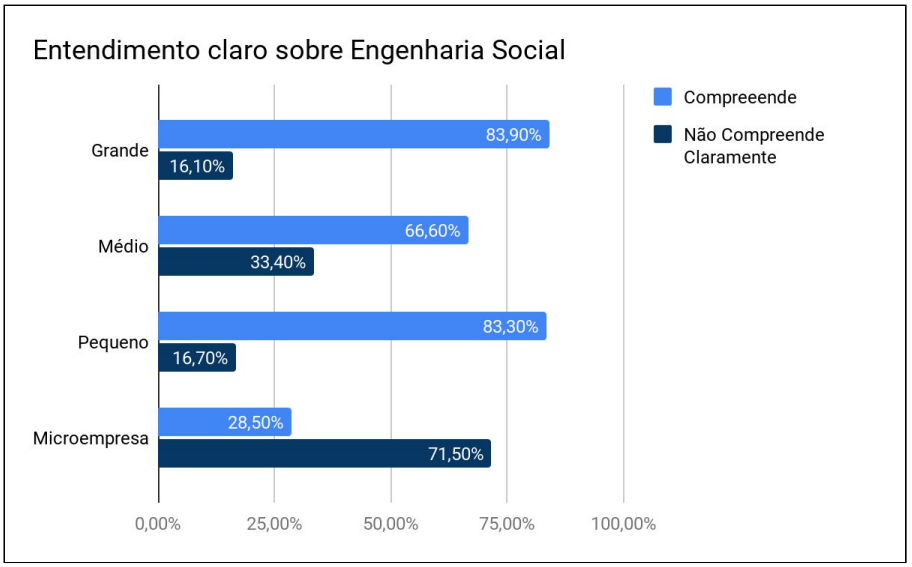

Figura 36 - Compreensão clara da definição de Engenharia Social.

- **Entendimento sobre a Política de Segurança da Informação:** É apresentado na Figura 37, que entre os respondentes de organizações de grande porte, cerca de 25% afirmaram não ter conhecimento sobre a política de segurança da informação de suas respectivas organizações. Nas respostas dos participantes de médio porte, cerca de 50% afirmou também não ter conhecimento sobre a política da organização. Já nas respostas dos participantes de microempresas, a grande maioria, cerca de 71,4% não tem ciência sobre a política de segurança da informação de suas organizações. E por fim, os respondentes de pequenas empresas, 50% afirmou não ter conhecimento sobre a política de segurança da informação de suas empresas. Com isso, pode ser observado que de maneira geral, os participantes de organizações de menor porte (Microempresa, Pequena e Média) possuem maior carência quanto a informações sobre a política de segurança da informação de suas respectivas organizações. Consequentemente, as chances de ocorrerem incidentes nessa empresas de

menor porte é bem maior, por conta do fator humano que é um dos maiores motivos de incidentes com informações (DA VEIGA e MARTINS, 2015).

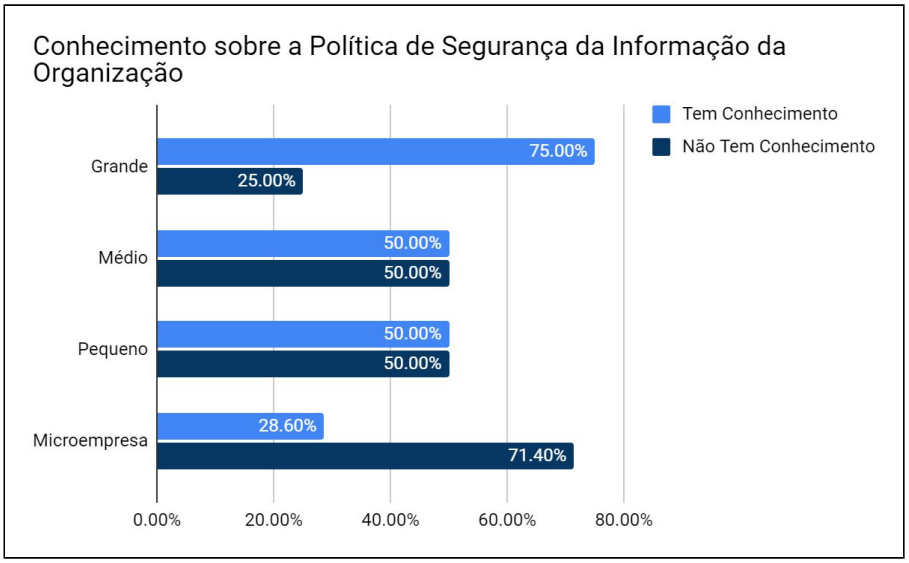

Figura 37 - Conhecimento da Política de Segurança da Informação.

4.12.3 Perfil de Tempo de Atuação

Os participantes possuem períodos distintos de atuação dentro das organizações que foram distribuídos nos intervalos de: Menos de 1 ano (20 respostas), De 1 a 5 anos (45 respostas), De 6 a 10 anos (4 respostas), De 11 a 15 anos (1 resposta), De 16 a 20 anos (1 resposta) e Mais de 20 anos (4 respostas). Dada essas circunstâncias, alguns padrões podem ser observados:

- **Participação em treinamentos:** Dos participantes com menos de 1 ano na organização, 70% não participaram de nenhum treinamento ou capacitação em segurança da informação. Os participantes com mais de 20 anos de atuação na organização em sua totalidade afirmaram já ter passado por algum treinamento ou capacitação, como visto na Figura 38. Com isso, é possível identificar que os participantes com até 5 anos de atuação nas organizações apresentaram um grau menor de treinamentos realizados sobre segurança da informação, seja oferecido pela organização ou por conta própria.

  Quando comparado com os participantes mais experientes em que todos afirmaram já ter passado por treinamentos (De 11 a 15 anos e Mais de 20 anos). É necessário que esses profissionais mais novos procurem por treinamentos e capacitações ou que a organização os proporcione, para que o conhecimento sobre segurança da informação desses colaboradores seja fortalecido para assim evitar futuros incidentes.

