UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO

FILIPE VALENÇA E SILVA

SEGURANÇA DA INFORMAÇÃO ENTRE SENIORES: ASPECTOS DE AFASTAMENTO A BOAS PRÁTICAS EM UMA ORGANIZAÇÃO SERGIPANA.

São Cristóvão – SE
2023

FILIPE VALENÇA E SILVA

SEGURANÇA DA INFORMAÇÃO ENTRE SENIORES: ASPECTOS DE AFASTAMENTO A BOAS PRÁTICAS EM UMA ORGANIZAÇÃO SERGIPANA.

Projeto de dissertação apresentado como requisito parcial para obtenção do título de Mestre pelo Programa de Pós-Graduação em Administração da Universidade Federal de Sergipe, de acordo com a resolução Nº 04/2021 do CONEPE.

Orientador: Professor Dr. Jefferson David Araújo Sales

Linha de Pesquisa: Inovação e Tecnologia

São Cristóvão – SE
2023

**FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE**

S586s

Silva, Filipe Valença e
Segurança da informação entre sêniores : aspectos de afastamento a boas práticas em uma organização sergipana / Filipe Valença e Silva ; orientador Jefferson David Araújo Sales. – São Cristóvão, SE, 2023.
113 f. : il.

Dissertação (mestrado em Administração) – Universidade Federal de Sergipe, 2023.

1. Administração. 2. Inovações tecnológicas. 3. Tecnologia da informação. 4. Tecnologia e idosos – Sergipe. 5. Trabalhadores idosos – Efeito da automação. 6. Comportamento organizacional – Estudo de casos. I. Sales, Jefferson David Araujo, orient. II. Título.

CDU 658:005.591.6

UNIVERSIDADE FEDERAL DE SERGIPE - UFS
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO
MESTRADO EM ADMINISTRAÇÃO

Ata de Defesa de Dissertação

Mestrando (a): FILIPE VALENCA E SILVA
Título da dissertação: SEGURANÇA DA INFORMAÇÃO ENTRE SENIORES: ASPECTOS DE AFASTAMENTO ÀS MELHORES PRÁTICAS EM UMA ORGANIZAÇÃO SERGIPANA.
Data e horário da defesa: 29/08/2023 às 14:00

Examinadores
- Prof.Dr.Jefferson David Araújo Sales (Presidente - Orientador)
- Profa.Dra. Maria Conceição Melo Silva Luft (Examinador Interno)
- Profa.Dra.Alessandra Cabral Nogueira Lima (Examinador Externo ao Programa)

Parecer: Depois de avaliarmos a dissertação e realizados os ritos acadêmicos da defesa, em que o (a) candidato (a) apresentou em sessão pública seu trabalho de pesquisa e respondeu aos nossos questionamentos, atribuímos, em sessão privada, o seguinte conceito:
_X_ Aprovado (a)
_____ Reprovado (a)

São Cristóvão, 29 de agosto de 2023.

Documento assinado digitalmente
JEFFERSON DAVID ARAUJO SALES
Data: 29/08/2023 15:01:27-0300
Verifique em https://validar.iti.gov.br

Prof.Dr.Jefferson David Araújo Sales
(Presidente - Orientador)

Documento assinado digitalmente
MARIA CONCEICAO MELO SILVA LUFT
Data: 30/08/2023 15:22:31-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Maria Conceição Melo Silva Luft
(Examinador Interno)

Documento assinado digitalmente
ALESSANDRA CABRAL NOGUEIRA LIMA
Data: 29/08/2023 15:06:53-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Alessandra Cabral Nogueira Lima
(Examinador Externo ao Programa)

Documento assinado digitalmente
FILIPE VALENCA E SILVA
Data: 30/08/2023 16:44:04-0300
Verifique em https://validar.iti.gov.br

(Discente)

Agradecimentos

Dedico o resultado desse esforço a quem devo tudo o que sou: dona Janja e seu Paulo, meus queridos e amados pais... Obrigado pelo exemplo, pelo sacrifício que fizeram por mim e pelo amor demonstrado. Agradeço a meus maravilhosos irmãos, Thiago, Paulinha e Paulinho, que desde o primeiro dia estiveram perto de mim, mesmo que à distância, e sempre ajudaram quando precisei.

No contexto do mestrado, começo agradecendo ao grande mestre, que apesar de ser doutor sempre chamarei assim. Professor Jefferson, serei eternamente grato pela paciência e valiosíssimos ensinamentos.

Professora Ceiça, sempre firme e generosa ao mesmo tempo, obrigado pelo conhecimento comigo compartilhado, pois sempre aprendi muito contigo.

Profa. Alessandra Nogueira, também agradeço pelas reflexões e aprendizado proporcionado, sobretudo em minha banca de qualificação.

Às professoras da graduação Alcione e Maria Teresa, que me transmitiram conhecimento e que, com sua generosidade e competência, tornaram essa jornada mais agradável e proveitosa.

Aos demais professores, Ludmilla, Florence, Rúbia e Marley, meu muito obrigado! À colega Manu (Emanuela), uma das pessoas mais doces, inteligentes e capazes que já conheci. É sempre um prazer!

À EMDAGRO, seus diretores e colegas do NUPORT (Ivan, Carlos, Reginaldo, Ângelo, Rafael e Marcelo) e demais empregados, sem vocês nada disso teria sido possível, desde o começo da caminhada. Obrigado pela parceria e pelas risadas, que tornaram todo o processo mais agradável e produtivo.

Ao PROPADM e seus integrantes, sempre solícitos e amáveis. Obrigado por me ajudarem a realizar o sonho de cursar um mestrado.

Quem quer ser mais do que é, um dia há de sofrer.

Gilberto Gil

RESUMO

Em um cenário onde estimativas indicam uma maior presença de sêniores, ou indivíduos com mais de 55 anos de idade, no mercado de trabalho nos próximos anos, possíveis riscos à segurança da informação (SI) advindos de uma mão-de-obra com menor conhecimento técnico acerca das ameaças e de técnicas de defesa são um ponto de atenção a organizações, cada vez mais dependentes de sistemas de informação digital. Dito isto, o presente estudo teve como objetivo investigar a percepção dos sêniores acerca dos aspectos da conscientização em segurança da informação (CSI) em um ambiente corporativo, identificando fatores de afastamento dessas pessoas às melhores práticas de proteção à informação em uma empresa pública sergipana. A CSI se divide em aspectos cognitivos, comportamentais e de processos, que representam as dimensões que compõem o uso seguro da tecnologia em um ambiente organizacional. Foi conduzido um estudo de caso qualitativo único, incorporado, de abordagem descritiva e exploratória, com dados coletados mediante entrevistas orientadas por um roteiro semiestruturado e por observação das atividades da empresa. Os dados foram analisados via análise de conteúdo. Os resultados da pesquisa apontam que dentre os fatores de afastamento dos sêniores às melhores práticas em SI, verificou-se: limitado contato com os especialistas de tecnologia da informação da empresa, que tende a proporcionar um maior intercâmbio de conhecimentos técnicos de qualidade; a reduzida percepção técnica das ameaças à segurança da informação, não tendo consciência do alcance dos danos de um comportamento inseguro; um menor grau de comprometimento com os objetivos de segurança da informação da organização, representado pela ausência de preocupação com possíveis prejuízos à empresa, sendo suas preocupações voltadas apenas a prejuízos pessoais; comunicação deficiente por parte da gestão de tecnologia da organização, pela ausência do envio de alertas e lembretes aos empregados; falta de envolvimento de gestores por parte da organização, seja no incentivo, atitude de exemplo ou cobrança/responsabilização em caso de comportamento inseguro; e uma baixa adesão a treinamentos, influenciada possivelmente por baixo interesse e sensação de baixa autoeficácia na operação de dispositivos digitais.

Palavras-chave: Segurança da informação; Empregados sêniores; Ambiente organizacional; Estudo de caso.

ABSTRACT

In a scenario where estimates indicate a greater participation of senior people, or individuals over 55 years of age, in the labour market in the coming years, possible risks to information security arising from an aging workforce with less technical knowledge about threats and defense techniques are a point of attention for organizations, increasingly dependent on digital information systems (IS). That said, the present study aimed to investigate the perception of seniors regarding aspects of information security awareness (ISA) in a corporate environment, identifying factors that keep these people away from the best information protection practices in a public sector company in the state of Sergipe. The ISA is divided into cognitive, behavioral and processes aspects, which represent the dimensions that constitute the safe use of technology in an organizational environment. A single, case-cohort qualitative case study was conducted, with a descriptive and exploratory approach, with data collected through interviews, guided by a semi-structured script and by observation of the company's daily activities. Data were analyzed via content analysis. The results of the research indicate the following among the factors that separate seniors from the best practices in IS: limited contact with the company's information technology specialists, practice that tends to provide a greater exchange of technical quality knowledge; a reduced technical perception of threats to information security, not being aware of the extent of damage from unsafe behavior; a lower degree of commitment to the organization's information security objectives, represented by the lack of concern with possible harm to the company, with concerns limited to personal harm; a poor communication by the organization's information technology management, due to the lack of sending alert messages and reminders to employees; the lack of involvement of managers and directors of the organization, either in the incentive, giving example or charge/accountability in case of unsafe behavior; and a low adherence to training, possibly influenced by low interest and a low sense of self-efficacy in operating digital devices.

Keywords: Information security; Senior employees; Organizational environment; Case study.

SUMÁRIO

Lista de Figuras

Lista de Quadros

Lista de Gráficos

Lista de siglas e abreviações

BANESE – Banco do Estado de Sergipe

CPF – Cadastro de Pessoa Física

CSI – Conscientização em Segurança da Informação

DIEESE - Departamento Intersindical de Estatística e Estudos Sócio Econômicos

EMGETIS – Empresa Sergipana de Tecnologia da Informação

ES – Engenharia Social

FEM - Fórum Econômico Mundial

IBGE – Instituto Brasileiro de Geografia e Estatística

ONU - Organização das Nações Unidas

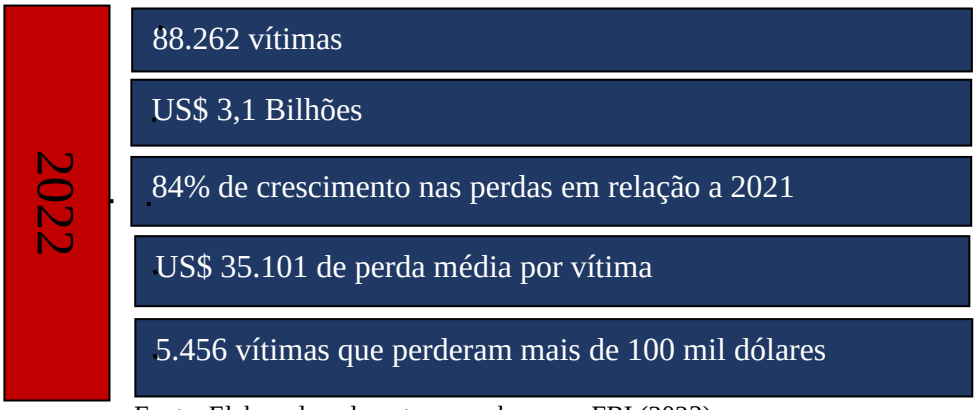
PEC - Proposta de Emenda à Constituição

SI – Segurança da Informação

1. INTRODUÇÃO

Sêniores, ou adultos com mais de 55 anos de idade, são vistos pela literatura especializada em segurança da informação (SI) como particularmente vulneráveis a cybercriminosos. O FBI, ou *Federal Bureau of Investigation* estadunidense, afirma que os prejuízos sofridos por essas pessoas aumentaram 84% entre 2020 e 2022, com perdas na casa dos US$ 3,1 bilhões. São os maiores valores entre as 06 faixas etárias verificadas no relatório anual de crimes digitais da entidade (FBI, 2023), cenário que pode ser visualizado na Figura 01.

Figura 01 – Perdas sofridas pelos sêniores com fraudes digitais nos Estados Unidos, no ano de 2022.



Fonte: Elaborado pelo autor, com base em FBI (2023).

Trazendo a discussão do crescimento do número de incidentes em segurança da informação para o âmbito organizacional brasileiro, observou-se um aumento de 274% desse tipo de incidente em empresas do país nos anos de 2018 a 2022 (PWC, 2022). Para Melo Neto e Araújo (2019) e Stelzer *et al*. (2019), organizações baseadas em grandes centros como a Europa e Estados Unidos demonstram maior maturidade em suas práticas de segurança da informação, enquanto a maioria das empresas brasileiras ainda buscam implementar boas práticas de SI em seus ambientes.

Nesse ínterim, a grandeza das cifras de valores perdidos por organizações com crimes cibernéticos cresce paralelamente à quantidade de dados pessoais de clientes sob o poder das empresas, a exemplo de números de cartões de crédito, senhas e outros dados sensíveis. Dessa maneira, acentua-se a atenção concedida por *stakeholders* a melhores práticas em gestão de segurança da informação, culminando em ações legais e prejuízos financeiros e de reputação. A própria Lei Geral de Proteção de Dados (LGPD), aprovada em 2020, regulamenta a gestão de dados e informações por parte das empresas, requerendo dos gestores adequação a boas práticas em SI (STELZER ET AL., 2019; FÓRUM ECONÔMICO MUNDIAL - FEM, 2022).

Adicionalmente, usuários são vistos como elo mais fraco na cadeia de proteção à informação em uma organização. Para Whitman e Mattord (2017) e FBI (2023), os próprios empregados originam 70% das falhas de segurança, causadas pelo uso não conforme com boas práticas em SI. Melo Neto e Araújo (2019) mencionam que, no contexto brasileiro, 39% de todos os incidentes ocorridos em 2019 nas pequenas empresas causados por seus próprios funcionários trouxeram prejuízos financeiros (GREEN; DOREY, 2016; WHITMAN; MATTORD, 2017).

No mesmo cenário, estimativas do IBGE sinalizam que sêniores estarão mais ativos no mercado de trabalho nos próximos anos, devido ao aumento da expectativa de vida no país e à aprovação da reforma da previdência, em 2016. Aspectos restritivos ao acesso à aposentadoria integral são vistos possíveis condutores dessas pessoas à busca por suplementação de renda nos próximos anos (DIEESE, 2017; IBGE, 2019; ESTEVES; GOMES, 2020).

A presente pesquisa recorre ao conceito da Conscientização em Segurança da Informação (CSI), observada como o conjunto de aspectos referentes à consciência do usuário de tecnologia quanto aos riscos e ameaças à segurança de dados e informações em ambientes organizacionais (PRAWOBO; TJONG, 2017; FRIK ET AL., 2019). Para os autores, a investigação de uma organização norteada pelos conceitos da CSI permite lançar luz a fatores de aproximação e afastamento de seus empregados a boas práticas em SI por fornecer aspectos abrangentes e bem definidos de análise (HAEUSSINGER, 2017). Tais aspectos, ou dimensões, são os seguintes:

- **Cognitivos**: relacionados à capacidade de raciocínio e absorção de conhecimento;
- **Comportamentais**: referem-se às atitudes práticas tomadas pelos usuários para proteger a informação;
- **Processos**: relacionam-se com processos estabelecidos pelas organizações para desenvolver conscientização em usuários.

Com efeito, por meio de seus aspectos, a CSI afeta a intenção do usuário em contribuir com políticas e diretrizes da organização. Em outras palavras, o usuário com alto grau de CSI exerce comportamento de proteção à informação, utilizando de computadores, tablets e smartphones de acordo com boas práticas de segurança da informação. O inverso ocorre com empregados com baixo grau de CSI, que desconhecem riscos aos quais estão sujeitos e boas práticas de proteção à informação (HAEUSSINGER, 2017; FRIK ET AL., 2019; FBI, 2023).

Em face da já mencionada estimativa do futuro do mercado de trabalho, da maior vulnerabilidade dos sêniores a crimes digitais e do aumento dos prejuízos causados pelos crimes digitais expostos até aqui, essa pesquisa teve como objetivo investigar a percepção dos sêniores acerca dos aspectos da conscientização em segurança da informação em um ambiente corporativo, identificando fatores de afastamento dessas pessoas a boas práticas de proteção à informação. Para que se alcance esse objetivo, aspectos cognitivos e comportamentais desses usuários foram investigados, bem como sua percepção acerca de processos estabelecidos pela organização com vias ao desenvolvimento da CSI nos empregados. Com intuito de facilitar a exposição das percepções dos sêniores participantes da pesquisa, utilizou-se o recurso dos mapas mentais, que são organizações gráficas de pensamentos e ideias (BUZAN, 2019).

Essa introdução segue com a apresentação do ambiente corporativo escolhido para investigação do objetivo da pesquisa, seguida da definição do problema, da declaração propriamente dita dos objetivos gerais e específicos que nortearam o estudo e da justificativa para a escolha do tema.

1.1. Ambiente de pesquisa

A presente pesquisa foi empreendida em uma organização pública sergipana: a EMDAGRO (Empresa de Desenvolvimento Agropecuário de Sergipe), organização vinculada à Secretaria do Estado da Agricultura, Desenvolvimento Agrário e Pesca. Fundada em 1962, atua junto ao produtor rural na execução de assistência técnica, extensão rural, pesquisa agropecuária, defesa animal e vegetal e ações fundiárias, tendo como missão fortalecer a agricultura familiar e o agronegócio do Estado de Sergipe (GOVERNO DO ESTADO, 2023).

Com uma força de trabalho composta por 339 empregados próprios e 65 terceirizados, distribuídos em escritórios em 60 dos 75 municípios do estado, a EMDAGRO foi escolhida como ambiente para essa pesquisa em virtude da elevada faixa etária média de seus trabalhadores: 70% deles são sêniores, ou adultos com mais de 55 anos de idade. Outro fator determinante para a escolha do ambiente de pesquisa é a participação do autor como integrante

do núcleo de informática da empresa, sendo responsável pelo atendimento e administração dos recursos tecnológicos do órgão (TRANSPARÊNCIA SERGIPE, 2023).

Pelo constante contato com os usuários e suas solicitações, tornou-se possível ao autor observar a interação dos sêniores com a tecnologia e a segurança da informação. A implementação de políticas de segurança, como a troca periódica de senhas e assinatura digital de documentos por parte do órgão centralizador de processamento de dados, a Empresa Sergipana de Tecnologia da Informação (EMGETIS), por vezes representam dificuldades aos usuários sêniores. Em virtude do aumento de incidentes de segurança relacionados ao e-mail reportados ao longo dos últimos anos, a EMGETIS definiu a política de troca de senha mensal, exigindo que os empregados a troquem todos os meses, respeitando altos critérios de complexidade. A partir disso, diversas solicitações de falta de acesso aos serviços de e-mail e acesso à internet, que utilizam a mesma credencial, eram registradas na empresa, pois os usuários sêniores apresentavam dificuldade de efetuar o procedimento.