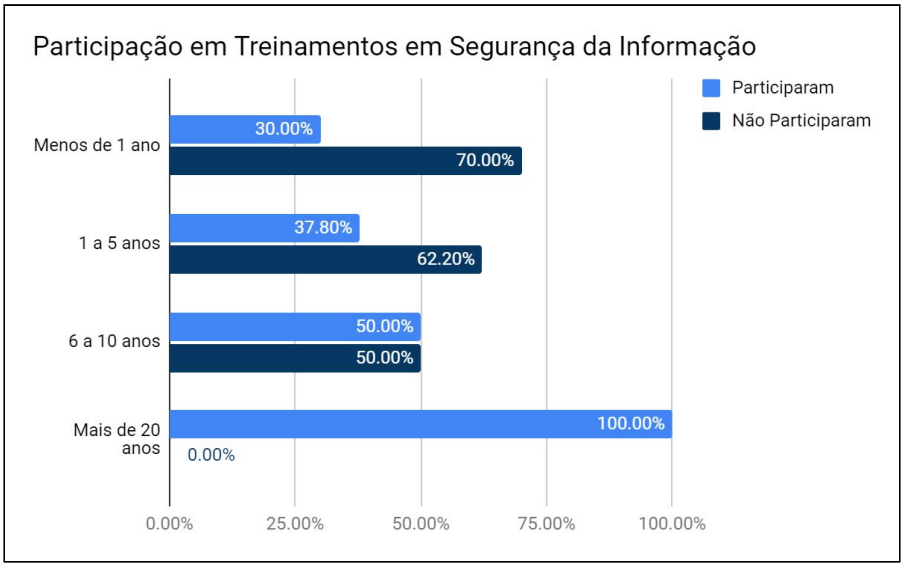

Figura 38 - Participação em Treinamentos e capacitações em Segurança da Informação.

- **Entendimento sobre a Política de Segurança da Informação:** Na Figura 39, dos respondentes com menos de 1 ano de atuação na organização, 35% afirmaram não ter conhecimento sobre a política de segurança da informação. Semelhante a esse valor, os participantes de 1 a 5 anos apresentaram um resultado similar com 37,8% sem conhecimento sobre a política. Em contrapartida, os participantes mais antigos nas organizações (Mais de 5 anos) 20% afirmou não conhecer a política de segurança da informação de suas respectivas organizações. Além disso, 60% ,desses profissionais mais antigos, afirmaram que a política de suas organizações é moderadamente difícil de ser entendida. É possível inferir com isso que, profissionais com menos tempo de atuação na organização conhecem menos a política de segurança da informação de suas organizações, mesmo os empregados mais antigos, ainda possuem um certo nível de dificuldade de compreensão da política. De certa forma, esse resultado pode ser considerado prejudicial para as organizações seria importante que as empresas mostrassem de forma mais clara para seus colaboradores para a execução das ações conforme a política da organização.

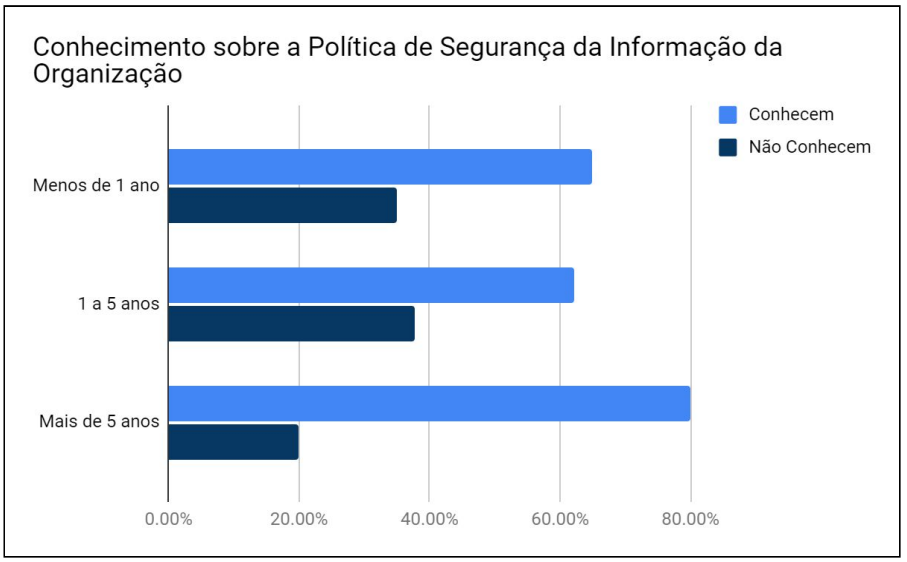

Figura 39 - Conhecimento dos participantes sobre a Política de Segurança da Informação.

4.12.4 Perfil de Segmento da Organização

Os participantes dessa pesquisa se originam de empresas de 15 diferentes segmentos de atuação, são eles: Educação, Informática, Saúde, Judiciário, Religioso, Varejo e atacadista, Distribuição, Aviação, Comércio Marketing, Funerária, Governamental, Industrial, Engenharia e Clima, Telecomunicações e Tecnologias. Dentre as respostas foram obtidas uma quantidade maior dos segmentos Informática (33 respostas) e Educação (21 respostas), os outros segmentos receberam números de respostas mais abaixo comparados a estes (de 1 a 4 respostas). Considerando esses perfis de segmentos dos participantes com um número maior de respostas foi possível perceber algumas características:

- **Participação em treinamentos:** Foi possível observar na Figura 40, que dos participantes do segmento de Informática e Educação, a maioria dos participantes nunca participou de treinamentos ou capacitações em segurança da informação. Sendo os participantes do segmento Informática 60,6% e o segmento Educação 76,2%, ou seja, um pouco a mais comparado a Informática. Isso indica que os participantes desses segmentos precisam de mais treinamentos para fortalecer a cultura de segurança da informação e assim, reduzir potenciais riscos que as organizações possam ser submetidas.

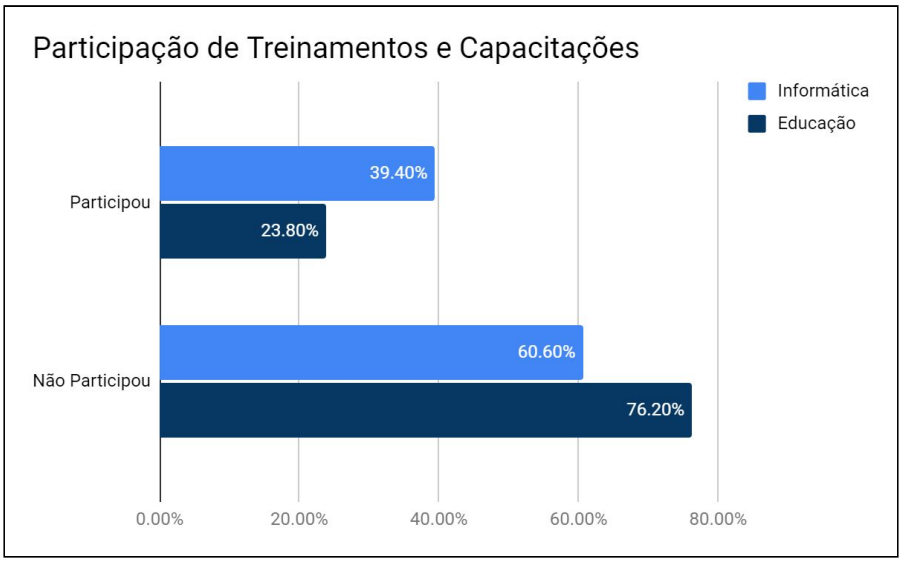

Figura 40 - Participação de treinamentos e capacitações dos respondentes.

- **Entendimento sobre a Política de Segurança da Informação:** Dos participantes que atuam em empresas do segmento de Informática, foi observado que cerca de 18,2% não tem conhecimento sobre a política de segurança da informação de suas organizações. Já os participantes do segmento de Educação, cerca de 42,9% afirmaram também conhecer sobre a política de sua empresa, como pode ser visto na Figura 41. Com isso, é possível destacar que os respondentes do segmento de Educação possuem bem menos conhecimento sobre a política de suas organizações, quando comparados aos participantes do segmento de Informática. Consequentemente possuem uma cultura de segurança da informação mais forte e estão com menos riscos de serem submetidos a incidentes, pelo menos considerando a ótica do conhecimento dos empregados.

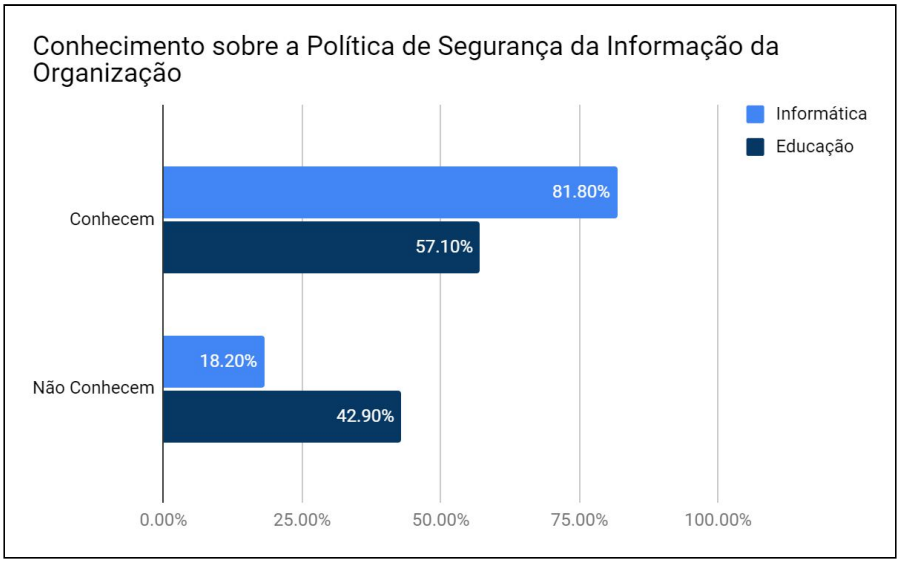

Figura 41 - Conhecimento sobre a Política de Segurança da Informação.

4.12.5 Comparando Dimensões

Os participantes desta pesquisa foram agrupados de acordo com alguns resultados que se destacaram, e assim foi realizado o cruzamento com outras respostas. Considerando isso, foi possível observar algumas características:

- **Conhecimento da Política e Engajamento:** Dos participantes que possuem maior facilidade de compreensão da política de suas organizações, percebe-se que 72,2%, a grande maioria, concorda que as suas respectivas organizações promovem engajamento em segurança da informação (Figura 42). Já para aqueles que não possuem conhecimento da política, foi possível notar que as organizações em que eles estão inseridos, em sua maioria, não promovem engajamento em segurança da informação, com cerca de 56,5% das respostas discordando da existência de engajamento. Isso pode demonstrar que aqueles que não possuem conhecimento sobre a política de segurança da informação, em sua maioria, pode ser por conta da falta de engajamento da organização quanto a segurança da informação com seus colaboradores.

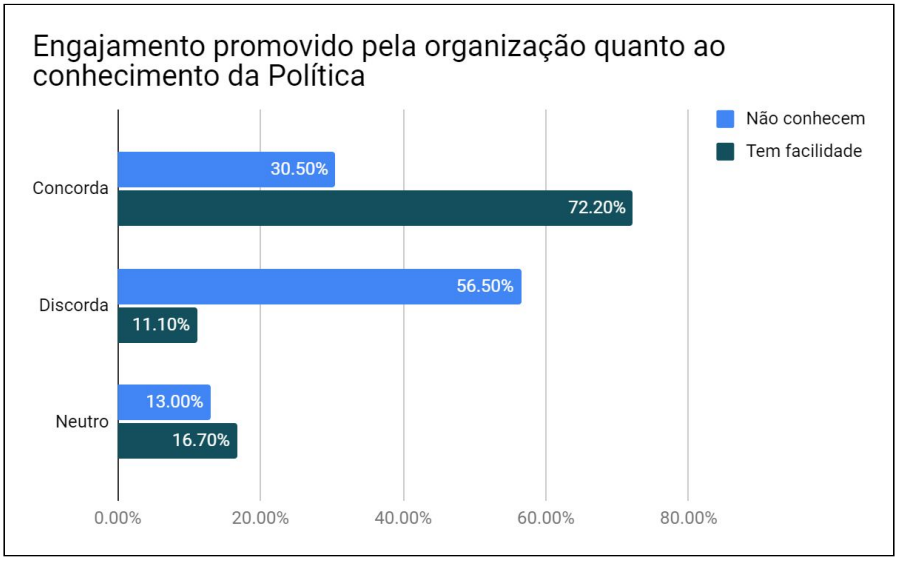

Figura 42 - Conhecimento sobre a Política de Segurança da Informação ligado ao engajamento promovido pelas organizações.

- **Definição quanto a Segurança da Informação e a Proteção de Ativos Físicos:** Do total de participantes, existe uma parcela que afirma acreditar que a organização define o que é esperado em Segurança da Informação de seus funcionários. Assim, cerca de 90,7%, concorda que suas respectivas organizações se empenham para proteger seus ativos físicos da informação (Figura 43). Já no grupo que não possui uma definição clara, foi possível observar que há uma percepção menor do grau de proteção de ativos físicos

se comparado à parcela anterior. Isso demonstra que as organizações que apresentam para seus colaboradores de forma clara e objetiva o comportamento que espera deles quanto a segurança da informação possui uma proteção aos ativos da informação mais adequada.