Percebe-se também no ambiente da empresa a percepção de que muitos usuários sêniores, incluindo coordenadores e diretores, apresentam baixa sensação de autoeficácia na operação de dispositivos digitais e sistemas. A gama de situações nas quais essa concepção se materializa vão desde a dificuldade em operar programas que executam tarefas do dia-a-dia, como o Microsoft Word e navegação de internet, à geração e interpretação de relatórios importantes.

Adicionalmente, com avanço do processo de digitalização dos processos da empresa, a exemplo do registro de atendimentos a produtores rurais, emissão de guias de trânsito vegetal e animal e da substituição do protocolo físico por sistema eletrônico, percebe-se ainda mais a dificuldade de adaptação de muitos desses usuários. Em contrapartida, não se observam na organização processos de estímulo à qualificação em segurança da informação por parte da diretoria e da maioria dos gestores.

1.2. Problema de pesquisa

Interessados na grande quantidade de dados e informações que circulam diariamente na internet e em redes privadas, indivíduos e grupos especializados em crimes cibernéticos trabalham para subtrair informações de modo não autorizado, causando, quase sempre, prejuízos aos usuários e organizações ora lesados. De acordo com a Ernest and Young (2021), as perdas em 2021 com crimes dessa natureza atingiram 725 bilhões de dólares, prejuízos oriundos de descontinuidades operacionais, ações legais iniciadas por consumidores prejudicados e danos estimados à reputação das marcas afetadas. Essa grandeza de perdas ocorre em meio a evoluções técnicas em controles de proteção de ambientes digitais, a exemplo de *firewalls*, agentes de segurança como softwares antivírus e anti-intrusão e patches de atualização em tempo real (WHITMAN; MATTORD, 2017).

Diante do exposto até aqui, materializa-se um cenário global de aumento de risco de segurança da informação às organizações, acompanhado do incremento na sofisticação técnica das ameaças às quais os usuários de tecnologia sêniores estão expostos. Esses indivíduos são apontados pela literatura como os mais vulneráveis aos cibercriminosos, característica que pode favorecer a ocorrência de falhas de SI em ambientes organizacionais. Em contrapartida, a gestão da informação executada de acordo com boas práticas reduz, de acordo com Prawobo e Tjong (2017), a exposição a riscos de segurança da informação, contribuindo à competitividade da organização (HARGITTAI; DOBRANSKY, 2017)

Adicionalmente, a conformidade às melhores práticas de gestão da segurança da informação evita descontinuidades operacionais, reduzindo interrupções de fluxos de trabalho e consequentes prejuízos derivados dessas contingências, a exemplo de perdas financeiras, de reputação e responsabilizações legais. Com efeito, contribui às chances de sobrevivência das

organizações em um cenário de atenção social à correta gestão de dados e informações (MASUCH ET AL., 2021).

Dito isto, em face da tendência de uma maior presença de sêniores no mercado de trabalho e da criticidade da informação no sucesso das organizações, discutir melhorias acerca da proteção de dados e informações em ambientes organizacionais se faz oportuno. Assim, pode-se considerar válida a discussão que lance luz à relação dos sêniores com a tecnologia digital, e que possa contribuir ao favorecimento da conscientização dessas pessoas em segurança da informação em organizações. Nesse ínterim, com os usuários sêniores da organização selecionada como ambiente de pesquisa enfrentando dificuldades na utilização de dispositivos digitais, muitas vezes apartados das melhores práticas em SI, definiu-se a seguinte questão de pesquisa: como a percepção dos usuários sêniores da organização acerca dos aspectos da CSI os afasta das boas práticas em segurança da informação?

Para conferir direcionamento lógico ao estudo, serão expostos na sequência os objetivos norteadores do estudo, que também iniciam a justificativa o desenvolvimento do problema de pesquisa.

1.3. Objetivos

A investigação da percepção dos sêniores da organização estudada acerca da CSI lançou base ao atendimento dos objetivos da pesquisa, que foram delineados da seguinte maneira:

1.3.1. Objetivo geral

Investigar a percepção dos sêniores acerca dos aspectos da conscientização em segurança da informação em um ambiente corporativo, identificando fatores de afastamento dessas pessoas a boas práticas de proteção à informação.

1.3.2. Objetivos específicos

1. Investigar aspectos cognitivos dos sêniores em relação à segurança da informação;
2. Investigar aspectos comportamentais dos sêniores da organização em relação à segurança da informação;
3. Conhecer a percepção dos usuários sêniores a respeito de aspectos de processos realizados na organização;
4. Elencar fatores de afastamento desses empregados às boas práticas de proteção à informação;

1.4. Justificativa

Sinteticamente, a justificativa de um estudo observa os motivos que conduziram o pesquisador à investigação de um determinado fenômeno. Dito isto, a presente pesquisa encontra justificativa pela relevância e contemporaneidade do tema, pelo contexto em que está inserida, pela carência de estudos relacionados ao tema no campo da Administração e de Sistemas de Informação e pelas contribuições aos campos teórico e aplicado.

Diante do até agora exposto, o cenário crescente de perdas de diversas ordens sofridas pelas organizações, sobretudo em virtude de falhas de segurança causadas por falhas humanas, traz consigo a necessidade do desenvolvimento da gestão da tecnologia da informação organizacional. Com efeito, a delimitação de estratégias que contemplem aspectos da relação de usuários sêniores com a segurança da informação tende a contribuir à minimização de riscos e possíveis prejuízos que podem advir de uma mão de obra cada vez mais envelhecida, apontada

pela literatura especializada como defasada em conhecimentos tecnológicos e mais vulnerável a ameaças de SI.

De maneira mais ampla, foi intenção dessa pesquisa construir conhecimentos acerca das limitações encontradas pelos sêniores na lida com a tecnologia, o que pode auxiliar no favorecimento da produtividade dessas pessoas em ambientes organizacionais, proporcionar oportunidades de inclusão social e incremento de sua percepção de sua autoeficácia no uso da tecnologia digital (MANNHEIM ET AL., 2019).

Outrossim, não são comuns na literatura científica atual estudos que possam contribuir acadêmica e profissionalmente no campo da Administração e da Tecnologia da Informação que analisem o tema, apesar de diversas análises sobre a interação do sênior com a tecnologia estarem disponíveis em plataformas científicas. Por conta disso, o estudo assume relevância aos campos mencionados, em virtude da pouca exploração das limitações de empregados sêniores em relação à segurança da informação no âmbito organizacional.

Conforme anteriormente mencionado, o contexto de cada vez maior interesse da sociedade por melhores práticas de gestão de dados e informações, bem como a entrada em vigor da LGPD, permitem que estudos que abordem a temática da percepção de empregados sêniores sejam considerados cada vez mais relevantes a organizações.

Buscam-se, também, maiores conhecimentos acerca de fatores que favoreçam a inclusão tecnológica e a empregabilidade de sêniores por órgãos internacionais, a exemplo da União Europeia e ONU que consideram essas questões como prioritárias em suas agendas. Assim, pesquisas que lancem luz sobre questões relacionadas à relação dos sêniores com a tecnologia digital podem fornecer conhecimentos oportunos à sua maior inclusão tecnológica, favorecendo a inserção e permanência no mercado de trabalho e incrementando a qualidade de vida desse grupo (FÉLIX, 2016; FBI, 2023).

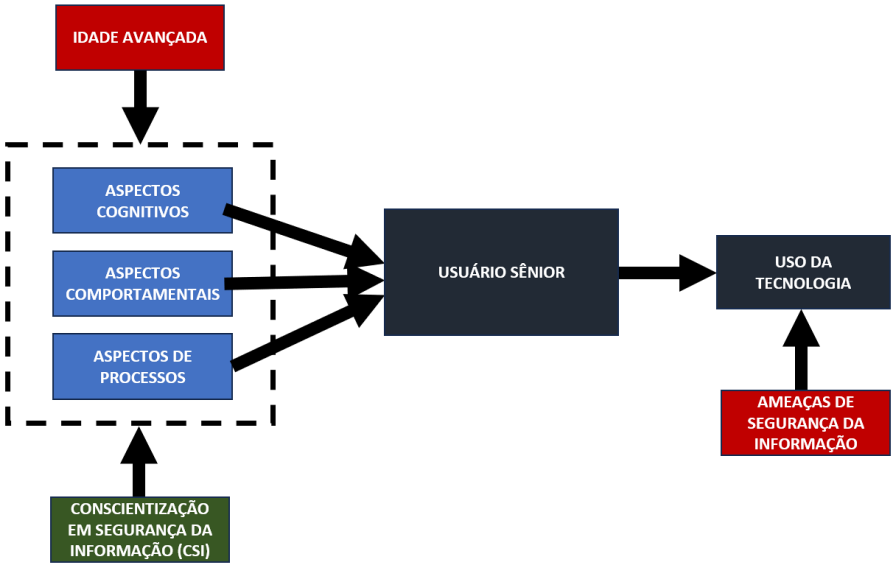
A ora apresentada pesquisa está organizada em cinco capítulos. A presente introdução constitui o capítulo 01 e contextualiza a temática, além de apresentar os seguintes elementos da pesquisa: problema, objetivos e justificativa. O capítulo 02 expõe a fundamentação teórica que embasa o estudo, a exemplo de aspectos da conscientização em segurança da informação, conceitos de segurança da informação e características do envelhecimento humano também serão apresentados. Em seguida serão abordados, no capítulo 03, os procedimentos metodológicos a serem adotados na pesquisa, seguido do capítulo 04 que fará a exposição da análise dos dados obtidos no estudo. Por fim, as considerações finais poderão ser visualizadas no capítulo 05.

Serão expostos, na sequência, a apresentação da base teórica da pesquisa, a descrição dos procedimentos metodológicos que a nortearam, a análise dos dados coletados e, por último, suas considerações finais.

2. REFERENCIAL TEÓRICO

Para que seja alcançado o produto desejado nesta investigação, empreendeu-se uma consulta à literatura especializada sobre os temas e teorias relevantes ao estudo, conforme diagrama conceitual da pesquisa apresentado na Figura 02.

Figura 02 – Diagrama conceitual da pesquisa.



Fonte: Elaborado pelo autor (2022).

O diagrama expõe a influência dos aspectos ou dimensões componentes da CSI no mapa mental dos usuários de tecnologia em organizações. No cenário da empresa estudada, a constituição de cada um desses aspectos nos sêniores sofre influência de sua idade avançada, fator visto como fonte de particularidades pela literatura especializada. Para autores como Kamariza (2017) e Llorente-Barroso *et al*. (2018) essa característica etária tende a dificultar a relação dessas pessoas com a tecnologia, e afastá-los das melhores práticas em SI. Tais características afetam o processo de tomada de decisão dos sêniores no uso de tecnologias digitais, constantemente sujeito a ameaças e riscos variados à segurança de seus dados e informações.

Dito isto, serão apresentadas noções teóricas acerca da segurança da informação e aspectos a ela relacionados, ameaças mais frequentes às quais os usuários estão expostos e práticas recomendadas pela literatura para reduzir os riscos de incidentes de segurança. Aspectos do envelhecimento humano, que afetam a relação dos sêniores com a tecnologia digital, também serão abordados. Por último, a conscientização em segurança da informação e seus aspectos, bem como os conceitos relacionados a modelos mentais e sua relação com a SI serão apresentados.

2.1. Segurança da informação

Registros históricos revelam que a preocupação com segurança da informação é antiga na história da humanidade, datando de milênios atrás. Um dos relatos mais remotos sobre o tema revela que os egípcios da antiguidade oriental já tomavam precauções no sentido de preservar informações sensíveis. Segundo França (2005, p. 2):

> Khnumhote, servo e arquiteto do faraó egípcio Amenemhet II, construiu monumentos e documentou características das construções de forma codificada, substituindo

> palavras ou partes do texto. As informações, registradas em tábuas de argila, não poderiam ser lidas e compreendidas por ladrões se fossem roubadas, dificultando a localização das câmaras dos tesouros. Os salteadores amargariam ainda morte por fome e sede, perdidos nas catacumbas das pirâmides (FRANÇA, 2005, p. 2).

Em tempos atuais, a SI pode ser compreendida como a proteção à informação contra diversos tipos de ameaças, com o objetivo de minimizar riscos e evitar a descontinuidade de negócios, segundo o padrão internacional ISO/IEC 27002 desenvolvido pela *International Organization for Standardization* (Organização Internacional para Padronização [tradução nossa] (ISO, 2022). A SI é descrita ainda como instrumento que auxilia na maximização do retorno sobre investimentos e nas oportunidades para as organizações (ISO, 2022). Rao e Nayak (2014) a definem como área multidisciplinar de estudo e atividade profissional que se ocupa em desenvolver e implementar contramedidas de segurança, com vias a manter a informação livre de ameaças, a exemplo de acessos não autorizados, alterações indevidas ou indisponibilidade.

Os autores supracitados ainda descrevem a segurança da informação como um processo contínuo que envolve os componentes de um sistema de informação, a saber: pessoas, tecnologias, políticas e processos. Com efeito, a situação da SI em uma organização pode ser observada a partir da interdependência desses componentes, conforme ilustrado na Figura 03.

Figura 03 – Componentes de sistemas de informação que amparam a segurança da informação.

Fonte: Elaborado pelo autor (2022), com base em Rao e Nayak (2014).

Os componentes exibidos na Figura 03 exercem, de maneira interdependente, influência sobre o sucesso na proteção às características da informação. De acordo com Rao e Nayak (2014), os componentes são:

- **Pessoas**: razão básica da existência da segurança da informação, uma vez que são responsáveis tanto pela implementação de medidas de proteção à informação quanto por realizarem ataques cibernéticos. Por esse motivo, sua vigilância e envolvimento nas práticas de SI devem ser assegurados;
- **Organização** (por meio de políticas, procedimentos e processos): para os autores, a segurança é incompleta sem a existência de políticas claras de orientação aos empregados, fornecedores e outras partes que manipulam dados e informações. Também são importantes à SI por representarem o envolvimento dos gestores no processo de proteção à informação. Os procedimentos, por sua vez, descrevem como as políticas devem ser implementadas, materializando-se como treinamentos ou como guias passo-a-passo aos envolvidos na manipulação de dados e informações;

- **Tecnologia**: Sistemas de alerta, de registro, de detecção de invasores e de recuperação, exemplificados como software antivírus ou *firewalls* que são implementados pela organização, no intuito de tornar seus dados e informações protegidos.

A constante relação dos componentes mencionados auxilia na asseguração das características da informação, também descritas pela literatura como objetivos da SI. Suas definições e características são apresentadas no Quadro 01, juntamente com as relações que estabelecem com cada componente dos sistemas de informação (CHERDANTSEVA; HILTON, 2013)

Quadro 01 – Objetivos da SI e suas relações com os componentes de sistemas de informação.

		Componentes			
Característica/Objetivo da SI	**Definição**	**Informação**	**Pessoas**	**Processos**	**Tecnologia**
Responsabilidade	Capacidade de responsabilizar usuários pelo mau uso.		x		
Autenticidade	Capacidade de verificar a identidade e estabelecer confiança em terceiros e na informação que ele fornece	x	x	x	x
Disponibilidade	Asseguração de que todos os componentes do sistema estão disponíveis e operacionais quando requeridos por usuários	x	x	x	x
Confidencialidade	Asseguração de que apenas usuários autorizados acessam a informação	x			
Integridade	Asseguração da completude e da ausência de modificações não autorizadas de todos os componentes do sistema	x	x	x	x
Não-repúdio	Capacidade de provar (de maneira legalmente reconhecida) a ocorrência (ou não) de um evento, ou a participação (ou não) de um indivíduo num evento	x		x	

Fonte: Elaborado pelo autor (2022), com base em Cherdantseva e Hilton, (2013).

O Quadro 01 lista os objetivos da SI e suas relações com os componentes de sistemas de informação. Exemplifica também algumas dessas relações, a exemplo o objetivo responsabilidade com as pessoas do sistema, uma vez que no processo de proteção à informação é considerado boa prática atribuir imputabilidade do usuário em caso de mau uso de sistemas e da informação, estando sujeito a responsabilização de acordo com regras vigentes na organização. A auditabilidade, por sua vez, relaciona-se aos processos implementados com vias ao registro de ações realizadas no ambiente, permitindo auditoria quando necessário (ISO, 2022).

Os objetivos integridade, confidencialidade e disponibilidade são vistos pela literatura como os pilares da segurança da informação, ou tríade CID (ISO, 2022). Como um tripé, são interdependentes, necessitando que todos estejam assegurados para fornecer amparo à segurança da informação.

Serão expostas, na sequência, as principais ameaças à SI e a seus objetivos.

2.1.1 Ameaças à segurança da informação

Conforme mencionado, a meta da busca pelos os objetivos da SI pelas organizações é salvaguardar de ameaças seus ativos de informação, que são: contratos e acordos, documentações de sistemas da empresa, e-mails confidenciais, senhas e outras credenciais de acesso, projetos, estimativas financeiras e de mercado, bancos de dados, trilhas de auditoria

entre outros. Software, em forma de aplicativos, sistemas, ferramentas e bancos de dados, hardware, ou aparelhos e equipamentos físicos, como pen drives, discos rígidos, computadores e outros, e o conhecimento e experiência obtidos por empregados também podem ser listados como ativos informacionais (LYRA, 2015; STEWART ET AL. 2015).

Já as ameaças e seus impactos às quais a informação está sujeita são exibidas na Figura 04, classificadas de acordo com seus agentes de ameaça, de acordo com Haeussinger (2017), Whitman e Mattord (2017) e ISO (2022).

Figura 04 – Agentes, ameaças e impactos resultantes das ações de ameaça à informação.

Humano	Tecnológico	Organizacional	Ambiental
Internos • Mau uso intencional • Mau uso acidental Externos • Ataques hackers • Engenharia Social • Espionagem • Sabotagem ou vandalismo • Extorsão • *Phishing* • Roubo	• Falhas de software • Falhas de hardware • Falhas de rede • *Malware* (vírus, cavalos de tróia e *worms*) • *Spyware* (vírus de propaganda, rastreadores de navegação, outros) • Segurança de aplicações falha	Insuficientes (relacionados à SI): • Responsabilizações • Estratégias • Processos • Políticas • *Documentação* • Programas de treinamento em educação de segurança • Cultura	• Desastres naturais • Ataques terroristas • Guerras • Legislação

Impactos das ameaças como resultados das ações de ameaça
Destruição da informação: Destruição deliberada de um componente do sistema para interromper sua operação ou disponibilidade
Corrupção da informação: Qualquer alteração não autorizada da informação
Exposição da informação: Disseminação da informação a qualquer pessoa que não esteja autorizada a acessá-la
Roubo de um serviço ou informação: Roubo de dados ou informações, bem como uso indevido de hardware
Negação de uso (*denial of use*): Degradação intencional ou bloqueio de recursos de rede ou de computadores
Uso ilegal: Uso de funções do sistema para atingir os objetivos do atacante

Fonte: Elaborado pelo autor (2022) com base em Whitman e Mattord (2017) e Haeussinger (2017) e ISO (2022).