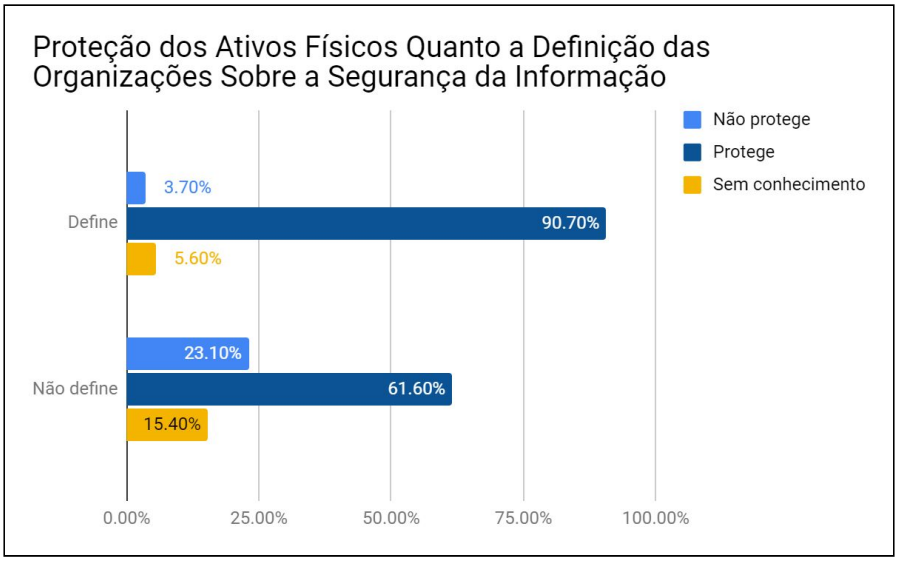

Figura 43 - Definição do que é esperado quanto a Segurança da Informação e a proteção de ativos físicos.

4.12.6 Recomendações

Como resultado da análise das respostas foi possível verificar alguns pontos de melhoria que as organizações, bem como os próprios participantes podem aprimorar as ações relacionadas à cultura da segurança da informação. Com isso, o objetivo dessa seção é apresentar algumas recomendações que podem auxiliar na melhoria de alguns pontos observados para a Cultura de Segurança da Informação.

- **Melhor Definição das Políticas de Segurança da Informação:** As organizações podem definir melhor suas Políticas de Segurança da Informação e apresentar as consequências da sua ausência para os colaboradores;

- **Melhorar a Divulgação das Políticas de Segurança da Informação:** Utilizar de divulgação constante da Política de Segurança da Informação das organizações e de outros aspectos da Segurança da Informação para os colaboradores para incentivá-los a se integrar com a temática;

- **Melhorar o entendimento dos funcionários com a Segurança da Informação**: As organizações podem promover treinamentos e capacitações para seus funcionários, além de incentivar palestras e outras iniciativas para demonstrar a importância de manter as informações seguras;

- **Reavaliar as Informações:** Reavaliar quais informações pessoais dos colaboradores são realmente necessárias de ser armazenadas. Muitas vezes algumas informações além de causar desconfortos aos colaboradores, também podem ser abstraídas nas coletas que as organizações fazem;

- **Definir a Responsabilidade quanto a Segurança:** As organizações devem apontar a segurança das informações é dever de todos os colaboradores e não só do departamento de Tecnologia da informação. Mostrar que esse dever é basicamente de todos por meio de iniciativas de sensibilização, como campanhas.

5. Conclusões e Trabalhos Futuros

O fator humano é um dos principais motivos pela qual ocorrem incidentes envolvendo informações nas organizações (DA VEIGA e MARTINS, 2015). Sendo assim, para auxiliar na redução dos riscos com vazamentos e roubo de informações, as empresas precisam melhorar a cultura de segurança da informação. Com uma cultura forte e disseminada é possível evitar futuros prejuízos financeiros e perda de reputação causados pelos incidentes relacionados à segurança da informação.

Este trabalho contribui nessa direção ao conduzir um *survey* sobre a cultura da segurança da informação nas organizações. As principais conclusões deste trabalho são apresentadas a seguir.

5.1. Conclusões

- **Perfil dos participantes.** A pesquisa teve a participação de profissionais de variados segmentos, períodos de atuação, domínios diferentes (Empresas Públicas e Privadas), Titulações, entre outros. Com isso, foi praticável obter respostas do mais variados cenários de empresa e funcionários. Foi possível observar que, de maneira geral, os participantes conseguiram demonstrar um bom conhecimento sobre a segurança da informação, porém, campanhas de conscientização e sensibilização devem ser realizadas pelas organizações. Um dos pontos que apresentam vulnerabilidades é a política de Segurança da Informação no qual uma parcela consideravelmente grande de participantes que não a conhecem ou possuem dificuldades em entendê-la.

- **Necessidade de treinamentos em Segurança da Informação.** A maioria dos participantes respondeu que nunca realizou um treinamento em segurança da informação e afirmaram precisar de treinamentos. Isso afeta diretamente a segurança das organizações, pois revela uma cultura de segurança da informação deficiente pelo fato dos colaboradores não serem bem capacitados. Além disso, a probabilidade de ocorrer incidentes com as

informações dessas organizações é bem maior do que as organizações que investem em capacitações.

- **Trabalho com informações sigilosas.** Foi possível concluir que os participantes do setor privado tiveram bem mais contato com informações consideradas sigilosas. Dessa forma, o setor público tem uma experiência menor e, possivelmente, está mais vulnerável que o setor privado.

- **Conhecimento sobre a Política de Segurança da Informação.** O segmento de Informática possui o conhecimento mais elevado comparado ao segmento de Educação que foi o segundo que mais obteve respostas. É possível concluir que existe uma maior probabilidade de que a maioria dos participantes da área de educação estejam mais expostos a riscos por não conhecerem quais as práticas da organização são necessárias para manter a segurança dos ativos da organização, por exemplo.

- **Grande aceitação de mudanças.** Foi possível observar que a maioria dos participantes está aberta a mudanças de comportamento no ambiente de trabalho para auxiliar na segurança dos ativos da informação das organizações.

5.2 Contribuições

Este trabalho proporcionou um entendimento do estado atual da cultura de segurança da informação nas organizações. Sendo assim, as principais contribuições deste trabalho são:

(i) Investigação de métodos de avaliação de cultura de segurança da informação nas organizações: Na Seção 1.4 são discutidos questionários existentes na literatura para realizar a avaliação de cultura de segurança da informação. Na Tabela 4 é apresentado uma comparação de áreas avaliadas neste tipo de avaliação;

(ii) Elaboração de um instrumento para avaliar a cultura de segurança da informação: o questionário aplicado nesta pesquisa contempla as dimensões relacionadas à cultura de segurança da informação propostas por Martins, Da Veiga e Eloff (2007) que é um dos trabalhos mais utilizados para avaliar a cultura nesta temática;

(iii) Aplicação do instrumento para coletar resultados e fazer uma avaliação: o questionário ficou disponível por três meses e foi divulgado em diversos meios como email, redes sociais e grupos de sistemas de informação;

(iv) Caracterização da cultura de segurança da informação a partir dos resultados obtidos no *survey*: observou-se que existe uma necessidade de capacitações dos funcionários sobre segurança da informação. Também existe incongruência entre conhecer, compreender e aplicar os procedimentos descritos na

política de segurança de informação, além de que as organizações precisam promover mais o engajamento da segurança da informação com os seus colaboradores.

5.3 Trabalhos Futuros

Este trabalho gerou algumas direções de pesquisas futuras que podem ser exploradas:

(i) ampliar a pesquisa para que sejam obtidas mais respostas, e desse modo, conseguir fazer uma avaliação com cenários maiores;

(ii) realizar entrevistas com funcionários de empresas de diversos segmentos para caracterizar com mais detalhes os aspectos relacionados a cultura de segurança da informação;

(iii) aplicar o questionário completo do ISCA em organizações previamente selecionadas;

(iv) fazer um comparativo de resultados ao decorrer dos anos, como proposto pelo ISCA, para avaliar a melhoria das organizações quanto ao nível da cultura segurança da informação;

(v) fazer um estudo de caso em uma organização para conseguir ter um parecer da cultura de forma mais ampla e segura;

(vi) realizar um estudo comparativo das práticas presentes nas políticas de segurança da informação de organizações selecionadas.

REFERÊNCIAS

[1] GOODRICH, Michael T.; TAMASSIA, Roberto. **Introduction to computer security**. Pearson, 2011. page.12

[2] HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. Brasport, 2018. page.19, page.27

[3] WHITMAN, Michael E.; MATTORD, Herbert J. **Principles of information security**. Cengage Learning, 2011.

[4] DA VEIGA, Adéle; MARTINS, Nico. Information security culture and information protection culture: A validated assessment instrument. **Computer law & security review**, v. 31, n. 2, p. 243-256, 2015.

[5] DA VEIGA, Adéle; ELOFF, Jan HP. A framework and assessment instrument for information security culture. **Computers & Security**, v. 29, n. 2, p. 196-207, 2010.

[6] VAN NIEKERK, J. F.; VON SOLMS, Rossouw. Information security culture: A management perspective. **Computers & security**, v. 29, n. 4, p. 476-486, 2010.

[7] Veiga, Adéle & Eloff, Jan. (2002). **Information Security Culture. IFIP TC11, 17th international conference on information security (SEC2002)**. 203-214. 10.1007/978-0-387-35586-3_16.

[8] **Cambridge** international **dictionary** of **English**. (2020). **Cambridge**: **Cambridge** University Press.

[9] HUMANOS, DECLARAÇÃO UNIVERSAL DOS DIREITOS. Declaração Universal dos Direitos Humanos. **Acesso em**, v. 13, 2015.

[10] VIANNA, Túlio. **Transparência pública, opacidade privada**. Rio de Janeiro: Revan, 2007. ISBN 978-85-7106-360-0.

[11] SWIRE, Peter P.; BERMANN, Sol (Ed.). **Information Privacy: Official Reference for the Certified Information Privacy Professional (CIPP)**. International Association of Privacy Professionals, 2007.

[12] FONSECA, Marcelo. Engenharia social: conscientizando o elo mais fraco da segurança da informação. **Inteligência de Segurança-Unisul Virtual**, 2017.

[13] SILVA, Francisco José Albino Faria Castro e. **Classificação Taxonómica dos Ataques de Engenharia Social. Caracterização da Problemática da Segurança de Informação em Portugal relativamente à Engenharia Social.** 2013. 132 p. Dissertação (Segurança dos Sistemas de Informação).

[14] CHANTLER, Alan N..; BROADHURST, Roderic. **Social Engineering and Crime Prevention in Cyberspace**. Draft Technical Report for the Australian Institute of Criminology - Futures of High Tech Crime Project. 2006.

[15] MITNICK, Kevin D.; SIMON, William L. **A arte de enganar.** São Paulo, 2003.

[16] HADNAGY, Christopher. **The Social Engineering Framework - Attack Vectors**. 2017.

[17] ROBBINS, Stephen P.; SOBRAL, Filipe. **Comportamento organizacional.** 14. ed. São Paulo: Prentice-Halll, 2012. page.501

[18] DEAL, Terrence E.; KENNEDY, Allen A. **Corporate cultures: The rites and rituals of corporate life.** Readin: Addison-Wesley, 1982.

[19] SCHEIN, Edgar H. **Organizational culture and leadership**. 2. ed. San Francisco: Jossey-Bass, 1992.

[20] Herold R. Managing an information security and privacy awareness and training program. Boca Raton: Taylor and Francis Group; 2011.

[21] Johnson ME, Goetz E. Embedding information security into the organization. IEEE Secur Priv 2007;5:16e24.

[22] PwC, PricewaterhouseCoopers. **The global state of information security survey.** 2014. Available from: http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml [accessed 20.02.14].

[23] HENRIQUES, Francisco de Assis Fialho. **A influência da Engenharia Social no fator humano das organizações**. 2017. Dissertação de Mestrado. Universidade Federal de Pernambuco.

[24] ALLEN, Malcolm. **Social Engineering: A Means To Violate A Computer System.** 2007. Disponível em: <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529>. Acesso em: 17/01/2017.

[25] MARTINS, Adéle; ELOFF, Jan. Information security culture. In: **Security in the information society**. Springer, Boston, MA, 2002b. p. 203-214.

[26] SCHLIENGER, Thomas; TEUFEL, Stephanie. Information security culture-from analysis to change. **South African Computer Journal**, v. 2003, n. 31, p. 46-52, 2003.

[27] MACHADO, Rodrigo et al. Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteçao de Dados. In: **Anais da XVII Escola Regional de Redes de Computadores**. SBC, 2019. p. 154-159.

[28] Security, H. N. (2018). 2018 in numbers: Data breaches cost $654 billion, expose 2.8
billion data records in the U.S. http://bit.do/e25NV.

[29] FONTES, Edison Luiz Gonçalves. **Segurança da informação**. Saraiva Educação SA, 2017.

[30] Data exfiltration study: Actors, tactics, and detection. 2017. Available at: https://www.mcafee.com/us/resources/reports/rp-data-exfiltration.pdf.(Accessed March 1, 2017).

[31] ALHOGAIL, Areej; MIRZA, Abdulrahman. A proposal of an organizational information security culture framework. In: **Proceedings of International Conference on Information, Communication Technology and System (ICTS) 2014**. IEEE, 2014. p. 243-250.

[32] AL-MAYAHI, Ibrahim; SA'AD, P. Mansoor. Information security culture assessment: Case study. In: **2013 IEEE Third International Conference on Information Science and Technology (ICIST)**. IEEE, 2013. p. 789-792.

[33] PARSONS, Kathryn et al. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. **Computers & Security**, v. 66, p. 40-51,. 2017

[34] MARTINS, N.; DA VEIGA, A.; ELOFF, Jan HP. Information security culture-validation of an assessment instrument. **Southern African Business Review**, v. 11, n. 1, p. 147-166, 2007.

[35] BAUER, CÉSAR ADRIANO. Política de segurança da informação para redes corporativas. **Monografia**, 2006.

[36] SÊMOLA, Marcos. **Gestão da segurança da informação**. Elsevier Brasil, 2014.