Conforme exposto na Figura 04, usuários de dispositivos digitais são expostos diariamente a ameaças, com técnicas de ataque cada vez mais sofisticadas. Essas técnicas buscam contornar o avanço tecnológico dos softwares e equipamentos de defesa utilizados pelas empresas (HADNAGY, 2018).

Implicações decorrentes de falhas de segurança e consequentes ataques cibernéticos podem ser exemplificados pela invasão dos sistemas que atingiram, em 2011, a corporação Sony, líder mundial em vendas de videogames. Ataques exploraram brechas de segurança causadas falhas de segurança em sistemas de informação da empresa em San Diego, Califórnia. Os criminosos roubaram dados e ameaçaram vazar informações pessoais de milhões de clientes, como senhas e números de cartões de crédito. A Sony então decidiu, como medida de defesa para impedir danos ainda mais severos, desativar por 30 dias seus serviços de mídia e a rede de jogos online do videogame mais vendido no mundo – a PlayStation Network (PSN), utilizada à época por 77 milhões de usuários (BONNER, 2012).

Desdobramentos do caso levaram a companhia japonesa a ser processada em países da Europa, Ásia e Américas em razão da ameaça dos criminosos de tornar públicos os dados dos clientes. A Sony foi multada em milhões de dólares em consequência dos processos judiciais, e ações legais derivadas do ataque também causaram danos à imagem da marca. Segundo

Olaniran *et al*. (2014) e Peter (2020) a indisponibilidade dos serviços, ações judiciais e os danos à reputação da empresa causaram um prejuízo estimado total de US$ 171 milhões.

Imagens dos executivos japoneses da empresa vindo a público para se desculparem pelas falhas de segurança, incluindo Kazuo Hirai, presidente da empresa à época, repercutiram mundialmente à época e podem retratar a já mencionada atenção da sociedade internacional à governança de TI. As características e implicações do caso são discutidas até os dias de hoje (PETER, 2020).

Figura 05 – Executivos da Sony vindo a público para se desculparem pelas falhas de segurança que afetaram a empresa em 2011.

Fonte: Peter (2020).

Ainda no que se refere aos tipos de ameaças que afetam a segurança da informação, o relatório *Global Information Security Survey 2021* (Levantamento Global de Segurança da Informação [tradução nossa]) da firma de auditoria Ernst and Young (2021) observa que ações humanas representam 72% das ameaças à segurança da informação das organizações. Intencionais ou acidentais, as ameaças de ordem humana são oriundas do mau uso de sistemas e da manipulação da informação apartada das boas práticas em SI.

Exemplos do mau uso de sistemas em ambientes organizacionais são, segundo Whitman e Mattord (2017):

- Download e execução de malware recebido por e-mail fraudulento em computadores corporativos;
- Conectar computadores pessoais infectados com vírus à rede interna da organização em empresas que autorizam o uso em seus ambientes;
- Compartilhamento de senhas com colegas;

2.1.2. Engenharia Social

Outro aspecto observado por autores como Hadnagy (2018) e Masuch *et al.* (2021) como favorecedor de riscos à SI por potencializar o alcance e a severidade dos ataques é a Engenharia Social (ES). A ES se constitui em uma área multidisciplinar de estudo que recorre a diversos campos, a exemplo do marketing, psicologia e da própria tecnologia da informação para desenvolver técnicas que auxiliam um indivíduo a se aproximar e obter a confiança ou aceitação de outra pessoa. No contexto de crimes digitais, é utilizada com objetivo de persuadir pessoas a fornecerem informações pessoais ou executarem programas maliciosos (HADNAGY, 2018).

Segundo Hadnagy (2018) e Lohani (2019), a frequência de ataques baseados em ES tem crescido anualmente, explorando a falta de conhecimento das vítimas acerca de suas técnicas de abordagem e execução utilizadas. Nesse sentido, os alvos desse tipo de ataque são abordados por meio de técnicas como *phishing*, *spear phishing*, *quid pro quo* e *baiting*, que serão descritas no Quadro 02.

Quadro 02 – Técnicas de ataque cibernético baseadas em Engenharia Social.

Técnica de ataque	Descrição
Phishing	O nome dessa técnica é uma adaptação do termo em inglês *fishing*, que significa pescar, e tem como objetivo "pescar" informações pessoais da vítima como senhas e números de cartão de crédito, solicitando sua inserção em sites de aparência legítima, que encaminham essas informações ao invasor. Usualmente a vítima recebe um e-mail com aparência semelhante ao de uma empresa real, como um banco ou loja, que solicita cadastro ou acesso com credenciais existentes (Figura 06). Quando isso ocorre, dados de login da vítima são visualizados e roubados. É apresentado também com a variação *Vishing*, no qual o ataque é conduzido por ligações de voz.
Spear phishing	O termo deriva do inglês pesca de arpão (*spear fishing*), pois é um ataque semelhante ao *phishing*, porém direcionado a alvos maiores. Ou seja, busca obter dados de grupos específicos (organizações). Esse tipo de ataque utiliza e-mails ou mensagens personalizadas, criadas com dados e informações exatos e próximos da realidade dos alvos, com características críveis para suas vítimas. Objetivam, assim, enganar funcionários em sua rotina de trabalho, fazendo-os enviarem informações confidenciais ou executarem programas maliciosos. Um exemplo de *spear phishing* pode ser visualizado na Figura 07.
Quid pro quo	Traduzido do italiano "tomar uma coisa por outra", envolve a oferta de falsos serviços prestados pelo atacante, como um atendimento de suporte em TI gratuito, bastando que a possível vítima desative o seu software antivírus. Dessa maneira o criminoso passa a ter controle do computador, podendo executar e instalar diversos programas e rotinas maliciosos.
Baiting	O modo de ataque pelo baiting ocorre, pela prática de despertar a curiosidade ou ganância da vítima. São oferecidos downloads gratuitos de programas, músicas, filmes dentre outros conteúdos em troca da instalação de programas ou do fornecimento de credenciais de acesso a um site.

Fonte: Elaborado pelo autor (2022), com base em Hadnagy (2018) e Lohani (2019).

Segundo Mamedova *et al*. (2019) cresce o interesse de especialistas de segurança digital na ES, com vias à criação de técnicas e estratégias de defesa contra ameaças baseadas nesta área de conhecimento. Kevin Mitnick, criador do termo Engenharia Social, afirma que a ES auxilia o atacante a conseguir dados e informações, bem como acesso a sistemas sem que seja necessário enfrentar contramedidas técnicas de segurança cada vez mais sofisticadas. Exemplos dessas contramedidas são os *firewalls*, software antivírus e sistemas anti-intrusão. Mitnick descreve ainda a utilidade da ES aos criminosos da seguinte maneira: "Em tantos anos, o que eu mais percebi ser verdadeiro é que é mais fácil manipular pessoas do que a tecnologia" (BBC, 2002, p. 1).

Autores como Lohani (2019) e Mamedova *et al*. (2019) descrevem as técnicas que baseiam os ataques de Engenharia Social como ferramentas para *hackear*, ou figurativamente acessar a mente humana e coletar dados pessoais. Os criminosos abordam as vítimas e escolhem uma das técnicas listadas no Quadro 02, e exemplos de sua aplicação estão ilustradas nas figuras 06, que se refere à técnica de *phishing* e 07, que diz respeito ao *spear phishing*.

A Figura 06 exibe um exemplo de website fraudulento exibindo uma falsa oferta visando a coleta de dados pessoais que podem ser utilizados pelos criminosos, como dados de cartão de crédito, números de documentos e senhas. Essas informações serão capturadas pelo criminoso, e posteriormente utilizadas para outras transações financeiras ou vendidas.

Figura 06 – Exemplo de técnica de *phishing*, em website desenvolvido para coletar dados pessoais.

Fonte: Código Fonte (2018).

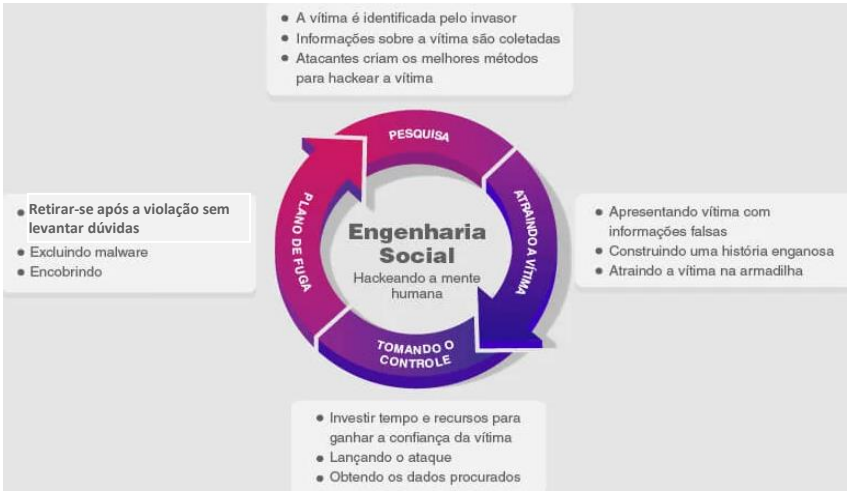
A Figura 07 expõe uma mensagem fraudulenta, tipicamente utilizada em ataques aplicados baseados na técnica de *spear phishing*. O criminoso, após a coleta de informações sobre os alvos, envia e-mails personalizados às vítimas. Anexos contendo programas maliciosos ou links para websites falsos são utilizados para perpetrar a coleta de dados, além de proporcionarem a invasão do sistema por meio da abertura de brechas de segurança.

Figura 07 – Exemplo de técnica de *spear phishing*, aplicada por meio de mensagem de e-mail.

Fonte: PSafe (2021).

Já o ciclo genérico de ataques desenvolvidos com base na ES pode ser verificado no esquema exposto na Figura 08.

Figura 08 – Ciclo de ataques baseados em Engenharia Social.



Fonte: Adaptado pelo autor (2022), com base em SafetyDetectives (2022).

Ataques baseados em Engenharia Social buscam inicialmente informações sobre a vítima, com o objetivo de customizar a abordagem e conseguir sua atenção. A partir disso, são apresentadas mais informações falsas que tendem à construção de uma história enganosa, para atrair a vítima e obter sua confiança. Alcançado esse estágio, o criminoso passa obter os dados pessoais da vítima, usualmente por meio do envio de mensagens de texto fraudulentas, envio de e-mails com anexos maliciosos ou de ligações telefônicas (HADNAGY, 2018; SAFETYDETECTIVES, 2022).

Expostas as principais ameaças às quais os usuários e organizações estão sujeitos, são apresentadas boas práticas em proteção à informação que auxiliam na utilização mais segura de dispositivos digitais.

2.1.3. Boas práticas em SI que reduzem riscos e evitam ameaças

Boas práticas em segurança da informação consistem na utilização de dispositivos digitais de maneira segura, de forma recomendada por especialistas. Buscam evitar que as ameaças à SI não obtenham sucesso, e que os riscos à integridade, confidencialidade disponibilidade a dados e informações sejam reduzidos (CSIRO, 2018). Com base em Green e Dorey (2016) e Whitman e Mattord (2017), exemplos de medidas nesse sentido são:

- Verificar a existência de software antivírus nos dispositivos que utilizam no ambiente de rede da organização, e se estes estão atualizados;
- Utilização de senhas intransferíveis, diferentes e complexas para cada serviço, a exemplo de contas de e-mail, redes sociais, bancos, e sites de compra.
- A notificação da equipe de TI em caso da presença de software desatualizado no computador, smartphone, tablet ou qualquer outro dispositivo utilizado no ambiente de rede da organização;
- Utilização de áreas de *backup* fornecidas pela organização em seu ambiente de rede, ou em dispositivos ou outros locais seguros protegidos por senha, como discos rígidos externos e serviços de nuvem;
- Não execução de programas de origem desconhecida nem anexos de mensagens de e-mail sem certificação de sua procedência;
- Proteção de dispositivos com senha e manter conexões sem fio desligadas quando não estiverem em uso;

- Evitar o acesso a redes públicas, a exemplo das oferecidas em hotéis e aeroportos. Em caso de urgência, evitar a digitação de dados sigilosos ou senhas em aplicativos/websites de bancos ou sites de compras.

O aumento das ameaças à SI das organizações, o crescimento do interesse da sociedade em boas práticas de gerenciamento de dados pelas empresas e a aprovação da LGPD, em 2020, estruturam um contexto em que são mais importantes que medidas sejam tomadas por gestores. Algumas práticas são citadas como fundamentais às organizações para a proteção de seus ambientes, a exemplo de (MASUCH ET AL., 2021; FBI, 2023):

- O correto dimensionamento e implementação de tecnologias, como software de segurança (antivírus e *firewall*) e equipamentos modernos e atualizados;
- A manutenção da força de trabalho tecnicamente atualizada, treinada de acordo com boas práticas em proteção à informação e comprometida com os objetivos da SI na organização;
- Exemplo dos gestores na utilização segura de dispositivos e sistemas no ambiente da organização, o que motiva a equipe a fazer o mesmo;
- A definição de políticas claras, com regras para a utilização de dispositivos e serviços. Exemplos são políticas de senhas, de classificação da informação quanto à sua confidencialidade, *backup*, responsabilização em caso de mau uso e controle de acesso a websites;
- A disponibilização de equipe de suporte técnico acessível, tecnicamente atualizada e comprometida com os objetivos da SI na organização.

De acordo com o exposto até aqui, os sêniores são apontados como vítimas mais comuns das ameaças em SI, sendo recomendado pela literatura que sejam o principal alvo das políticas de segurança das organizações (LLORENTE-BARROSO ET AL., 2018; FRIK ET AL., 2019). Justifica-se essa percepção pela possessão de características particulares relacionadas ao envelhecimento humano, que afetam sua relação com a tecnologia. Essas características serão abordadas na sequência (HADNAGY, 2018; SAFETYDETECTIVES, 2022).

2.2. Idade avançada e tecnologias digitais

Para Thompson e Mayhorn (2012), tecnologias digitais têm potencial para impulsionar ou criar obstáculos a indivíduos sêniores, tanto em relação a digitalização de atividades cotidianas quanto à inserção em mercados de trabalho cada vez mais digitalizados. Embora as tecnologias digitais favoreçam a acessibilidade a grupos com limitações físicas e mentais, trazem consigo a necessidade de adequação técnica para sua utilização, o que tende a estabelecer desafios a serem sobrepostos para sua adequada utilização.

Segundo Dias (2012), o processo de adaptação dos sêniores à implementação de tecnologias digitais é afetado pela interferência de conhecimentos anteriormente adquiridos em suas vidas, como a ausência de treinamentos desde a infância e o costume à utilização de outras ferramentas para a execução de atividades diárias. Dito isso, domínios populacionais que apresentem déficit de conhecimento tecnológico tendem a ter sua relevância profissional reduzida, conforme Adamczyk e Betlej (2020) que citam tais competências técnicas necessárias para o processo de adaptação à utilização de tecnologias de informação, que se tornaram parte importante da vida das pessoas e das organizações.

Ainda de acordo com os argumentos das autoras, o afastamento à utilização de dispositivos digitais em atividades cotidianas tende a ser proporcional à faixa etária do indivíduo. Ou seja, quanto mais velha a pessoa, menor é a sua sensação de autoeficácia e

interesse em utilizar smartphones, computadores e outros aparelhos conectados à internet. Adicionalmente, apesar do desenvolvimento de aplicativos, websites e dispositivos buscar facilitar a inclusão e utilização pelos usuários, a aceitação no uso das tecnologias digitais enfrenta resistência com maior frequência entre usuários sêniores do que indivíduos mais jovens (ADAMCZYK; BETLEJ, 2020). Li e Luximon (2016) mencionam menor interesse, sensação de aumento de ansiedade e uma menor percepção de autoeficácia como fatores de afastamento dos sêniores à utilização dessas tecnologias.

Para Li e Luximon (2016) a percepção de autoeficácia, ou seja, a percepção que o indivíduo possui sobre sua capacidade de realizar uma tarefa é fator determinante à utilização de dispositivos digitais. A autoeficácia é favorecida pela possessão de conhecimentos técnicos de utilização, sobretudo no tocante a aplicativos e websites de compra e venda de produtos, assim como de serviços bancários. Nesse sentido, adultos mais velhos consideram, segundo os estudos de Farivar *et al*. (2020) e Soh *et al*. (2020), que a adaptação a tecnologias digitais demanda a necessidade de exercer um comportamento diferente do que estão acostumados em suas vidas.

Dias (2012) afirma ainda que, em termos gerais, o organismo se torna menos eficiente com o tempo, e algumas de suas capacidades que declinam nesse processo são a inteligência fluida e o tempo de reação. O termo "inteligência fluida" é oriundo da classificação desenvolvida no campo da psicologia, que define como dois os tipos de inteligência humana: a fluida e a cristalizada. Schelini (2006) associa a primeira à capacidade de lidar com situações pouco ou não dependentes de conhecimentos adquiridos previamente. Tarefas novas ou pouco conhecidas, não executadas de maneira automática são conduzidas pela inteligência fluida. Em outras palavras, representa a capacidade da mente humana de raciocinar corretamente com velocidade em situações não usuais, a exemplo de situações de risco em SI. A inteligência fluida tende a declinar após os 21 anos de idade, devido à gradual degeneração das estruturas biológicas humanas (CATTELL, 1998; CARROLL, 1993).

A inteligência fluida decai com o avanço da idade do indivíduo, e o contrário ocorre com a inteligência cristalizada, que é construída a partir de conhecimentos educacionais e experiências obtidos durante a vida. Através desse prisma, entende-se que quanto maior a idade do indivíduo, maior é sua capacidade de tomada de decisões em situações por ele já vivenciadas, ou que sejam relacionadas a experiências anteriores. A compreensão acerca dos tipos de inteligência humana pode auxiliar no favorecimento da retenção de habilidades e competências necessárias para evitar riscos à segurança da informação, especialmente a camadas sociais mais vulneráveis nesse sentido, a exemplo dos sêniores (SCHELINI, 2006).

Adamczyk e Betlej (2020) mencionam também que os adultos sêniores são mais resistentes a adaptar-se à utilização de novas tecnologias. Meng *et al*. (2019) citam que condições fisiológicas e psicológicas dos mais velhos produzem capacidades cognitivas reduzidas se comparadas às de mais jovens, o que limita a capacidade dessas pessoas de lidarem com tecnologias digitais, que de maneira crescente abarcam ameaças de SI. A Kaspersky (2017) menciona características da usabilidade de dispositivos digitais por parte dos sêniores que os expõem a riscos de SI, como menores taxas de utilização de software antivírus em seus dispositivos e capacidade de memorização de senhas, e uma maior propensão ao compartilhamento de dados com desconhecidos.