[37] McAfee (2017), Grand Theft Data: Data exfiltration study: Actors, tactics, and detection.
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-data-exfiltration.pdf

[38] PIRES, José Calixto de Souza; MACÊDO, Kátia Barbosa. Cultura organizacional em organizações públicas no Brasil. **Revista de Administração Pública**, v. 40, n. 1, p. 81-104, 2006.

[39] ARTEIRO, Iveruska Carmen Jatobá Bastos. **Como a cultura organizacional influencia iniciativas de gestão de processos de negócios: um estudo de caso exploratório**. 2015. Dissertação de Mestrado. Universidade Federal de Pernambuco.

[40] TOM, Jake. Assessing and Improving Compliance to Privacy Regulations in Business Processes.

[41] SCHEIN, E.1990. Organizacional Culture. Sloan Schoolof Management, Massachusetts Institute of Techonology.

[42] Payao, F. (2019). Dados de 1,4 milhao de clientes do Banco Inter estavam expostos para acesso. https://bit.ly/2LKotJR.

[43] Preta G. ,Schaeffer C. (2019). Vazamento expõe dados de 267 milhões de usuários do Facebook. https://bit.ly/3jRDnuP.

[44] Europeu, Parlamento (2016). Regulamento Geral sobre a Proteção de Dados. Jornal Oficial da União Europeia https://bit.ly/35aaWnU

[45] MAHFUTH, Amjad et al. A systematic literature review: Information security culture. In: **2017 International Conference on Research and Innovation in Information Systems (ICRIIS)**. IEEE, 2017. p. 1-6.

[46] BRASIL, Parlamento do (2020). Lei Geral de Proteção de Dados Pessoais (LGPD). https://bit.ly/2ZmHfMS

[47] SCHMIEDEL, T.;VOM BROCKE, J.;RECKER, J. 2013. Which cultural values matter to business process management?Results from a global delphi study. Business Process Management Journal, v.19, n.2. Emerald.

[48] MARTINS, Adéle; ELOFF, J. Assessing Information Security Culture. In: **ISSA**. 2002c. p. 1-14.

[49] VEGRO, Thamiris Cavazzani et al. Cultura organizacional de um hospital privado. **Revista Gaúcha de Enfermagem**, v. 37, n. 2, 2016.

[50] Ferreira MC, Assmar EML, Estol KMF, Helena MCCC, Cisne MCF. Desenvolvimento de um instrumento brasileiro para avaliação da cultura organizacional. Estud Psicol. 2002 jul-dez;7(2):271-80

[51] LIŽBETINOVÁ, Lenka; LORINCOVÁ, Silvia; CAHA, Zdenek. The application of the organizational culture assessment instrument (OCAI) to logistics enterprises. **NAŠE MORE: znanstveno-stručni časopis za more i pomorstvo**, v. 63, n. 3 Special Issue, p. 170-176, 2016.

[52] Cameron, K. S., Quinn, R. E. Diagnosing and Changing Organizational Culture Based on the Competing Values Framework. Reading, Addison – Wesley, 221 p. ISBN 0201338718. 1999

[53] SANTOS, Sabina Mota. **Práticas de segurança da informação: um estudo de caso num centro hospitalar**. 2014. Tese de Doutorado. Instituto Politécnico do Porto. Instituto Superior de Contabilidade e Administração do Porto.

[54] DA VEIGA, Adéle. Comparing the information security culture of employees who had read the information security policy and those who had not. **Information & Computer Security**, 2016.

[55] LIM, Joo Soon et al. Embedding Information Security Culture Emerging Concerns and Challenges. In: **PACIS**. 2010. p. 43.

[56] YOON, Cheolho; HWANG, Jae-Won; KIM, Rosemary. Exploring factors that influence students' behaviors in information security. **Journal of information systems education**, v. 23, n. 4, p. 7, 2019.

[57] SILVA, Edna Lúcia Da.; MENEZES, Estera Muszkat. Metodologia da pesquisa e elaboração de dissertação. 2005. Disponível em: <https://projetos.inf.ufsc.br/arquivos/Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes_4ed.pdf>. Acesso em: 25/09/2016.

[58] GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. 6. ed. São Paulo: Atlas, 2008.

[59] KASUNIC, Mark. **Designing an effective survey**. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, 2005.

[60] CERVO, Amado Luiz.; BERVIAN, Pedro Alcino. Metodologia científica. . 5. ed. [S.l.]: Prentice Hall, 2002.

[61] Adéle Da Veiga, (2018) "An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture", Information & Computer Security, Vol.26 Issue: 5, pp.584-612, https://doi.org/10.1108/ICS-08-2017-0056

[62] ALVES, Leonardo Lacerda. Problema de pesquisa não é o problema – TCC o q? 2015.
Disponível em:
<http://lacerda.eti.br/2015/02/problema-de-pesquisa-nao-e-o-problema-tcc-o-q/>.

[63] NASIR, Akhyari et al. An analysis on the dimensions of information security culture concept: A review. **Journal of information security and applications**, v. 44, p. 12-22, 2019.

[64] Ramzan, Zulfikar (2010). «Phishing attacks and countermeasures». In: Stamp, Mark; Stavroulakis, Peter. *Handbook of Information and Communication Security*. [S.l.]: Springer. ISBN 978-3-642-04117-4

[65] DA VEIGA, Adele; MARTINS, Nico. Improving the information security culture through monitoring and implementation actions illustrated through a case study. **Computers & Security**, v. 49, p. 162-176, 2015b.

[66] MARTINS, Nico; DA VEIGA, Adéle. The value of using a validated information security culture assessment instrument. **Retrieved on**, v. 8, n. 30, p. 2017, 2014.

[67] DA VEIGA, Adele. An Information Security Training and Awareness Approach (ISTAAP) to Instil an Information Security-Positive Culture. In: **HAISA**. 2015c. p. 95-107.

[68] WOHLIN, Claes et al. **Experimentation in software engineering**. Springer Science & Business Media, 2012.

[69] DIAS-NETO, Arilo Claudio et al. Toward the characterization of software testing practices in South America: looking at Brazil and Uruguay. **Software Quality Journal**, v. 25, n. 4, p. 1145-1183, 2017.

[70] ABNT. Tecnologia da informação –Técnicas de segurança – Código de prática para controles de segurança : ABNT NBR ISO/IEC 27002:2013. 1. ed. Rio de Janeiro, 2013.

[71] HADNAGY, Christopher. The Art of Human Hacking. 1. ed. Indianapolis: Wiley Publishing, Inc, 2011.

[72] SEBRAE-NA/ Dieese. Anuário do trabalho na micro e pequena empresa 2013, p. 17. www.sebrae.com.br/Sebrae/Portal%20Sebrae/Anexos/Anuario%20do%20Trabalho%20Na%20Micro%20e%20Pequena%20Empresa_2013.pdf

[73] LIMA, Vagner Carlos Marcolino; NETO, Adolfo Gustavo Serra Seca; EMER, Maria Claudia Figueiredo Pereira. Investigação Experimental E Práticas Ágeis: Ameaças À Validade De Experimentos Envolvendo A Prática Ágil Programação em Par/Experimental Investigation And Agile Practices: Threats To The Validity Of Experiments Involving The Pair Programming Agile Practice. **Revista Electronica de Sistemas de Informaçao**, v. 13, n. 1, p. 1, 2014.