Sêniores são descritos ainda como pessoas com mais tempo livre para explorar o mundo on-line e mais com mais dinheiro disponível, por vezes economizados durante sua vida, que os coloca como alvos a ameaças. Outra conclusão da pesquisa da Kaspersky afirma que os usuários sêniores costumam levar mais tempo para perceberem que estão sendo alvos de fraudes cibernéticas do que pessoas de faixas etárias mais jovens. Outrossim, Carlson (2015) observa os mais velhos vêm de uma geração em que negócios e acordos eram conduzidos, muitas vezes, a partir de apenas um aperto de mão, pois foram educados a serem mais corteses e acreditarem

com maior frequência na palavra das pessoas, fazendo com que levem mais tempo a desconfiar de alguma atitude suspeita (CARLSON, 2015; KASPERSKY, 2017).

Outra característica relacionada à idade avançada é observada por Schelini (2006), que considera, assim como Esteves (2014), que um maior grau de escolaridade afeta positivamente a relação do empregado com novas tecnologias. Em contrapartida, segundo o IBGE, 38,4% da população analfabeta do Brasil possui mais que 55 anos de idade, o que representa a maior parcela de analfabetos do país, e que 50% da população dessa faixa etária está ocupada no mercado de trabalho (IBGE, 2019).

Adicionalmente, segundo Friedberg (2001), aproximação da aposentadoria desestimula sêniores a fazerem investimentos de tempo e recursos financeiros em treinamentos, que tendem a incrementar suas habilidades com vias a uma utilização de maneira mais segura computadores e outros dispositivos digitais. De acordo com o autor, para os trabalhadores mais velhos e às empresas nas quais estas pessoas trabalham, por vezes não haverá tempo hábil para o investimento ser recuperado em sua vida profissional, uma vez que lhes resta reduzido tempo de serviço em comparação com indivíduos mais jovens.

Autores como Haeussinger (2017) e ISO (2022) consideram que a ausência de treinamentos desfavorece a retenção de conhecimentos pelos sêniores, reduzindo sua capacidade de conscientizar-se das ameaças à segurança da informação e da necessidade de proteger os dados e informações que utilizam diariamente, tanto em ambientes privados como nas organizações. No que diz respeito a programas de qualificação de empregados, considera-se favorável à organização buscar a conscientizar em SI sua força de trabalho, sobretudo quando em caso de sêniores em atividade (FRIK ET AL., 2019; FBI, 2023). Dito isto, será abordado na sequência, o conceito da CSI e seus aspectos.

2.3. Conscientização em Segurança da Informação

O termo conscientização pode assumir diferentes significados, dependendo do prisma observado. Usualmente, a interpretação básica conduz a algo que ocorre na mente de alguém, prestando atenção a certas questões, o saber e compreender determinada coisa ou situação. De maneira similar, o dicionário Michaelis (2004) especifica conscientização e o estado de estar consciente da seguinte maneira:

- **Conscientização** – substantivo: o fato ou estado de estar atento, ou consciente, especialmente a assuntos que são relevantes;
- **Consciente** – adjetivo: (usualmente consciente de algo ou alguém) Ato ou efeito de conscientizar-se;

Em relação à segurança da informação, não se estabelece definição universal na literatura especializada, o que pode ser explicado pela natureza informal e socialmente construída, segundo Tsohou *et al*. (2008). Nesse ínterim, alguns conceitos podem ser citados com diferentes níveis de cobertura aos aspectos da SI, a saber: os cognitivos, comportamentais e de processos. Para que se estabeleça visualização desse cenário foi criado o Quadro 03, que expõe as definições desenvolvidas por diferentes autores, e os aspectos da segurança da informação que se relacionam com cada definição.

Quadro 03 – Definições da conscientização em SI.

Autor(es)	Definição	Aspectos da CSI		
		COG.	COMP.	PROC.
Spears e Barki (2010)	Conscientização que os usuários demonstram sobre políticas organizacionais, procedimentos e a necessidade de proteger informações sensíveis.	x	x	
Banerjee *et al*. (2013)	Conhecimento que membros de uma organização possuem acerca da proteção da informação na organização.	x		
Haeussinger (2017)	Estado mental do usuário de tecnologias digitais, caracterizado pelo reconhecimento e compreensão de riscos e ameaças à segurança da informação, bem como seus objetivos. Possuir conhecimentos necessários para utilizar sistemas de informação de maneira responsável.	x		
ISO (2022)	Programas de conscientização em SI buscam focar atenção em segurança, permitindo que usuários de TI reconheçam ameaças em segurança da informação e respondam adequadamente.	x	x	x

Fonte: Elaborado pelo autor (2022).

Serão abordados, na sequência, os conceitos relacionados aos diferentes aspectos da conscientização em SI citados pelos autores.

2.3.1. Aspectos cognitivos

O dicionário Michaelis (2004) define cognição da seguinte maneira:

> Cognição – substantivo: 1 - Ato ou efeito de conhecer. 2- Conjunto de processos mentais conscientes que se baseiam em experiências sensoriais, pensamentos, representações e recordações (DICIONÁRIO MICHAELIS, 2004).

Relacionando-se ao ato de conhecer ou obter conhecimento, a definição de conscientização no âmbito da SI encontra-se mais frequentemente baseada em aspectos cognitivos, conforme pode ser visualizado no Quadro 03. Segundo Haeussinger (2017), a CSI é definida como um estado mental do usuário, caracterizado pelo reconhecimento e compreensão de riscos e ameaças à segurança da informação, bem como a ciência acerca de boas práticas de defesa. Dito isto, o alcance o estado de conscientização em SI perpassa a possessão de conhecimentos que auxiliem o indivíduo a utilizar dispositivos digitais de maneira adequada, com boas práticas de proteção dos dados e informações (HAEUSSINGER, 2017).

Banerjee *et al*. (2013) trazem uma compreensão da CSI ao âmbito organizacional, definindo-a como o conhecimento que membros de uma organização possuem no tocante à proteção de seus dados e informações. Para Spears e Barki (2010) a CSI se refere a aspectos cognitivos, relacionados a maneiras de como proteger ativos informacionais sensíveis. Em outras palavras, os aspectos cognitivos se referem saber o que proteger, como proteger e por que proteger, sobretudo quando operando dados e informações em ambientes organizacionais.

2.3.2. Aspectos comportamentais

Conforme verificado no Quadro 03, as definições descrevem a CSI como o exercício de um comportamento de observância, ou *compliance*, à SI. Assim, o conceito compreende a tomada de ações de resposta ou prevenção às ameaças em segurança da informação de acordo com as regras definidas pela organização, uma atitude de comprometimento com os objetivos e metas da gestão de SI (ISO, 2022). Hellqvist *et al*. (2013) mencionam o conhecimento e o cumprimento de políticas de proteção à informação como sendo pré-requisitos para o alcance de uma atitude consciente em relação à segurança da informação.

As supracitadas definições de conscientização em segurança da informação lançam luz à relação estreita entre dois de seus aspectos: os cognitivos e os comportamentais. Isto é, faz-se necessário possuir conhecimentos técnicos acerca da utilização dos dispositivos para que sejam percebidas ameaças em SI, permitindo que uma atitude, ou comportamento de acordo com as boas práticas em segurança da informação seja exercido (HAEUSSINGER, 2017).

2.3.3. Aspectos de processos

A terceira dimensão componente da CSI é baseada na percepção de que tal conscientização não é apenas um estado mental cognitivo, ou um comportamento em relação à segurança da informação. É, sim, descrita como o produto de processos desenvolvidos pela organização (HAEUSSINGER, 2017).

O investimento de muitas organizações em treinamento de empregados e na aquisição de ferramentas técnicas cada vez mais sensíveis em detectar e bloquear ameaças à SI, a exemplo de *firewalls*, atualizações para correção de falhas e software antivírus, não é acompanhada pela conscientização dos usuários que manipulam dados e informações existentes no ambiente da organização. Com efeito, cresce a quantidade de evidências a sugerir que vulnerabilidades humanas são cada vez mais utilizadas como forma de acesso a informações e redes não autorizados (KASPERSKY, 2017; FBI, 2023).

Em outras palavras, tem se tornado mais vantajoso aos *hackers* e outros criminosos do mundo digital – até pelo avanço no uso de técnicas da já citada ES – convencer os próprios usuários que abram portas e janelas digitais, ou "caminhos" para seu acesso, do que tentar contornar sistemas de defesa cada vez mais avançados. Esses caminhos podem se referir à execução de anexos maliciosos em e-mails (que por vezes abrem portas de acesso a invasores), fraudes perpetradas por telefone e aplicativos de mensagens ou sites falsos, nos quais o usuário pode digitar seus dados pessoais (ERNST AND YOUNG, 2021, p. 15).

Em resumo, a situação dos profissionais de segurança da informação de organizações, em face das técnicas utilizadas pelos criminosos para explorar vulnerabilidades causadas por usuários, pode ser ilustrado pela Figura 09 (GREEN; DOREY, 2016; ERNST AND YOUNG, 2021).

Figura 2 – Expectativa *versus* realidade da cibersegurança atual.

Fonte: Elaborado pelo autor (2022).

Processos conduzidos por organizações para desenvolver a CSI em empregados dizem respeito à implementação de políticas de segurança, a exemplo do requerimento de trocas de senhas periódicas para acesso a seus sistemas, limitação de acesso a websites maliciosos, treinamentos, lembretes de procedimentos seguros enviados por e-mail, dentre outros. Observa-se que a ausência de processos como esses reduzem o engajamento da força de trabalho aos objetivos da SI na organização, reduzindo a eficiência de recursos investidos. Falhas de segurança continuam a ocorrer, algumas com sérias consequências às organizações (BONNER, 2012).

Autores citam algumas razões que favorecem a ocorrência de tais falhas, a exemplo de problemas na usabilidade de sistemas de informação, decisões equivocadas acerca dos riscos e limitações à tolerância dos humanos em cumprir instruções. Nesse sentido, compreender o processo de organização do pensamento e conhecimento, que embasam a tomada de decisão dos usuários torna-se oportuno a organizações, possibilitando um maior conhecimento acerca dos empregados. Adicionalmente, favorece o desenvolvimento de políticas que incrementem a autoeficácia e inclusão tecnológica dos sêniores, aumentando a capacidade desses usuários de exercerem um comportamento mais seguro (GREEN; DOREY, 2016).

Uma vez que o presente estudo busca compreender as percepções dos empregados sêniores da EMDAGRO nos aspectos da conscientização em SI, recorreu-se ao conceito de mapas mentais para a organização e exposição gráfica do pensamento e conhecimento dos usuários acerca desses aspectos. Dito isto, serão abordadas, na sequência, as definições acerca do tema.

2.4. Mapas mentais

Segundo Buzan (2019), mapas mentais atuam como ferramentas para potencializar a criatividade humana, pois aproveita ideias criativas do cérebro por ajudar a organizá-las. Dito isto, podem ser entendidos como processos gráficos de organização de conteúdos e do pensamento, permitindo a concatenação de várias ideias visualmente em um mesmo espaço. Telas de computador e folhas de papel podem ser utilizadas com esse fim, e mapas mentais são aplicáveis para elaborar planejamentos, ajudar na comunicação com outras pessoas ou organizar o raciocínio (SILVA, 2010).

Mapas mentais são iniciados a partir de uma ideia central que pode ser representada graficamente, por meio de desenhos ou gravuras. Para Ontoria Peña *et al*. (2004), do ponto de vista técnico, é uma estrutura gráfica que busca trabalhar de maneira semelhante ao cérebro no processamento da informação, utilizando para isso a combinação de formas, cores e desenhos. Já Belluzzo (2007) considera que esses mapas são considerados como ferramentas que auxiliam na exposição de relações temáticas e causais, servindo assim como referência para tomadas de decisão. A Figura 10 ilustra o conceito, expondo um mapa mental relacionado ao movimento do realismo.

Figura 10 – Exemplo de mapa mental, representando o movimento do realismo.

Fonte: Elaborado pelo autor (2023).

Observa-se, de acordo com a Figura 10, que mapas mentais agrupam e concatenam palavras e ideias relacionadas, ramificadas hierarquicamente a partir de uma ideia central, maior, que usualmente está centralizada. No exemplo citado, percebe-se que a ideia central é o realismo, e dela se ramificam ideias como seu início, características, o aspecto da denúncia social, dentre outras. A partir dessas ramificações, são expostos elementos que a elas se relacionam e que mantém ligação com a ideia central, ou realismo. Isto é, a partir da ideia central surgem pensamentos acerca do início do movimento realista: o local e ano em que se deu e o nome e temática de sua obra seminal.

É percebido por autores como Belluzo (2007) e Buzan (2019) que os mapas mentais são de valiosa ajuda como organizadores de elementos que influenciam processos de tomada de decisão. Conforme Kraisig e Braibante (2017), esse motivo faz com que mapas mentais sejam utilizados em pesquisas qualitativas, inclusive em ciências sociais e na área da educação.

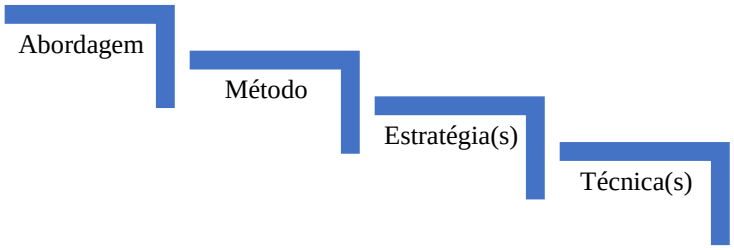
Com efeito, recorreu-se ao recurso na presente pesquisa para auxílio à exposição gráfica da percepção dos usuários acerca dos aspectos componentes da CSI, colocado em prática aqui pela criação de mapas mentais dos participantes, à medida que os aspectos eram citados. Os temas mencionados foram inseridos como ideias concatenadas ao aspecto referido, servindo como ponto de partida para a inserção da percepção do participante acerca do tema. Buscou-se, assim, sintetizar graficamente a percepção dos sêniores da empresa sobre os aspectos da conscientização em SI.

Finalizada a apresentação dos temas relacionados à base teórica da presente dissertação, segue-se à exposição dos procedimentos metodológicos que nortearam o estudo.

3. PROCEDIMENTOS METODOLÓGICOS

Neste capítulo são apresentadas e explicadas as escolhas de procedimentos metodológicos que foram utilizados para a condução da pesquisa, visando atender seus objetivos. O conhecimento foi construído seguindo com a sequência lógica exposta na Figura 11, visualizada abaixo.

Figura 11 – Esquema de pesquisa.



Fonte: Elaborado pelo autor (2022).

3.1. Abordagem da pesquisa

Buscando coerência com as necessidades do estudo, recorreu-se à literatura para exame dos tipos de abordagem de pesquisa disponíveis. Após análise, a investigação em tela apresenta traços descritivos, pois buscou expor características de uma determinada população. Pretendeu também proporcionar a obtenção de conhecimentos aprofundados sobre a percepção dessa população acerca de um fenômeno ou de sua realidade. Cervo e Bervian (1996) afirmam que pesquisas descritivas viabilizam extensa compreensão sobre aspectos do comportamento humano, sejam eles relacionados a indivíduos particulares ou quando organizados em grupos.

A pesquisa assumiu ainda características exploratórias, em virtude de sua intenção de investigar um tema pouco aprofundado, de reduzido conhecimento sistematizado disponível. Segundo Hair Jr. *et al*. (2007), pesquisas exploratórias tendem a orientar a descoberta de um fenômeno, pois o conhecimento que se dispõe acerca do tema é incipiente. Dado o objetivo geral da pesquisa, pode-se afirmar que o estudo se enquadra também nesse viés pelo interesse na obtenção de mais conhecimentos em um tema pouco explorado pela comunidade científica. Adicionalmente, a pesquisa buscou desenvolver ideias para investigação, sobretudo em futuras pesquisas quantitativas que objetivem maior compreensão sobre as particularidades da relação dos sêniores com a segurança da informação. Dessa maneira, indícios relacionados a fatores de afastamento dos sêniores às melhores práticas de segurança da informação advindos dos achados da pesquisa podem contribuir para o desenvolvimento de teorias relacionadas ao tema (VOSS ET AL., 2002).

3.2. Método de pesquisa

No que se refere à definição do método de pesquisa, compreendido como o conjunto de técnicas utilizadas para abordar o problema, três deles são descritos na literatura com esse fim: qualitativos, quantitativos e mistos, que compreendem a junção dos dois padrões anteriores (FLICK, 2009). Métodos qualitativos analisam os processos que não são medidos empiricamente em termos de quantidade, regularidade e frequência. Em contrapartida, um aspecto importante desse tipo de método é que eles contemplam perspectivas enxergadas nas realidades de cada sujeito em sua diversidade, possuindo ainda uma extensa variedade de estratégias para a coleta de dados (FLICK, 2009). Para Liebscher (1998), o método qualitativo

é usualmente utilizado em pesquisas exploratórias, pois possibilita estratégias de coleta de dados de caráter narrativo, a exemplo de entrevistas e observações. Os objetivos da pesquisa foram assim abordados de maneira qualitativa, pois se considerou adequado o uso de um método qualitativo em face do paradigma interpretativista da pesquisa em tela, que é motivada pelo interesse de se buscarem informações profundas acerca da relação dos empregados sêniores da organização estudada com a segurança da informação.

Ainda discutindo premissas ontológicas e epistemológicas do estudo, Walsham (2006) considera que pesquisas interpretativistas buscam investigar pessoas em seus contextos sociais, propondo um diálogo entre campo e teoria, por meio do qual surgem reflexões e teorizações. Já Chua e Myers (2017) afirmam que estudos interpretativistas assimilam de maneira de subjetiva também as relações entre pessoas e tecnologias. Sob esse prisma, mesmo em se tratando de objetos de pesquisa que envolvam a utilização de dispositivos tecnológicos a exemplo de sistemas de informação, tais objetos não devem ser compreendidos estritamente de maneira técnica ou positivista, e sim como fenômenos sociais a serem interpretados (WALSHAM, 2006).

A escolha do método qualitativo perpassa também a consideração do contexto de presença maciça de sêniores da empresa estudada, inclusive em posições de gestão. Buscou-se assim obter conhecimentos sobre as percepções e hábitos desses empregados, o que também tende a influenciar a própria visão do pesquisador e da organização sobre aquela realidade, além de contribuir à construção de conhecimentos concernentes ao tema.