APÊNDICE A - Questionário utilizado no survey

Pesquisa sobre Cultura de Segurança da Informação nas Organizações

Termo de Consentimento Livre e Esclarecido ao Responsável

Prezado voluntário,

Através deste questionário, convidamos você a participar de uma pesquisa para obtenção de dados relacionados a cultura de segurança da informação nas organizações.

Esta pesquisa pertence a um trabalho de conclusão de curso do Centro de Informática (CIn) da Universidade Federal de Pernambuco (UFPE).

O objetivo deste estudo consiste na sua participação de modo que possa responder às perguntas apresentadas, com a finalidade de diagnosticarmos o estado da prática referente a cultura de segurança da informação nas organizações; além da coleta de outras informações consideradas pertinentes.

Gostaríamos de enfatizar que:
1. Sua participação é totalmente voluntária e anônima.
2. Todas as informações que você fornecer serão mantidas em sigilo.
3. Não há a intenção de julgá-lo como pessoa ou a empresa. Existe apenas o interesse em investigar a sua opinião profissional perante a área coberta nesta pesquisa. 4. A qualquer momento você pode desistir de participar e retirar seu consentimento. 6. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou com a instituição.
7. Os dados coletados neste formulário não serão divulgados de forma a possibilitar sua identificação.

Pesquisadores Responsáveis:
- Pedro Vinícius de Lima Santos (Graduando em Sistemas de Informação no CIn/UFPE) - pvls@cin.ufpe.br
- Jéssyka Vilela (Professora Doutora no CIn/UFPE) - jffv@cin.ufpe.br
- Mariana Peixoto (Pesquisadora e Doutoranda no CIn/UFPE) - mmp2@cin.ufpe.br Caso necessário,

fique à vontade para entrar em contato com esse comitê responsável.

Este questionário é composto de 10 perguntas rápidas sobre seu perfil e experiência mais 20 perguntas sobre sua opinião em relação a cultura de segurança da informação. Caso você decida participar, o mesmo leva aproximadamente 10 minutos para ser respondido. *Obrigatório

1. Declaro que entendi os objetivos, riscos e benefícios de minha participação na pesquisa. *Este termo de consentimento será considerado assinado, com o aceite no formulário eletrônico. Entretanto, caso os participantes queiram uma versão impressa, basta requerê-la aos pesquisadores. *

Marcar apenas uma oval.

○ Aceito participar

Perfil do Participante

Essa seção tem como objetivo identificar o perfil do profissional que está respondendo essa pesquisa bem como sua experiência educacional e com a área de segurança da informação que é o foco desta pesquisa

1) Qual o tipo de instituição que você atua?*

Marcar apenas uma oval.

○ Instituição Pública

○ Instituição Privada

○ Instituição Política

○ Instituição Jurídica

○ Instituição Religiosa

○ Outro: _____

2) Em qual estado brasileiro a organização que você trabalha está localizada?*

Marcar apenas uma oval.

○ Trabalho para uma empresa localizada fora do Brasil.

○ AL	○ GO	○ PR	○ RR
○ AP	○ MA	○ PE	○ SC
○ AM	○ MT	○ PI	○ SP

○ BA	○ MS	○ RJ	○ SE
○ CE	○ MG	○ RN	○ TO
○ DF	○ PA	○ RS	
○ ES	○ PB	○ RO	

3) Qual é o porte da empresa que você trabalha? *

Marcar apenas uma oval.

- ○ Microempresa (até 9 funcionários)
- ○ Pequeno (de 10 a 49 funcionários)
- ○ Médio (de 50 a 99 funcionários)
- ○ Grande (100 ou mais funcionários)

4) A empresa atua em qual segmento? *

Marcar apenas uma oval.

- ○ Educação
- ○ Informática
- ○ Saúde
- ○ Judiciário
- ○ Religião
- ○ Outro:_____

5) Qual é o seu cargo na empresa? Exemplo: Analista *

_____

6) Há quanto tempo você trabalha na organização (em anos)?*

Marcar apenas uma oval.

- ○ Menos de 1
- ○ 1 - 5
- ○ 6 - 10
- ○ 11-15
- ○ 16 - 20
- ○ Mais de 20

7) Qual é a sua maior titulação concluída? *

Marcar apenas uma oval.

- ○ Ensino Médio/Técnico
- ○ Graduação
- ○ Especialização
- ○ Mestrado
- ○ Doutorado
- ○ Pós-doutorado

8) Você já fez algum curso de capacitação ou participou de algum treinamento sobre segurança da informação? *

Marcar apenas uma oval.

- ○ Não
- ○ Sim

9) Se você já fez algum curso de capacitação ou participou de algum treinamento, poderia apresentar detalhes? Por exemplo: ano, carga horária, tópicos abordados.

_____
_____
_____

10) Você trabalha ou já trabalhou com informações sigilosas? Como foi a experiência? *

_____
_____
_____

Percepção em Segurança da Informação

Essa seção tem como objetivo identificar o comportamento do profissional que está respondendo essa pesquisa bem como sua percepção em algumas dimensões que compõem a cultura de segurança da informação. As perguntas estão divididas em cinco escalas diferentes de resposta, a escolha deve ser baseada em concordância com o que o voluntário acredita.

.

1) Eu compreendo que Engenharia Social é a habilidade de coletar dados confidenciais por meio da persuasão. *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Neutro
- ○ Discordo parcialmente
- ○ Discordo totalmente

2) Acredito que todas as solicitações de informações sobre a empresa devem ser concedidas somente a quem tem autorização. *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Neutro
- ○ Discordo parcialmente
- ○ Discordo totalmente

3) Já recebi algum contato através de email, chamadas telefônicas ou SMS e desconfiei que tenha sido um ”trote“ para capturar informações que tenho acesso. *

Marcar apenas uma oval.

- ○ Nunca
- ○ Uma vez
- ○ Algumas vezes
- ○ Muitas vezes

4) A minha empresa define claramente o que se espera que eu faça a respeito da segurança da informação. *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Discordo parcialmente
- ○ Discordo totalmente
- ○ Não tenho conhecimento

5) Os meus colegas de trabalho demonstram comprometimento e iniciativas em segurança da informação. *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Discordo parcialmente
- ○ Discordo totalmente
- ○ Não tenho conhecimento

6) Acredito que ativos de informação* em formato físico (ex: documentos e equipamentos) e em formato eletrônico (Por exemplo: informação guardada no computador, pen drive, CDs ou Google Drive) precisam sempre ser protegidos. *Ativo de informação é composto pela informação e tudo aquilo que a suporta ou se utiliza dela (Por exemplo: pessoas, software, hardware, serviços e bens intangíveis). *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Discordo parcialmente
- ○ Discordo totalmente
- ○ Não tenho conhecimento

7) Na sua opinião, qual nível de proteção a empresa oferece aos ativos da informação em formato físico (Por exemplo: documentos impressos e equipamentos)? *

Marcar apenas uma oval.