Por último, outra razão para a escolha da abordagem qualitativa é que o tema de pesquisa é relativamente novo e não foi possível encontrar, em bases científicas como o *Google Scholar*, *Web of Science* e SCIELO, pesquisas que contemplassem a investigação da relação de empregados sêniores com a segurança da informação, e dos fatores de afastamento desses empregados às melhores práticas em SI. Dito isto, a execução de uma pesquisa qualitativa pode ser considerada apropriada nesse contexto, permitindo a descrição e exploração do fenômeno antes que este possa ser quantificado (HAIR JR. ET AL., 2007).

3.3 Estratégia de pesquisa

A etapa de exposição do processo de seleção da estratégia de investigação diz respeito à forma como foram conduzidos os procedimentos em campo (CRESWELL, 2010). As possibilidades de estratégia são descritas por Yin (2019): experimento, levantamento (*survey*), análise de arquivo, pesquisa histórica e estudo de caso. É comum que o pesquisador se questione acerca da ocasião adequada para a utilização de cada estratégia, baseada na consideração de três condições básicas: o tipo de questão de pesquisa, o controle sobre o evento do objeto de estudo e o foco nos acontecimentos históricos em oposição aos contemporâneos. O Quadro 04 expõe como as principais estratégias de pesquisa interagem às mencionadas condições de escolha.

Quadro 04 - Situações relevantes para diferentes tipos de pesquisa.

Estratégia	Forma da questão	Exige controle sobre eventos comportamentais	Focaliza acontecimentos contemporâneos
Experimento	Como, por quê	Sim	Sim
Levantamento	Quem, o quê, onde, quantos, quanto	Não	Sim
Análise de arquivo	Quem, o quê, onde, quantos, quanto	Não	Sim/Não
Pesquisa histórica	Como, por quê	Não	Não
Estudo de caso	Como, por quê	Não	Sim

Fonte: Elaborado pelo autor, adaptado de Yin (2019).

Dito isto, estudos de caso se apresentam como escolha adequada quando a questão problematizadora da pesquisa se inicia com os termos como ou por quê. O mesmo ocorre quando o pesquisador não detém controle sobre os eventos investigados, e esses surgem de maneira contemporânea. Yin (2019) ainda menciona que pesquisas levadas a cabo em situações contextuais que incluem política, sociologia e estudos organizacionais e gerenciais comportam - e normalmente os utilizam - estudos de caso como estratégia de pesquisa. Logo, o fato de que o presente estudo se baseou em uma questão problematizadora iniciada com termos do tipo como ou por quê foi o primeiro aspecto considerado na escolha da estratégia de estudo de caso.

Outro fator determinante para a escolha foi o objetivo da pesquisa em adquirir conhecimentos "mediante mergulho profundo e exaustivo em um objeto delimitado, possibilitando uma penetração em uma realidade social não conseguida plenamente por levantamento amostrado e avaliação exclusivamente quantitativa" (MARTINS, 2008, p.11). No contexto da pesquisa, estudos de caso qualitativos possibilitam que se compreendam, de maneira adequada e abrangente, características da percepção dos sêniores da organização pesquisada acerca dos aspectos da conscientização segurança da informação, investigadas no desenrolar suas de atividades diárias. Contemplam-se, assim, as duas condições expostas no Quadro 04, referentes à ausência de controle do pesquisador dos eventos investigados e ao foco em acontecimentos contemporâneos.

Estudos de caso são ainda empreendidos com diferentes finalidades, a exemplo da exploração de um fenômeno para o desenvolvimento de ideias e hipóteses, além da construção, teste e aperfeiçoamento de teorias mediante casos contundentes e seu posterior uso para validar resultados empíricos (VOSS ET AL., 2002). Nesse respeito, o estudo empreendido lança olhar à percepção dos sêniores sobre a segurança da informação em um ambiente organizacional, trazendo em consideração o observado pela literatura de que essas pessoas são especialmente vulneráveis a ameaças (KASPERSKY, 2017; FBI, 2023).

Com efeito, Alves-Mazzotti (2006) considera que estudos de caso norteiam investigações em uma unidade específica, idealmente selecionada mediante critérios predeterminados, definidos pelo pesquisador. Convém que tais critérios sejam explícitos para a seleção do caso, ou seja, que exista uma situação específica, complexa e/ou intrigante, relevante para a justificação do esforço de compreensão mediante mergulho profundo e exaustivo, levado a cabo mediante a utilização de múltiplas fontes de dados. Permite-se, assim, uma visão mais abrangente do fenômeno e que se alcancem os objetivos pretendidos.

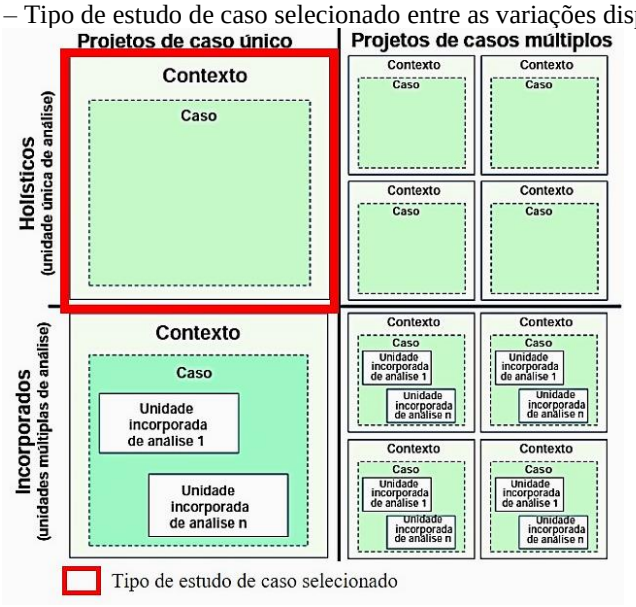
No contexto do estudo executado, os critérios escolhidos para a estratégia de pesquisa foram os seguintes:

- A organização pesquisada possui um número elevado de sêniores em relação ao total de empregados (70% da força de trabalho da empresa);
- Sêniores da organização apresentam dificuldades na utilização de tecnologias digitais, gerando incidentes de segurança e constantes demandas à equipe de suporte em informática;
- O pesquisador é empregado do setor de informática da empresa, o que permite a utilização da observação no ambiente da organização como procedimento de coleta de dados adicional, possibilitando uma visão mais abrangente do fenômeno estudado.

Uma vez que os critérios acima retratam o cenário encontrado na organização, avaliou-se que a estratégia de estudo de caso é oportuna ao atendimento dos objetivos da pesquisa. No que se refere à escolha entre os variados tipos de estudos de caso, duas dimensões precisam ser consideradas (YIN, 2019): o número de casos observados e a natureza da pesquisa. Acerca da primeira, apenas um contexto (EMDAGRO) contendo apenas um caso (empregados sêniores)

foi definido como objeto de estudo. No que se refere à natureza da pesquisa, definiu-se que dentre estudos de caso holísticos ou incorporados, classifica-se como holística, uma vez que se selecionou apenas uma unidade de análise: empregados sêniores da própria organização. Essa definição da pesquisa pode ser visualizada na Figura 15.

Figura 12 – Tipo de estudo de caso selecionado entre as variações disponíveis.



Fonte: Elaborado pelo autor, com base em Yin (2019).

Parte-se agora à exposição de detalhes acerca do caso escolhido.

3.3.1. O caso selecionado

O estudo foi empreendido em uma empresa pública sergipana: a EMDAGRO (Empresa de Desenvolvimento Agropecuário de Sergipe), escolhida em virtude da elevada faixa etária média de sua força de trabalho, pois 70% de seus empregados tem 55 anos ou mais (TRANSPARÊNCIA SERGIPE, 2023). Outros pontos a serem destacados no ambiente escolhido é que muitos sêniores apresentam dificuldades na utilização de tecnologias digitais, cenário observado e registrado em 03 dos 04 scripts de observação anexados a essa pesquisa. Não se verificam na organização, também, processos de estímulo à qualificação em segurança da informação.

Apesar de que se recomendem estudos de casos múltiplos para maior qualidade e confiabilidade, estudos de caso único comportam tentativas de generalização quando possuem características típicas, raras, longitudinais e reveladoras (FREITAS; JABOOUR, 2011; YIN, 2019). Com efeito, acredita-se que as características e critérios apresentados justifiquem a escolha da EMDAGRO como caso único, já que compreende elementos que enquadram em um fenômeno organizacional relevante para o esforço empreendido.

Foram escolhidos participantes com base em princípios de homogeneidade fundamental, que diz respeito à existência de uma característica importante em comum aos participantes. Esse princípio difere da homogeneidade ampla, quando os participantes compartilham vários atributos (MAXWELL, 2005). Considerou-se assim relevante o fator faixa etária dos empregados (possuírem ao menos 55 anos), e serem utilizadores de dispositivos digitais fornecidos pela organização. Intencionou-se selecionar entre 06 e 10 entrevistados nos critérios mencionados e, por fim, a quantidade foi alcançada pelo critério da saturação, obtida a partir da repetição de padrões de respostas acerca dos aspectos da CSI, chegando a 07 entrevistados.

Adicionalmente, buscou-se incluir gestores no grupo de participantes, intencionando a diversificação e representatividade dos usuários. Pretende-se analisar como coordenadores e gerentes da organização estão lidando com a tecnologia digital, pois segundo o observado pela literatura, gestores podem exercer influência em empregados (GARDNER; THOMAS, 2014). Dito isto, o Quadro 05 apresenta características dos entrevistados escolhidos.

Quadro 05 – Perfil dos participantes.

Código	Idade	Função	Ano de Ingresso	Grau de escolaridade	Sexo
E1	68	Assistente administrativo	1977	Nível Técnico	M
E2	69	Gestora de programa de desenvolvimento	1980	Pós-graduação	F
E3	59	Coordenador de Geoprocessamento	1984	Superior completo	M
E4	72	Assessor técnico	1974	Superior completo	M
E5	62	Coordenadora do setor de contabilidade	1977	Pós-graduação	F
E6	61	Supervisora de compras	1984	Ensino Médio completo	F
E7	61	Secretária de Diretor	1985	Ensino Médio completo	F

Fonte: Elaborado pelo autor (2022).

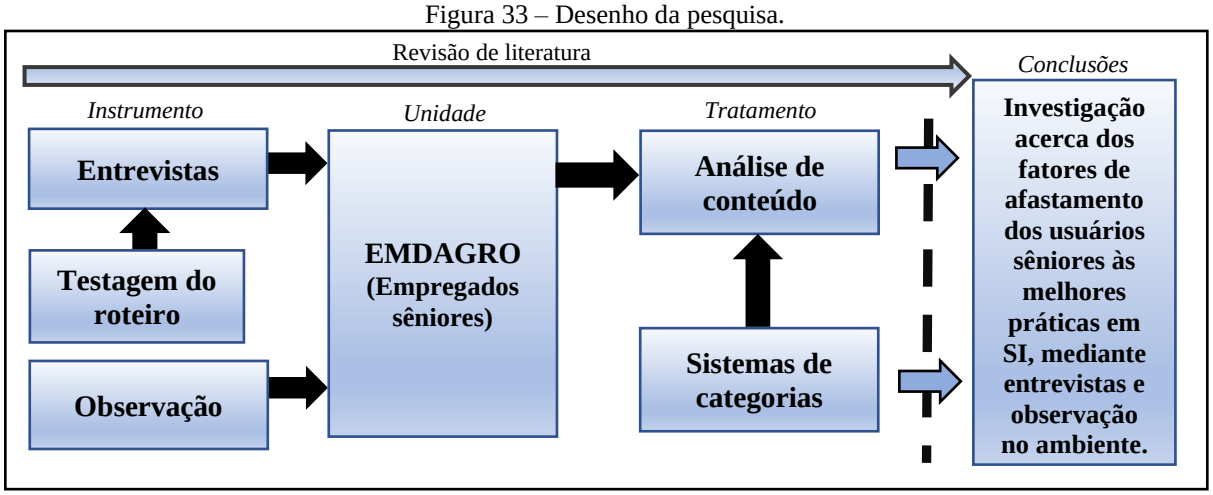
Dentre os participantes escolhidos, 03 são do sexo masculino e 04 do feminino. Assim como na escolha da diversificação relacionada à hierarquia dos empregados selecionados, a proporção do sexo dos participantes também ocorre de maneira deliberada, intencionando adicional diversificação. Verifica-se, ainda, o ano de ingresso dos participantes, além do seu nível de escolaridade. Conforme mencionado anteriormente, buscou-se diversificar o quadro de entrevistados nesses aspectos, observando possíveis vínculos de fatores como a escolaridade e o sexo à percepção dos participantes em relação à segurança da informação. Objetivou-se, assim, o enriquecimento dos resultados da pesquisa.

Estudos de caso também consideram o fator tempo, com as pesquisas assumindo formatos transversais, que retratam a realidade no momento da investigação, ou longitudinais, que observam mudanças em um período de tempo, de acordo com Richardson (1999). O presente estudo assumiu o caráter transversal, uma vez que pretendeu investigar o estado de indivíduos da organização. Pesquisas transversais também comportam a coleta de fontes diretas (ou primárias) ou a partir de fontes secundárias, ambas utilizadas no estudo.

3.2. Desenho da pesquisa

Será apresentado, na Figura 13, o desenho definido da pesquisa. Seu objetivo é tornar visível a sequência lógica das etapas escolhidas para a operacionalização do estudo empreendido.

Figura 33 – Desenho da pesquisa.



Fonte: Elaborado pelo autor (2023).

A partir do planejamento e da definição dos procedimentos metodológicos, partiu-se ao delineamento das categorias e elementos de análise, que forneceram orientação à elaboração do roteiro de entrevistas e dos scripts de observação. Após essa fase, teve lugar a testagem do referido roteiro e, após seus oportunos ajustes à melhor adequação aos objetivos da pesquisa, seguiu-se à aplicação na unidade componente do estudo de caso. O tópico 3.7 apresenta os detalhes da coleta de dados. De acordo com o sistema de categorias definido, foi estabelecida uma análise de conteúdo com inferência dos dados, seguida da discussão dos resultados e das considerações finais do estudo.

3.5. Protocolo do estudo de caso

No intuito de conferir maior confiabilidade à pesquisa, elaborou-se um protocolo de estudo de caso a ser empreendido. Tais protocolos auxiliam o pesquisador por fornecer orientação na condução da estratégia de pesquisa escolhida, segundo Yin (2019). Para o autor, essa ferramenta se faz importante em qualquer estudo levado a campo por meio de estudos de caso, porém se torna imprescindível quando da existência de várias unidades estudadas.

O Quadro 06, exposto em seguida, foi elaborado para nortear a condução da estratégia escolhida.

Quadro 06 – Protocolo do estudo de caso da pesquisa

Visão geral da pesquisa	**Objetivos do estudo de caso**	Investigar aspectos cognitivos e comportamentais dos sêniores em relação à segurança da informação
		Conhecer a percepção dos usuários sêniores a respeito de aspectos de processos realizados na organização
		Elencar e discutir fatores de afastamento dos participantes às melhores práticas de SI
	Ambiente e cenário da pesquisa	EMDAGRO
Procedimentos de campo do protocolo	**Preparação**	Desenvolvimento de script de observação do ambiente
		Elaboração do roteiro de entrevistas
		Testagem do roteiro de entrevistas
		Contato com a organização objeto da pesquisa
	Ação	Observação do ambiente da empresa
		Elaboração dos relatórios de observação do ambiente
		Agendamento das entrevistas
		Realização das entrevistas
		Gravação das entrevistas
		Transcrição das entrevistas
Relatório do estudo de caso	**Resultados**	Análise individual dos sistemas de categorias
		Caracterização dos sistemas de categorias
		Consolidação dos dados
		Confronto dos dados com os objetivos da pesquisa
	Conclusão	Discussão acerca dos achados da pesquisa
		Direcionamentos futuros

Fonte: Elaborado pelo autor (2022) com base em Sales (2012).

3.6. Categorias de análise

Estão apresentadas, na sequência, as categorias de análise pré-definidas para norteamento da etapa de coleta dos dados, e de sua posterior discussão. Para isso, foram desenvolvidas questões de pesquisa que buscaram auxiliar na resposta ao objetivo geral do estudo, baseadas nos três aspectos da conscientização em segurança da informação que servem

como as categorias da pesquisa, que foram denominadas a partir dos nomes dos mesmos aspectos da CSI. A escolha se deveu ao fato de que o estudo da percepção de usuários de tecnologia a esses aspectos lança luz à fatores de afastamento a boas práticas em SI. Definidas as questões de pesquisa e as categorias, definiram-se os elementos de análise, naturalmente ligados a cada um dos aspectos da CSI.

Detalhando os elementos de análise definidos, podem ser descritos da seguinte maneira: no caso dos relacionados aos cognitivos, referem-se à percepção dos usuários acerca de aspectos técnicos da segurança; os comportamentais dizem respeito à sua atitude prática no cotidiano das atividades da empresa e a preocupação e comprometimento com os objetivos da SI na organização; já os de processos se relacionam à maneira de como os usuários percebem os processos conduzidos pela organização com vias ao desenvolvimento da conscientização nos empregados (HAEUSSINGER, 2017). De maneira sintética, os elementos de análise de cada aspecto da CSI foram delineados buscando trazer achados relacionados a:

- **Cognitivos**: conhecimentos acerca de práticas de *backup*, de gerenciamento de senhas, antivírus, e riscos relacionados às ameaças de segurança;
- **Comportamentais**: comportamento do usuário comprometido aos objetivos da SI na empresa, evitando executar programas desconhecidos ou inserir dados em sites não confiáveis;
- **De processos**: consciência e percepção acerca da importância de políticas conduzidas pela organização, a exemplo da política de senhas e de estímulo ao treinamento. Pode-se referir também à sugestão de melhorias nas práticas de proteção à informação levadas ou não a cabo na empresa.

O resumo da descrição do esquema de categorias, questões de pesquisa norteadoras elementos de análise podem ser visualizados no Quadro 07.

Quadro 07 – Sistemas de categorias pré-definidas para a pesquisa.

SISTEMA: Conscientização em SI			
Categoria	**Descrição**	**Questão de pesquisa**	**Elementos de análise**
COG (Cognitivos)	Descreve um estado mental de reconhecimento e compreensão de riscos e ameaças à SI.	Qual a percepção dos sêniores acerca dos aspectos cognitivos da conscientização em segurança da informação?	- Conhecimento técnico sobre ameaças e seus respectivos riscos; - Conhecimentos acerca de práticas de mitigação de riscos;
COM (Comportamentais)	Descreve o exercício de comportamento de observância à segurança da informação organizacional dos participantes.	Qual a percepção dos sêniores acerca dos aspectos comportamentais da conscientização em segurança da informação?	- Preocupação com possíveis danos à organização; - Busca por informações quando deparados com situações de risco; - Comprometimento aos objetivos da SI na organização.
PRO (de Processos)	Descreve a percepção dos usuários acerca dos processos estabelecidos pela organização a fim de fomentar a CSI nos empregados.	Qual a percepção dos sêniores acerca dos aspectos de processos da conscientização em segurança da informação?	- Percepção acerca de processos que fomentem a SI na organização. - Sugestões de criação/melhoria de processos à organização.