- ○ Protege Bem
- ○ Protege Parcialmente

- ○ Não protege
- ○ Não tenho conhecimento

8) Na sua opinião, qual nível de proteção a empresa oferece aos ativos da informação em formato eletrônico (Por exemplo: informação guardada no computador, pen drive, CDs ou Google Drive)? *

Marcar apenas uma oval.

- ○ Protege Bem
- ○ Protege Parcialmente
- ○ Não protege
- ○ Não tenho conhecimento

9) Acredito que a segurança da informação é de responsabilidade do departamento de TI (Tecnologia da Informação). *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente.
- ○ Neutro
- ○ Discordo parcialmente
- ○ Discordo totalmente

10) Acredito que devem ser aplicadas penalidades (por exemplo, processo disciplinar) contra qualquer pessoa que não respeite a política de segurança da informação da empresa (por exemplo, se compartilharem senhas, forneçam informações confidenciais ou visitar sites de Internet proibidos). *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente.

- ○ Neutro
- ○ Discordo parcialmente
- ○ Discordo totalmente

Princípios em Segurança da Informação

Essa seção tem como objetivo identificar o entendimento do profissional que está respondendo essa pesquisa em relação ao funcionamento dos princípios de segurança da informação na empresa que trabalha bem como sua percepção de ambiente e tolerância em relação a segurança da informação. As perguntas estão divididas em cinco escalas diferentes de resposta, a escolha deve ser baseada em concordância com o que o voluntário acredita

11) Qual o nível de dificuldade de entendimento do conteúdo da política de segurança da informação* da sua empresa? * Política de segurança é um documento com as regras sobre segurança da informação. *

Marcar apenas uma oval.

- ○ Muito Difícil
- ○ Moderadamente difícil
- ○ Nem fácil nem difícil
- ○ Moderadamente fácil
- ○ Muito Fácil
- ○ Não conheço a política da segurança da informação da empresa

12) Acredito que sou comprometido com a política de segurança da informação da minha empresa durante a execução das minhas tarefas diárias. *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Neutro
- ○ Discordo parcialmente
- ○ Discordo totalmente

13) Acredito que a minha empresa promove engajamento das pessoas em segurança da informação. *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Neutro
- ○ Discordo parcialmente
- ○ Discordo totalmente

14) Eu aceito positivamente mudanças nas minhas práticas de trabalho a fim de garantir a segurança dos ativos de informação da empresa (por exemplo, a mudança da minha senha regularmente, bloqueando documentos confidenciais ou de apoio). *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Neutro
- ○ Discordo parcialmente
- ○ Discordo totalmente

15) Acredito que prestadores de serviço que têm acesso a informações confidenciais da minha empresa preservam a sua confidencialidade. *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Neutro
- ○ Discordo parcialmente
- ○ Discordo totalmente

16) Acredito que a minha empresa protege as minhas informações privadas (por exemplo, dados pessoais ou avaliação de desempenho). *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Neutro
- ○ Discordo parcialmente
- ○ Discordo totalmente

17) Acredito que há necessidade de treinamentos para melhor compreensão das normas de segurança da informação a fim de proteger a informação. *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Neutro
- ○ Discordo parcialmente
- ○ Discordo totalmente

18) Acredito que as iniciativas de sensibilização (por exemplo, treinamentos, campanhas, cursos de capacitação) para a segurança da informação são eficazes. *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Neutro
- ○ Discordo parcialmente
- ○ Discordo totalmente

19) Acredito que, quando necessário, a privacidade deve ser abordada ao planejar atividades na empresa. *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Neutro
- ○ Discordo parcialmente
- ○ Discordo totalmente

20) Acredito que é importante limitar a coleta e compartilhamento de informações pessoais sensíveis (por exemplo, religião, orientação sexual). *

Marcar apenas uma oval.

- ○ Concordo totalmente
- ○ Concordo parcialmente
- ○ Neutro
- ○ Discordo parcialmente
- ○ Discordo totalmente

Você gostaria de fazer algum comentário ou sugestão sobre essa pesquisa?

_____
_____
_____

APÊNDICE B - Termo de Consentimento

Pesquisa sobre Cultura de Segurança da Informação nas Organizações

Termo de Consentimento Livre e Esclarecido ao Responsável

Prezado voluntário,

Através deste questionário, convidamos você a participar de uma pesquisa para obtenção de dados relacionados a cultura de segurança da informação nas organizações.

Esta pesquisa pertence a um trabalho de conclusão de curso do Centro de Informática (CIn) da Universidade Federal de Pernambuco (UFPE).

O objetivo deste estudo consiste na sua participação de modo que possa responder às perguntas apresentadas, com a finalidade de diagnosticarmos o estado da prática referente a cultura de segurança da informação nas organizações; além da coleta de outras informações consideradas pertinentes.

Gostaríamos de enfatizar que:
1. Sua participação é totalmente voluntária e anônima.
2. Todas as informações que você fornecer serão mantidas em sigilo.
3. Não há a intenção de julgá-lo como pessoa ou a empresa. Existe apenas o interesse em investigar a sua opinião profissional perante a área coberta nesta pesquisa.
4. A qualquer momento você pode desistir de participar e retirar seu consentimento.
6. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou com a instituição.
7. Os dados coletados neste formulário não serão divulgados de forma a possibilitar sua identificação.

Pesquisadores Responsáveis:
- Pedro Vinícius de Lima Santos (Graduando em Sistemas de Informação no CIn/UFPE) - pvls@cin.ufpe.br
- Jéssyka Vilela (Professora Doutora no CIn/UFPE) - jffv@cin.ufpe.br
- Mariana Peixoto (Pesquisadora e Doutoranda no CIn/UFPE) - mmp2@cin.ufpe.br

Caso necessário, fique à vontade para entrar em contato com esse comitê responsável.

Este questionário é composto de 10 perguntas rápidas sobre seu perfil e experiência mais 20 perguntas sobre sua opinião em relação a cultura de segurança da informação. Caso você decida participar, o mesmo leva aproximadamente 10 minutos para ser respondido.
*Declaro que entendi os objetivos, riscos e benefícios de minha participação na pesquisa. *Este termo de consentimento será considerado assinado, com o aceite no formulário eletrônico. Entretanto, caso os participantes queiram uma versão impressa, basta requerê-la aos pesquisadores.*

( ) Aceito participar