Fonte: Elaborado pelo autor (2022).

Logo, os instrumentos de coleta de dados expostos em seguida foram desenvolvidos para auxiliar na resposta às questões de pesquisa descritas no Quadro 07, dando atenção aos critérios delineados pelos elementos de análise.

3.7. Coleta de dados

Serão apresentados e discutidos aqui os direcionamentos da pesquisa relacionados à definição das ações e instrumentos utilizados para a coleta de dados. Os procedimentos escolhidos foram as entrevistas e a observação, e detalhes acerca de suas características e critérios de escolha são expostos nos subtópicos a seguir.

3.7.1. Entrevistas

As fontes primárias de coleta de dados da pesquisa foram entrevistas qualitativas, orientadas por roteiros semiestruturados (VERGARA, 2005). Creswell (2010) afirma que esse tipo de entrevista busca extrair concepções e pontos de vista dos participantes, permitindo a expressão de opiniões com maior profundidade. A construção do roteiro (apresentado no Apêndice A), foi orientado sistema de categorias apresentado no Quadro 07. Dessa maneira, as entrevistas buscaram conhecer, inicialmente, conhecimentos que os participantes possuem sobre a SI, no que se refere a ameaças e suas respectivas formas de defesa.

Adicionalmente, o comportamento relacionado aos objetivos da SI da organização, de acordo com boas práticas também foi investigado. Por último, foram definidas perguntas para lançar luz à percepção dos entrevistados acerca de processos conduzidos pela organização no tocante ao desenvolvimento de conscientização em SI, a exemplo de políticas de segurança e treinamentos.

As entrevistas envolveram os sujeitos mencionados no tópico 3.3.1, e foram gravadas para maior confiabilidade, com o objetivo de que não se perdessem detalhes porventura importantes à análise, a exemplo de demonstrações de hesitação, firmeza ou espontaneidade. Foi solicitado aos participantes que se pudessem fazer anotações durante a realização das conversas. Os indivíduos foram contactados pessoalmente, de maneira individual, momentos nos quais foram definidas e agendadas as datas para a execução das entrevistas, que ocorreram entre os meses de dezembro de 2022 a março de 2023 nas próprias instalações da organização. O tempo de duração variou entre 55 min (E3) e 25 min (E7), sobretudo por diferença do nível de conhecimento e familiaridade com o tema dos participantes. Os encontros começaram com a exposição dos objetivos da pesquisa, seguida da declaração de que a gestão da organização não estava envolvida no projeto.

Dito isto, assim que as conversas eram finalizadas, foram transcritas, salvas em formato eletrônico .doc e inseridas como fontes (unidades de registro) no software Nvivo, versão 10 para posterior tratamento e análise. O procedimento foi adotado com o objetivo de evitar a perda de elementos que foram manifestos durante o processo, a exemplo de expressões faciais e ênfase em algum ponto específico da entrevista. Por fim, foram retornadas suas transcrições aos entrevistados, tanto para possível complementação de informações como para a confirmação de autenticidade/rejeição de interpretações realizadas pelo pesquisador (ZANELLI, 2002).

3.7.2. Observação

Para Queiroz *et al*. (2018), a técnica da observação busca ver, com todos os sentidos, determinada realidade. Os autores afirmam ainda que ao observar ambientes, pessoas, comportamentos e interações cotidianas, torna-se possível aproximar-se do que as pessoas realmente fazem, e, adicionalmente, preenche lacunas que outras técnicas de coleta de dados não são capazes de alcançar, a exemplo das próprias entrevistas.

Marcon e Elsen (2000) consideram que a observação é um procedimento de coleta de dados que tem como característica a facilidade de acesso aos dados pretendidos. O registro da observação é feito no momento em que esta ocorre e pode assumir formas diversas, a exemplo

de anotações, gravações em áudio ou vídeo e fotografias. No caso da presente pesquisa a observação se deu pela presença do pesquisador no ambiente da empresa como técnico da equipe de informática da organização, e participante das atividades como fornecedor de serviços de suporte e consultoria à sua operação.

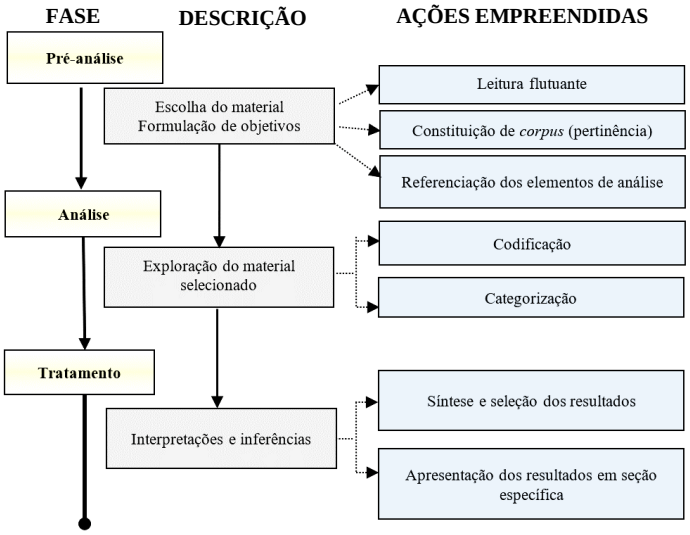
O processo de observação foi registrado em scripts (expostos no Apêndice B), desenvolvidos de acordo com os aspectos da conscientização em segurança da informação. Logo, foram observados os conhecimentos técnicos dos usuários sêniores da organização, seu comportamento exercido no dia a dia da empresa em relação à SI e a maneira que esses empregados percebem os processos conduzidos pela organização. A definição do período de observação é do ano de 2019 até meados de 2023, em virtude da participação do autor da pesquisa no ambiente da organização nesse período.

3.8. Análise dos dados

Uma vez angariados os dados qualitativos, transcritas as entrevistas e desenvolvidos os relatórios de observação, foi empreendida uma análise desses dados com o objetivo de transforma-los de um estado bruto em formatos apropriados ao atendimento aos objetivos da pesquisa. Utilizou-se a análise de conteúdo para apreciação das transcrições das entrevistas e dos relatórios de observação no ambiente da organização.

Acerca da análise de conteúdo, Franco (2008, p. 10) considera que se situa no âmbito epistemológico “apoiado em uma concepção de ciência que reconhece o papel ativo do sujeito na produção do conhecimento”. O método parte essencialmente da mensagem, seja verbal (oral ou escrita), gestual, figurativa, documental ou diretamente provocada. Tais mensagens expressam significados e sentidos, que não podem ser considerados isoladamente, uma vez que as emissões dessas mensagens estão vinculadas às circunstâncias e conjunturas de seus sujeitos produtores. Para Bardin (2009), a matéria-prima da análise de conteúdo compreende a utilização de mensagens oriundas de comunicação verbal, a exemplo de entrevistas e discursos. Esta parte do estudo contemplará as etapas descritas na Figura 14, exposta a seguir:

Figura 14 - Etapas da análise de conteúdo.



Fonte: Elaborado pelo autor (2022), com base em Bardin (2009).

A pré-análise consiste na organização dos trabalhos e materiais a serem executados nas próximas fases, segundo Bardin (2009). No contexto da pesquisa, o escopo de materiais definido foi constituído de relatórios de observação no ambiente da empresa e transcrições das entrevistas com os usuários. Foi executada, inicialmente, uma leitura flutuante do material,

buscando impressões e orientações para etapas restantes da fase. A escolha dos documentos e suas partes relevantes foi baseada em sua pertinência ao atendimento dos objetivos da pesquisa, seguida do recorte e definição dos elementos, ação que finalizou a pré-análise. Segundo Bardin (2009), elementos de análise podem ser palavras, temas, objetos, acontecimentos, personagens, dentre padrões relevantes à temática definida. No caso da pesquisa, referem-se a aspectos relacionados à conscientização em segurança da informação, mencionados pelos participantes nas entrevistas e observados durante as atividades diárias.

Em seguida, foi estabelecida a análise propriamente dita, explorando o material anteriormente selecionado e partindo para a sua codificação. Três etapas foram realizadas nesse momento da pesquisa: a categorização, feita a partir da referência dos elementos de análise baseada na tabela de categorias; o inventário, ou isolamento dos termos comuns; e a classificação, onde foi feita a repartição e organização dos elementos. A técnica de análise de conteúdo foi escolhida para organização dos termos comuns, agrupando menções semelhantes aos elementos de análise, destacando temas relacionados aos três aspectos da CSI.

Conduziu-se também confronto dos dados obtidos nas entrevistas com os dados coletados a partir da observação das atividades, executadas no ambiente da empresa pelos empregados sêniores. O objetivo do uso desse desenho metodológico é a apreensão da realidade da organização por diversos ângulos, possibilitando o confrontamento das informações e a minimização de vieses da utilização de única perspectiva de análise. Os dados referentes à observação estão expostos no Apêndice B, e apresentados ao longo do texto do capítulo de análise de dados.

Finalizada a etapa de análise do material, o tratamento compreendeu a inferência e a interpretação dos resultados da pesquisa, feitos a partir da leitura profunda dos dados obtidos e organizados nas fases anteriores. Os resultados foram sintetizados, e os mais relevantes foram selecionados e apresentados a partir da elaboração de textos, figuras e mapas mentais em seção específica do capítulo de análise de dados. A estrutura do capítulo foi assim definida: os aspectos citados em cada dimensão da CSI foram apresentados e discutidos, em ordem exposta de acordo com sua frequência de citações. A espontaneidade nas respostas e nas atitudes observadas nos scripts de observação também foram levadas em consideração à análise, pois conforme Santiago (1985), indicam mínima manipulação pelo processo racional e tendem a apontar maior familiaridade com o tema discutido.

Ao final do capítulo, os participantes que apresentaram de adesão às práticas recomendadas em SI de frequência igual ou maior que 50% foram agrupados entre os mais conscientes, classificados como Grupo 01. Os demais, que apresentaram adesão menor que 50% a boas práticas, foram assim classificados no Grupo 02, ou usuários menos conscientes. Isso foi feito com vias unicamente ao destaque de fatores de diferenciação de suas percepções. Foram também desenvolvidos mapas mentais genéricos de cada grupo, com o intuito de expor didaticamente como os grupos de participantes percebem cada um dos aspectos da CSI.

Foram assim definidos dois grupos de participantes, que podem ser visualizados no tópico 4.4. Dito isto, a discussão da pesquisa que será exposta na sequência, trazendo a exploração e discussão acerca do material previamente selecionado.

4. ANÁLISE DE DADOS

Este capítulo apresenta e discute os dados coletados na pesquisa. Durante a exposição do texto, partes dos depoimentos obtidos por meio das entrevistas foram citados com o intuito de embasar as análises realizadas, juntamente com dados referentes às observações do autor que são apresentados de acordo com sua relevância. Esta análise de dados está dividida em quatro etapas, delineadas de acordo com os objetivos específicos do estudo. As três primeiras são norteadas por dimensões definidas *a priori* com base nos aspectos da conscientização em segurança da informação.

Dito isto, a primeira etapa apresentará os resultados relativos à percepção dos entrevistados acerca de aspectos técnicos da segurança da informação, sobretudo a capacidade de identificar situações de risco e maneiras de evitá-las. A segunda etapa trará a exposição de dados relacionados aos aspectos comportamentais dos sêniores em relação à segurança da informação, que são constituídos pela soma da percepção de riscos com as ações efetivamente tomadas diante dos mesmos riscos com vias a boas práticas de SI.

A terceira etapa traz dados acerca da percepção dos entrevistados a processos conduzidos pela organização para desenvolver conscientização de segurança da informação em seus empregados. Buscou-se conhecer a percepção dos participantes da pesquisa acerca da eficácia desses processos, se consideram que influenciam o comportamento dos empregados. Também foram investigados processos que os entrevistados consideram contribuir a esse fim, mesmo que não implementados na organização.

Por fim, a quarta etapa apresentará uma discussão acerca dos fatores de afastamento às melhores práticas de proteção à informação observados durante a análise dos aspectos componentes das etapas anteriores. Os usuários participantes serão divididos em dois grupos, de acordo com a frequência com que seus aspectos da CSI se aproximam de boas práticas, e mapas mentais referentes a cada grupo serão apresentados para visualização de suas percepções.

4.1. Aspectos Cognitivos

Apresentam-se aqui os dados referentes aos aspectos cognitivos mencionados principalmente nas respostas dos sêniores às perguntas 01, 02 e 03 do roteiro de entrevistas, juntamente com a observação da utilização de tecnologias digitais no dia a dia da empresa.

4.1.1. Conhecimentos Sobre Proteção à Informação no Ambiente Organizacional

O Quadro 08 expõe aspectos relacionados à dimensão cognitiva mencionados, juntamente com suas frequências de citações e proporções de menções espontâneas.

Quadro 08 – Aspectos cognitivos, aspectos mencionados e respectivas frequências de citações.

Dimensão	Nome do aspecto	Número de citações	Citações espontâneas
Aspectos Cognitivos	Bloqueio do computador ao sair	2	1 (50%)
	Conscientização de colegas	2	1 (50%)
	Hackers e outros criminosos da internet	7	3 (42%)
	Atualizações de software	2	1 (50%)
	Backup	10	3 (30%)
	Antivírus	7	3 (42%)
	Senhas	8	3 (37,5%)
	Baixa autoeficácia, insegurança ou medo	4	3 (75%)
	Websites/aplicativos inseguros/desconhecidos	5	2 (50%)

Fonte: Dados da pesquisa (2023).

O aspecto cognitivo da proteção à informação que mais foi citado foi o *backup*, seguido do gerenciamento de senhas e da preocupação com furto de dados pela ação de cybercriminosos. A definição conceitual dos aspectos e suas bases teóricas serão apresentados no Quadro 09.

Quadro 09 – Definições gerais dos aspectos cognitivos mencionados.

Aspecto cognitivo	Definição	Base teórica
Bloqueio do computador ao sair	Participante menciona a importância de se evitar deixar o computador desbloqueado, evitando acessos indevidos com suas credenciais.	Lohani (2019)
Conscientizar colegas	Entrevistado pensa que se faz necessária a conscientização de colegas, pois crê que há pessoas utilizando dispositivos de maneira insegura.	ISO (2022)
Hackers e outros criminosos da internet	Usuário reconhece riscos de ataques cibernéticos que buscam furto de dados e informações pessoais e da organização.	Hadnagy (2018)
Atualizações	Participante pensa que atualizações de *software* são importantes.	Prawobo; Tjong (2017)
Backup	Entrevistado acredita que *backups* são importantes para evitar perda de dados.	FBI (2023b)
Antivírus	Usuário crê que é necessário instalar/atualizar antivírus para evitar danos/perda/furto de dados e informações.	Masuch *et al*. (2021)
Senhas	Participante pensa que uma gestão de senhas adequada é importante para a proteção à informação.	Masuch *et al*. (2021)
Baixa autoeficácia, insegurança ou medo	Entrevistado acredita que se sentir mais seguro na lida com a tecnologia digital é importante para a proteção à informação.	Mannheim *et al*. (2019)
Websites/aplicativos inseguros/desconhecidos	Participante pensa que se faz necessário checar a legitimidade de websites e aplicativos desconhecidos e potencialmente inseguros antes de fazer o acesso/instalação dos mesmos.	Frik *et al*. (2019)

Fonte: Dados da pesquisa (2023).

Parte-se à análise das menções dos entrevistados, que serão apresentadas pela ordem do número de citações e apresentadas separadamente em subtópicos. Terá assim início com a prática de *backup*, exposta na sequência.

4.1.1.1 *Backup*

Os entrevistados E1 e E3 mencionaram, de forma espontânea, considerar importante possuir cópias de segurança de dados para evitar problemas relacionados à segurança da informação:

> Eu tenho uma pasta que eu trabalho ali, eu tenho um sistema que é de patrimônio que eu não posso deixar liberado. Aí uma pessoa maldosa vem, vai destruir tudo o que eu tenho. E aí? E agora? Se eu não tiver um, se eu não tiver um *backup* de reserva, como é que eu vou recuperar aqueles dados de informação? Tem que existir. (E1)

A importância de *backups* é ressaltada outra vez na resposta à Questão 01 por E1, mencionando que cópias de segurança são fundamentais para ele:

> Voltando um pouco ao *backup*, veja só, eu vejo que você deve ter um *backup* de segurança. Você deve ter mais um, mais um dispositivo de segurança. Caso você venha a perder aquele *backup*, você tem onde recuperar os seus dados daquele *backup* que é o mesmo. Entendeu? (E1).

Já E3 afirma ter tido problemas anteriormente com uma mensagem de e-mail maliciosa que lhe causou a perda de arquivos importantes (usuária executou o anexo contido), e que ter feito um *backup* anteriormente, em mais de uma instância, evitou que maiores transtornos ocorressem:

> Eu faço *backups*, e eu vou dizer agora, na prática, uma coisa que eu senti. Recentemente eu recebi um e-mail com os arquivos de uma empresa que estava executando o trabalho aqui pro Estado. Eu associo o problema que deu ao arquivo que eu recebi e que eu abri. Por exemplo, eu não tive o cuidado de passar antivírus nos arquivos. Eu sei que quando eu baixei as plantas que eu recebi de um trabalho lá de cima, um dia o computador deu uma pane que eu não conseguia acessar nada aqui. Tudo o que os programas que eu abri, Topograph, AutoCAD, não conseguia ser sanado, não conseguia produzir nada, não conseguia salvar nada. O que é que me salvou? O *backup*, o *backup* que eu tinha que eu tinha nos HDs. Então, além da nuvem, eu tenho dois HDs onde eu guardo meus arquivos (E3).

Interessante observar o fato de E3 afirmar possuir *backup* em nuvem, pois relatou que "além da nuvem, eu tenho dois HDs onde eu guardo meus arquivos". Tanto o aspecto da redunância de HDs externos para segurança extra comentados por E1 e E3 quanto o uso de armazenamento em nuvem podem ser ressaltados pela sofisticação técnica, pois não são práticas comuns entre os entrevistados e estão de acordo com o estado da arte de recomendações de proteção à informação (RAO; NAYAK, 2014).

De acordo com a literatura especializada, ameaças à integridade, disponibilidade e confiabilidade de dados e informações são passíveis de serem minimizadas, e até evitadas, com a utilização de *backups*, sobretudo em serviços de nuvem (STEWART ET AL., 2015; WHITMAN; MATTORD, 2017).

Convém ressaltar a espontaneidade dos dois entrevistados não só na demonstração de sua compreensão acerca da importância dos *backups* na conservação da integridade, disponibilidade e confiabilidade da informação, mas também quando se referiram ao hábito de fazer cópias de segurança. Tal prática é definida na literatura como prática fundamental à SI, de acordo com autores como Whitman e Mattord (2017) e Frik *et al*. (2019), pois mantém dados disponíveis e íntegros e evita interrupções operacionais.

Adiciona-se aqui o fato observado pelo pesquisador de que E1 e E3 têm contato constante com a equipe de informática da empresa, seja por experiência prévia no setor (E1 trabalhou por 02 anos como assistente administrativo na TI do órgão), como pela existência constante de demandas do setor no qual E3 é responsável, ou área técnica de georreferenciamento e regularização fundiária da organização. Esta área da empresa apresenta alta utilização de recursos tecnológicos, como grandes áreas de armazenamento em rede, diversos programas de alto requerimento de desempenho de hardware, como o AutoCAD e o Topograph, e impressão em impressoras administrados pela equipe de informática.

Outras menções aos *backups* ocorreram unicamente de maneira estimulada, usualmente indicando a reação a alguma perda de dados que seus respondentes enfrentaram, seja pela ação de vírus, por falhas de hardware (discos rígidos) ou por exclusões acidentais. Esta última situação já ocorreu diversas vezes com E2, de acordo com a própria entrevistada:

> A única coisa que eu uso é o pen drive, para salvar os dados. Só. Eu já perdi muitos arquivos assim, porque eu não sei, assim, mas eu já perdi. A partir dessas perdas eu comecei a usar pen drive, assim, não tem muita segurança, nem pen drive nem HD externo, nada disso tem. Eu perdi dados importantes e alguns dados eu protejo nesse sentido, de botar pendrive, de ter uma cópia, tenho uns dois ou três pen drives q eu faço isso. (E2)

A entrevistada afirma que utiliza pen drives para fazer suas cópias de segurança, mas admite que não confia que esses dispositivos vão conferir muita confiabilidade ao afirmar que não ofereciam muita segurança. Todavia, não soube mencionar que recurso poderia fornecer armazenamento confiável, e que os *backups* eram sua única prática observada de proteção à informação. E4 também fez menção aos *backups* após enfrentar falha de hardware no computador que utilizava na empresa, que, segundo ele, quase o fez perder todos os seus dados importantes de uso na organização:

> Outra coisa... *Backup*. A empresa não tem, pelo menos aqui. Eu tenho aqui o meu pessoal no HD, certo? Eu comprei um HD pessoal, meu, que eu uso aqui direto, entende? Então já aconteceu aqui no computador, não nesse, no anterior, Já deu pau. Não perdi porque eu tinha o meu HD. Mas não pela empresa, pela empresa não tem nada. Quero dizer... pode ter, mas aqui não chega. (E4)

O caso citado por E4 lança luz à necessidade da organização de, apesar de possuir área de rede em servidor de arquivos com *backup* diário e de já ter comunicado isso aos próprios usuários citados, desenvolver maneiras eficazes de informar e instruir os usuários no uso dos serviços que estão disponíveis, sobretudo aos que possuem maior dificuldade técnica no uso das tecnologias digitais. E4 finaliza seu depoimento acerca do tema dizendo que "pode ter, mais aqui não chega", referindo-se ao recurso de *backup* em rede fornecido pela organização, caso semelhante à entrevistada E2, que afirma desconhecer o recurso e utiliza os pendrives para realizar suas cópias de segurança.

Todavia, observa-se no cotidiano da empresa que esses usuários possuem dificuldades técnicas que os afasta da utilização desse recurso. Nesse ínterim, a comunicação entre organização e empregados é fundamental para a implementação de políticas de segurança, conforme Thompson e Mayhorn (2012). Ainda segundo os autores, a comunicação e o treinamento eficientes poderiam auxiliar usuários que possuem poucos conhecimentos na operação de dispositivos digitais, a exemplo de E2 e E7, a utilizarem os recursos tecnológicos de maneira mais segura.

Nesse ínterim, E5, E6 e E7, apesar de afirmaram reconhecer o recurso do *backup* como importante por entenderem apenas o seu conceito, reconheceram não fazê-lo por apresentaram baixa sensação de autoeficácia na operação dos dispositivos:

> É uma segurança... Porque se você tiver o *backup* atualizado, se acontecer alguma coisa, você está lá com seus dados guardados. É uma outra segurança, uma outra segurança pro usuário, porque não vai proteger alguém de fazer alguma coisa, mas apagar... Você tem em outro local. (E5)

> O *backup* já ajuda nisso, né [a evitar a perda de dados importantes – grifo nosso]? (E6)

Com efeito, E5 e E6 demonstraram entender a função dos *backups* e seus benefícios, mas ao serem perguntadas se possuem cópias de segurança de seus arquivos, negaram. Já E7 mencionou a necessidade de solicitar ao pessoal da informática que sejam feitas cópias de segurança de seus arquivos importantes:

> Eu acho que é possível sim [proteger-se das ameaças]. *Backup*, senhas, essas coisas, porque você está com as informações guardadas em outro local. (E6)

> Isso aí nós temos que ver com o pessoal da informática pra a gente fazer isso [*backup* – grifo nosso], porque senão a gente acaba perdendo... E aí com o auxílio do CPD, né? Aí a gente fica garantido, né? De não perder. (E7)

Apesar de importante para a segurança da informação, a percepção de que *backups* podem auxiliar na salvaguarda de dados e informações no ambiente corporativo, de acordo com Green e Dorey (2016). Segundo os próprios autores, a ausência dessa prática é potencializada por fatores como a falta de conhecimento na operação dos dispositivos e a sensação de autoeficácia na realização da tarefa pelos próprios usuários. O depoimento de E7 demonstra esse ultimo fator, já que a mesma considera necesária a intervenção da equipe de informática para que sejam feitos cópias de segurança de arquivos importantes. *Backups* podem evitar maiores danos em caso de incidentes de segurança, a exemplo de invasões de sistemas por *hackers* e infecção por *malware*, como ransomware e outros programas maliciosos (WHITMAN; MATTORD, 2017).

Exemplificando prejuízos que podem advir da ausência da prática do *backup* e da própria, a própria empresa estudada sofreu um ataque de ransomware em 2022. Como resultado, houve a perda de todos os dados que eram armazenados localmente no computador de um gestor sênior que, ao executar um anexo malicioso recebido em sua caixa de e-mails pessoal, criptografou invonluntariamente todos os arquivos existentes no disco rígido, incluindo declarações de imposto de renda e documentos referentes à assinatura de convênios. Pelo modo de operação do malware em questão, juntamente com a ausência de *backup* de tais dados, não houve forma de restaurá-los. O caso foi observado e registrado no Script de Observação 03 (RAO; NAYAK, 2014).

A Figura 15, exposta na sequência, expõe a distribuição da situação dos entrevistados no tocante à sua capacidade de fazer cópias de segurança de seus arquivos importantes.

Figura 15 – Situação dos entrevistados em relação à capacidade de fazer backups.

Fonte: Dados da pesquisa (2023).

A partir dos dados apresentados nessa seção, pode-se considerar oportuna a discussão no âmbito da conscientização dos usuários acerca de como os *backups* podem ajudá-los a evitar riscos de SI, além da instrução em maneiras de realizar cópias de segurança no ambiente da organização. Com efeito, a própria empresa dispõe de área de armazenamento em rede para este fim, e observa-se nos relatos que poucos entrevistados estão cientes disso.

Nesse interim, de acordo com as melhores práticas de proteção à informação, observa-se como positivo o fato de que todos os entrevistados na empresa conhecem o conceito, mesmo que não o façam. Segundo Llorente-Barroso *et al*. (2018), o conhecimento favorece a sensação autoeficácia dos sêniores em relação à utilização de tecnologias digitais, e isso, por consequência, tende a aproximá-los às melhores práticas de SI.

Porém, autores como Thompson e Mayhorn (2012) e Whitman e Mattord (2017) sugerem que muitos usuários passam a adotar essa prática após uma perda de dados sensíveis, e que a conscientização acerca dos riscos é fundamental no processo de tornar os *backups* uma prática preventiva na organização. Esse dado corrobora o que foi encontrado durante as entrevistas, já que 03 de 07 (42%) dos participantes representam casos de utilização de *backup*

apenas após incidentes de segurança. Tal cenário também vai de encontro ao que diz a literatura no que tange à reduzida aderência dos usuários sêniores à prática de *backups* (MANNHEIM ET AL., 2019; FBI 2023).

4.1.1.2 Senhas

O segundo fator mais citado entre os entrevistados teve relação com o correto gerenciamento de senhas, que consiste na utilização de individual e intransferível de palavras-chave. A criação de credenciais que seguem parâmetros classificados pela literatura especializada como senhas seguras ou fortes é recomendada, bem como a sua memorização por parte do usuário. Autores como Frik *et al*. (2019) e Masuch *et al.* (2021) afirmam que a prática de decorar senhas incrementa a segurança por evitar que sejam anotadas e guardadas em lugares de fácil acesso.

Repetindo o padrão verificado no fator anterior, entrevistados como E1 e E3 mencionaram de maneira espontânea compreender a importância desse aspecto na proteção à informação. Adiciona-se a isso o fato de que esses participantes citaram o assunto como o primeiro fator fundamental à SI, bem como a sua familiaridade com possíveis desdobramentos da utilização incorreta de senhas no uso de computadores e sistemas:

> No momento que você quer uma parte segura entre computador e celular, é necessário que você tenha uma senha, né, para poder ter a sua segurança, a sua segurança. Que ninguém descubra seus dados, todos os documentos de uma empresa como os documento pessoais, certo? Isso se chama segurança de celular, segurança de trabalho dentro da sua empresa, do ambiente de rede. (E1)

> Uma prática que eu acho muito perigosa, que é a disponibilização de senhas, minha senha. Então a senha é uma coisa extremamente pessoal, qualquer uma que seja, as pessoas tem que tratar as senhas que eles utiliza de acessos na empresa, como ele utiliza ele, como ele guarda informações da senha do banco, por exemplo. (E3)

Percebe-se, em seu posicionamento, que E1 aponta como importante o sigilo das informações, tanto de dados pessoais quanto da organização. Além disso, demonstrou que conservar o acesso restrito por meio de senhas é importante em todos os dispositivos que utiliza na empresa, citando inclusive a necessidade de se proteger o ambiente de rede. E3, por sua vez, considera críticas tanto a intransferibilidade das senhas quanto a restrição de acesso ao ambiente da empresa e a dados importantes. Traz ainda ao debate a importância que percebe na característica da auditabilidade e responsabilização pelo mau uso de dados e informações, vista como um dos objetivos fundamentais da SI por autores como Cherdantseva e Hilton (2013) e ISO (2022):

> Por exemplo, a senha do Expresso [e-mail corporativo – grifo nosso]... Aquilo ali é pessoal e é você quem tem acesso. Até porque você é responsável por aquela senha, a partir do momento que recebo do Estado, por exemplo, uma senha para abrir o Expresso e eu disponibilizo para qualquer pessoa acessar, entra ali uma pessoa que manda uma mensagem para o governador, ou xingando todo mundo que vai chegar lá em meu nome. Então, isso eu procuro fazer [não compartilhar a credencial – grifo nosso]. (E3)

Segundo Haeussinger (2017) e ISO (2022), o aspecto da auditabilidade, constantemente vinculado ao não-repúdio, permite a auditoria e a responsabilização de possíveis incidentes de segurança, a exemplo do cenário relatado por E3, ou a utilização de senhas de terceiros para acesso ao e-mail corporativo. O empregado ainda traz à discussão mais detalhes acerca de sua preocupação com esse aspecto:

> Às vezes... Às vezes eu tenho impressão, sabe, que as pessoas ainda não entenderam a responsabilidade que é quando receber uma senha daqui da empresa. Eu acho que não entenderam. E a gente tá vivendo no mundo, cara, que não dá pra você baixar a guarda pra nada. Infelizmente. (E3)

E3 considera que o cenário de crescimento de riscos não permite a gestão descuidada de senhas, percepção amparada pela literatura especializada. Autores como Llorente-Barroso *et al*. (2018) e FBI (2023) mencionam que técnicas de obtenção senhas e outras credenciais de acesso utilizadas por criminosos e cada vez mais baseadas em engenharia social, são especialmente perigosas a usuários sêniores. E4 e E5 também mencionaram o aspecto, após o entrevistador descrever práticas de proteção à informação. Inicialmente, E4 demonstrou compreender os riscos a que uma senha compartilhada pode representar à organização:

> Assim. veja bem, porque cada um tem a sua senha, né? Embora seja uma só, pelo menos aqui. Aqui com a gente tudo é "emdagro" [senha padrão utilizada para acesso aos computadores definida pela equipe de TI – grifo nosso]. Aí eu posso entrar no computador ali do meu colega, ele pode entrar no meu assim, entendeu? Qualquer um acessa. Por um lado é bom por que é prático, né? Porque às vezes o colega tá viajando, eu tenho de acessar o computador dele. Preciso de uma informação dele. Olhando por esse lado é bom, já por outro... Se o camarada quiser fazer alguma coisa, ele faz... Ele abre, entra aqui no meu, deleta... Salvo se eu tivesse a dele, ele tivesse a própria, mas é geral. (E4)

Além de demonstrar entender o princípio do compartilhamento de arquivos nos computadores dos colegas de seu setor, o que considera útil e prático, considera que tal configuração constitui uma falha se segurança, pois abre a possibilidade do mau uso de dados e informações. Também é possível inferir da fala do entrevistado que o mesmo observa que o princípio da auditabilidade pode ser ferido quando se utiliza senha comum de acesso a todos os computadores, mesmo sob usuários diferentes, pois tal prática dificulta a rastreabilidade do uso e uma possível imputação de responsabilidades.

Tal política de senha comum para acesso à maioria dos computadores implementada pela equipe de TI foi levada a cabo em virtude da dificuldade de muitos usuários sêniores da organização em memorizar senhas, especialmente quando existe política concomitante de troca mensal de senha do e-mail corporativo e internet, conforme mencionado anteriormente. A observação do participante E4 serve também como ponto de atenção aos processos da organização, no sentido de falhas de segurança como essa existirem em seu ambiente.

E5 também considera que as senhas são importantes, exemplificando seu ponto de vista ao relatar uma recente invasão do ambiente digital do Conselho Regional de Contabilidade. Segundo a participante, ao ser perguntada como se reduziria a possibilidade de incidentes como esse ocorrerem, mencionou, mesmo que de maneira hesitante, a importância de uma gestão correta de senhas, mantendo sobretudo sua confidencialidade e intransferibilidade. Convém ressaltar aqui que foi a única participante a fazer menção tanto à política de alteração periódica de senha em vigor na organização, quanto ao conceito de senha segura:

> Eu acho que é possível sim. Inclusive com essas que a gente já falou na primeira pergunta. Senhas seguras, devido a isso, tem a sempre alterada, mudada. (E5)

O posicionamento de E5 nesse sentido corrobora o que é recomendado pelas melhores práticas em proteção à informação, mencionadas por autores como Green e Dorey (2016) e Stelzer e*t al*. (2019). Segundo seus estudos, senhas devem ser pessoais, intransferíveis e definidas seguindo padrões seguros que dificultem ataques de criminosos, pois esses utilizam sofisticados programas de quebra de senhas.

Os entrevistados E6 e E7 trouxeram em suas respostas citações às senhas, mas demonstram uma preocupação restrita, ou seja, não consideram estar vulneráveis a incidentes que possam advir do acesso não autorizado a suas credenciais de acesso. Nesse ínterim, E7 afirma que não se preocupa muito com sua senha fornecida pela organização, apenas com seu smartphone pessoal:

> Eu não, porque não tem coisas sigilosas que eu vou fazer que precise de senha não... Senha só particular, no celular, mas aqui na empresa, não. (E7)

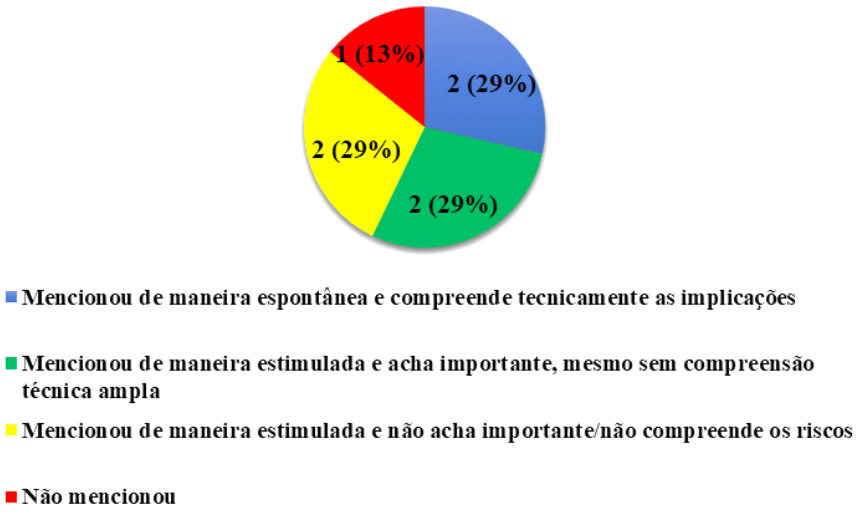
Com efeito, por considerar manipular apenas dados e informações não sigilosas no computador que utiliza na empresa, E7 disse não se preocupar com acessos não autorizados no dispositivo, afirmando ainda não ter a preocupação de bloqueá-lo ao se ausentar de sua estação de trabalho. A esse respeito, E6 revelou percepção semelhante, ao afirmar:

> Não possuo nada sigiloso nem nada importante no computador da empresa ou no meu celular. Porque assim... Eu não tenho senha nenhuma gravada no celular. Minhas senhas são gravadas numa agenda em papel, tá? Então, se eu... Se eu não as gravar no celular, eu não tenho problema. Não faço nada. Não tem nada no meu celular. Então se... Pode até entrar e ver as mensagens que eu recebo de cartão de crédito. Eu recebo mensagens, mas assim foto não tem e não tenho senha. Então essa parte eu não me preocupo. (E6)

Pode-se observar que as participantes não consideram estar sujeitas a riscos, o que demonstra a possessão de limitados conhecimentos acerca das ameaças de SI às quais estão sujeitas. Tal percepção é apartada das boas práticas de SI, uma vez que não havendo conscientização de que existem ameaças à segurança de seus dados e informações, é improvável que o usuário tenha capacidade técnica de evitá-las. Green e Dorey (2016) recorrem à analogia de uma doença que só pode ser tratada quando se sabe de sua existência, bem como se conhecem suas características. Trazendo a referência à discussão, não estar consciente acerca das ameaças é potencialmente tecnicamente perigoso ao usuário e à organização como um todo, pois expõe a integridade, confidencialidade e disponibilidade dos dados e informações . Esse cenário representa a ausência de aspectos cognitivos pelas entrevistadas, condição que pode favorecer incidentes de segurança (HAEUSSINGER, 2017).

Será exposta na sequência a Figura 16, que expõe a percepepção dos entrevistados acerca do aspecto gerenciamento de senhas, de acordo com a espontaneidade com que o mencionaram e seu nível técnico demonstrado e confrontado com a literatura.

Figura 16 – Percepção dos entrevistados acerca da gestão de senhas na proteção à informação.



Fonte: Dados da pesquisa (2023).

Percebe-se que mais da metade dos entrevistados (04, ou 58%) consideram importante gerir senhas de maneira correta, e demonstraram compreender de maneira tecnicamente adequada os riscos e consequências aos quais estão sujeitos. Adiciona-se ainda à discussão que 03 desses 04 participantes possuem constante contato com o setor de informática da organização, especialmente E1 e E3 conforme observado no aspecto anterior. Já E4 exerce o contato com a equipe de TI por sanar dúvidas frequentemente com seus integrantes, quando esses visitam o setor no qual o participante trabalha. Tal característica concernente à frequência de interação sênior/técnicos de tecnologia fato pode auxiliar na compreensão acerca da construção do conhecimento desses usuários, segundo Green e Dorey (2016) e Masuch *et al*. (2021).

Em contrapartida, 03 participantes demonstraram não compreender os riscos que uma má gestão de senhas pode acarretar, tanto para seus dados pessoais como os da organização. Dito isto, possível notar que a empresa, apesar de implementar política de troca de senha mensal, não alcança o objetivo de conscientizar todos os seus empregados sêniores quanto à necessidade de conhecer e seguir boas práticas na gestão de senhas. Adicionalmente, não há nenhuma política de responsabilização em caso de mau uso de credenciais de acesso em vigor na empresa estudada, o que também vai em direção oposta às boas práticas de SI (THOMPSON; MAYHORN, 2012).

4.1.1.3 *Hackers* e outros criminosos da internet

O terceiro aspecto mais citado pelos entrevistados trouxe menções à ação de *hackers* e outros indivíduos mal intencionados que atuam em ambientes digitais, buscando invadir dispositivos e furtar, destruir ou ter acesso a dados e informações não autorizados. Diversas são as técnicas utilizadas pelos atacantes para alcançar tal objetivo, a exemplo de *vishing*, *phishing*, e-mails fraudulentos e aplicativos de mensagem.

Buscou-se, então, conhecer a percepção dos entrevistados acerca de riscos e ameaças perpetradas por esses indivíduos/grupos. Ou seja, os conhecimentos dos participantes sobre a existência, severidade, padrões de abordagem e objetivos que os criminosos do mundo digital utilizam. Uma vez que a literatura aponta a consciência dos usuários sobre características das ameaças como fundamental à manutenção dos pilares da SI, esse tópico objetiva lançar luz nesse sentido (GREEN; DOREY, 2016; MASUCH ET AL., 2021).

Iniciando-se a análise propriamente dita, E3 traz à discussão, de maneira espontânea, o aspecto da exposição a usuários mal intencionados quando do acesso a redes wi-fi públicas. O usuário cita exemplos o acesso à internet fornecido em ambientes de grande circulação como shoppings centers e aeroportos:

> Então você, por exemplo, vai fazer um cadastro da DAP [documento preenchido em *website* do Ministério da Agricultura – grifo nosso], não sei se é possível ou só a título de exemplo, mas se você acessa de uma rede aberta, se não for rede segura, "vou trabalhar no shopping que vou almoçar e vou trabalhar na rede", ou no aeroporto. Você está deixando aberto ali todos aqueles dados. E não é que vai acontecer, mas pode acontecer porque não tem a mesma segurança. (E3)

Em se tratando do acesso a esse tipo de conexão à internet, o usuário demonstrou compreender os riscos aos quais está sujeito, sobretudo no tocante à invasão de seu dispositivo e de um possível furto de dados. Nesse sentido, E3 continua:

> Hoje todo local que você chega, tem um Wi-Fi disponível. A partir do momento que você acessa aquilo ali, você está abrindo sua caixa preta. Isso se você acessa através

> de um tablet ou de um celular, dependendo da segurança daquela rede, todos seus dados são muito mais vulneráveis do que um ambiente mais seguro. Por exemplo, eu confio muito mais em abrir um celular meu, um aplicativo de banco, por exemplo, num celular meu, através de uma rede aqui da EMDAGRO, por exemplo, do que chegar numa clínica e eu acessar. Ou no aeroporto, ou no shopping. (E3)

Com efeito, conectar-se a redes públicas, de acordo com Whitman e Mattord (2017) e Hadnagy (2018) é uma prática comum e potencialmente insegura, que expõe o dispositivo utilizado a riscos, como o acesso não autorizado a arquivos particulares, controle remoto e instalação de malware. De maneira também espontânea, E1 expôs preocupação acerca do acesso não autorizado a dados e documentos, nesse caso considerando o acesso não autorizado de dispositivos no próprio ambiente de trabalho:

> Que ninguém descubra seus dados, todos os documentos de uma empresa como os documento pessoais, certo? Isso se chama segurança de celular, segurança de trabalho dentro da sua empresa, do ambiente de rede. (E1)

Observa-se que para o entrevistado é importante manter seguros os ativos informacionais inclusive no celular, o que, segundo ele, confere segurança de trabalho por também proteger o ambiente de rede da organização. Tal preocupação é similarmente observada por E4, que cita e descreve espontaneamente possíveis consequências de uma invasão por um *hacker* à rede da empresa:

> O prejuízo é bem maior para a empresa, né? Sem contar que pode entrar um cara aqui, um *hacker*, né, E pode alterar aqui um bocado de coisa, né? Mexer aqui e passar informação distorcida, tudo isso... não é tanto pra mim, não, entendeu? Eu vejo mais o lado da empresa porque perde as informações e tudo mais. Tá certo, porque eu não tenho nada. Praticamente eu não tenho nada meu aqui no computador. O que eu tenho é basicamente da empresa ou tem alguma besteira ou outra coisa minha, mas o resto é tudo a empresa. (E4)

O usuário descreve, com razoável nível de detalhe, a ameaça aos objetivos da segurança da informação da empresa caso haja uso indevido que permita uma invasão por um *hacker*, conjuntura que encontra aderência teórica na literatura. Segundo Cherdantseva e Hilton (2013), o acesso indevido a ambientes restritos de rede é uma séria ameaça à autenticidade, confidencialidade e integridade dos dados de uma organização, bem como aos seus serviços e operações, e o mau uso pelos usuários continua sendo o principal motivo pelo qual incidentes como esse ocorrem (GREEN; DOREY, 2016).

Nesse sentido, outros entrevistados apresentaram ter noção de que existem riscos de invasões a dispositivos e ambientes de rede, porém demonstram não possuir tantas informações sobre possíveis consequências que podem advir desses ataques:

> Agora eu vou dar um exemplo. Pronto, depois você tira daí. A semana passada houve uma invasão no nosso Conselho [Conselho Regional de Contabilidade – CRC – grifo nosso]. Agora recente, semana passada. Houve uma invasão, roubaram. A preocupação é essa, tomaram todas as providências e comunicaram a gente. Estou com o comunicado aí. Se há uma invasão, eu entendo que pode ocorrer vários prejuízos, porque lá está toda a sua vida, toda sua, o seu CPF, toda a sua documentação está lá. Em muitos casos tem até, em muitos casos... Fraude de conta bancária... (E5)

> Ave maria... Isso aí acontece direto. Isso é ruim, mesmo [invasão e furto de dados em smarphones e computadores – grifo nosso]. Ah, isso aí já aconteceu... Eu já ouvi falar que aconteceu. Comigo não, com outras pessoas. Ouvi falar que entraram e acessaram a conta. (E7)

> Então, se eu... Se eu não as gravar no celular, eu não volto. Não faço nada. Não tem nada no meu celular. Então se... Pode até entrar e ver as mensagens que eu recebo de cartão de crédito. Eu recebo mensagens, mas assim foto não tem e não tenho senha. Então essa parte eu não me preocupo. (E6)

O cenário citado por E5 traz à discussão que ouviu o relato de um caso de invasão a uma outra organização, da qual foram extraídos dados sensíveis, a exemplo do CPF de pessoas e outros documentos. E7, por sua vez, citou que já ouviu falar de casos de invasões e furtos de dados em aparelhos celulares, nos quais houve acesso a contas bancárias, e afirmou que apesar de considerar a possibilidade de ter seu telefone celular invadido não se preocupa muito com isso, pois não tem dados pessoais sensíveis que possam causar maiores prejuízos. Já E2 tem uma percepção que leva em consideração a intenção de pessoas em acessar informações pessoais de maneira ilegal:

> Acho que existe um conjunto de procedimentos, né? Quem cria esses instrumentos aí tem a preocupação com as pessoas que fazem uso dessas tecnologias, de proteger a informação, né? Essas informações que estão espalhadas por aí afora, todos eles querem informação da gente. E eu acho sim que existem esses procedimentos e preocupação. Agora eu queria gostar mais, para me proteger mais. (E2)

Os seguintes trechos da declaração de E2 expostos na sequência serão discutidos e confrontados com a literatura:

1- O conjunto de procedimentos que afirmou pensar que existe;

A aparente hesitação da entrevistada demonstra a sua já mencionada reduzida sensação de autoeficácia na proteção à informação, por uma declarada falta de habilidade que, nesse caso, refere-se ao desconhecimento sobre maneiras de se proteger de ameaças. Isto vai de encontro às observações de Llorente-Barroso *et al*. (2018) no tocante à importância da sensação de autoeficácia à correta utilização de dispositivos digitais.

2- Citou, de maneira clara, a prática de proteger a informação por meio de instrumentos;

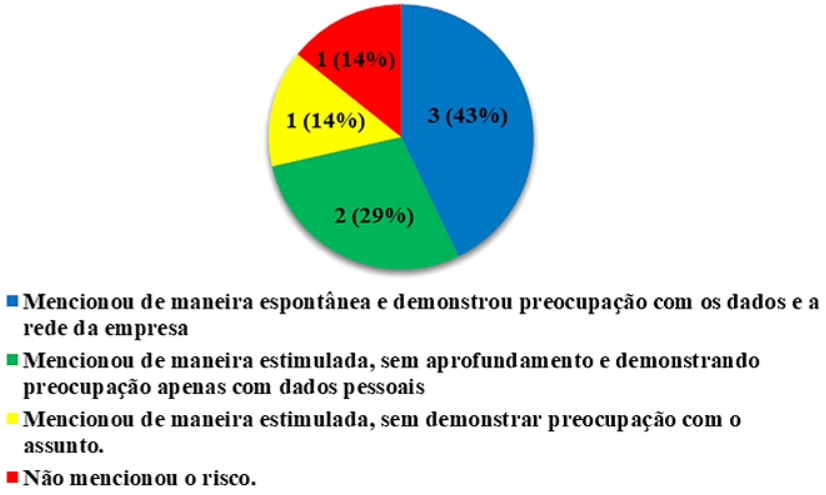
Apesar de mencionar que existem instrumentos que auxiliam na proteção à informação, demonstrou no fator referente à utilização de backups que aquele era sua única prática e cuidado em proteção à informação. Tecnicamente, considera-se positiva à SI a percepção de que existem mais instrumentos que reduzem os riscos, porém não houve nenhuma citação em relação a que instrumentos seriam esses, nem como utilizá-los (WHITMAN; MATTORD, 2017).

3- Afirmou que queria gostar mais do assunto, para proteger seus dados na internet de maneira mais eficiente;

O comentário que finaliza a citação da entrevistada traz ao debate o aspecto elementar do interesse: o usuário não se interessa por tecnologias digitais e por segurança da informação, logo se protege menos. Nesse sentido, Li e Luximon (2016) e Adamczyk e Betlej (2020) observam em suas pesquisas que os empregados sêniores apresentam menor interesse na utilização de dispositivos digitais, e que isso tende a reduzir sua sensação de autoeficácia nessa atividade. Tal aspecto também pode ser considerado oportuno à discussão pelo fato de a entrevistada citar apenas o interesse de criminosos em dados que estão fora do ambiente doméstico/organizacional, e não fazer menção à proteção de dados no ambiente organizacional.

A Figura 17 expõe os posicionamentos dos entrevistados em relação aos seus conhecimentos sobre a atuação de *hackers* e outros indivíduos mal intencionados em ambientes digitais.

Figura 17 – Percepção dos entrevistados em relação a *hackers* e outros indivíduos mal intencionados que atuam em ambientes digitais.



Fonte: Dados da pesquisa (2023)

Pode-se observar que menos da metade dos participantes da pesquisa (03 de 07, ou 43%) mencionaram de maneira espontânea terem algum conhecimento acerca de ataques e suas possíveis consequências, especialmente voltadas aos dados e ao ambiente de rede da organização. Em relação aos demais entrevistados, alguns comentaram após estímulo pelo entrevistador, enquanto outros não mencionaram o tema. Traz-se ainda atenção ao dado de que mais da metade (04 de 07, ou 57%) dos participantes não demonstraram preocupação com a possibilidade de invasão da rede da empresa e que dados e informações importantes pudessem ser alvo de furto, alteração indevida ou até mesmo destruição.

A conscientização do usuário acerca da existência de indivíduos ou grupos interessados em invadir redes de organizações acessar indevidamente seus dados e informações é fundamental à SI da empresa, segundo Thompson e Mayhorn (2012), Rao e Nayak (2014) e Masuch *et al*. (2021). Diante da particular vulnerabilidade do usuário sênior a ataques baseados em engenharia social, cada vez mais utilizada por *hackers* e outros criminosos em sua busca por brechas de segurança, o tema se torna ainda mais oportuno a gestores em um cenário de crescente digitalização de processos e atividades (FRIK ET AL., 2019; FBI, 2023).

4.1.1.4. Antivírus

Outro aspecto mencionado nas entrevistas foi em relação a software antivírus, sobretudo no que se refere à percepção do entrevistado em relação à importância da existência e da atualização desse agente de segurança nos dispositivos. Antivírus são programas considerados fundamentais à proteção da informação por sua capacidade não só de detectar a presença de malware em computadores, tablets e smartphones, mas também de evitar que programas maliciosos sejam executados. Quando isso ocorre, diversas consequências nocivas ao bom funcionamento do sistema podem advir, desde o aparecimento de propagandas indesejadas e redução no desempenho do dispositivo até a destruição de dados e invasão do sistema (STEWART ET AL., 2015).

Nesse contexto, E1 descreve de maneira estimulada a sua percepção sobre software antivírus na proteção à informação:

> É importante [a presença do agente – grifo nosso]. Veja só: se você não tiver um antivírus no seu computador ou em outro dispositivo você pode perder seus dados,

> né? O vírus vai chegar um momento em que ele vai destruir tudo o que você tem. Por isso que o antivírus é necessário. (E1)

Diferentemente de E3 e E4, que são citados na sequência, E1 não menciona a prática da atualização do agente, mas afirma que considera o antivírus de fundamental importância à integridade de dados e informações. Este posicionamento encontra amparo na literatura especializada, mas esse tipo de software só alcança o máximo de performance quando está atualizado. Logo, a consciência acerca desse aspecto da proteção por parte do usuário é considerada importante (WHITMAN; MATTORD, 2017).

Com efeito, E3 e E4 responderam estar mais alinhados às boas práticas nesse sentido:

> Sim, e a questão do antivírus, a atualização do antivírus, você tem que estar com antivírus em condições né? E para isso também tem que ter uma coisa que seja sempre atualizado o antivírus. E isso é fundamental. Mas você tem um antivírus, se instala há dez anos atrás porque os vírus são só mutantes, digamos assim. Eles vão sendo aperfeiçoados a cada dia. (E3)

> O antivírus aqui... De vez em quando tá dando aqui que tá desatualizado, está atrasada a licença, expirou, desatualizado. Agora eu não sei, tá, eu fico na dúvida se realmente o antivírus está desatualizado, não tá? Entendeu? Sim, eu não sei qual é a frequência que vocês fazem lá. Se fazem toda hora. Eu acho que essa questão do antivírus é importante sim. (E4)

O fator da atualização é espontaneamente mencionado pelos dois entrevistados, o que demonstra uma percepção correta acerca do funcionamento do agente de segurança. Convém à analise acrescentar que E3 mencionou o aspecto mutação dos vírus, o que também encontra amparo na literatura, segundo Hadnagy (2018). Uma vez que os virus são constantemente modificados para se adaptarem às defesas, os programas antivírus também precisam contemplar atualizações para neutralizar novas versões de softwares nocivos (MASUCH ET AL., 2021). Adicionalmente, E4 trouxe à discussão o fator da licença do agente de segurança, que torna-se necessário quando a organização utiliza uma solução paga. Uma vez que a licença em questão está vencida, a proteção pode estar comprometida ou até mesmo desativada (LYRA, 2015).

E5, por sua vez, cita de maneira estimulada e hesitante a questão do antivírus, após mencionar senhas como aspecto fundamental à proteção da informação:

> Será que não é através de senha? Através até de... Como é que chama? De... Antivírus? Será que não é através de um antivírus bons que possa fazer essa proteção? Para não entrar com isso... Se algum vírus, desses vírus brabo que tem por aí. (E5)

Após dizer que um antivírus de qualidade pode proteger o usuário, evitando a entrada de programas maliciosos, descritos como “virus brabo”, continuou expondo sua percepção ao citar novamente a invasão ao Conselho Regional de Contabilidade, órgão ao qual a usuária é vinculada:

> A falta naturalmente de um antivírus bom para proteção das nossas informações lá. (E5)

Dessa maneira, E5 associou a defesa contra o incidente ao antivírus, o que é parcialmente aderente ao que diz a literatura. Esses agentes de segurança podem evitar a execução de malware que possa facilitar o acesso de invasores, mas *hackers* podem utilizar outras maneiras para invadir ambientes privados, a exemplo do acesso a senhas de usuários ou pela exploração de vulnerabilidades em sistemas (WHITMAN; MATTORD, 2017).

E2 também menciona de maneira estimulada o antivírus como importante, mas afirmou não ter preocupação nem paciência para gerenciá-lo:

> Eu acho que tem a questão do vírus, por exemplo. São assim, são prejuízos enormes que causam. Agora, talvez também eu não tenha paciência muito de utilizar o antivírus. Eu não tenho essa preocupação. Quando ele aparece, eu sempre peço para alguém. Aquela preocupação, por exemplo, você quando botar um pendrive, você passar o antivírus. Às vezes eu faço isso quando estou bem segura, que eu sei fazer isso porque não é como eu disse a você, o meu conhecimento de computação é muito limitado. (E2)

Apesar de afirmar reconhecer que vírus são perigosos por causarem "prejuízos enormes", é potencialmente insegura a opção de não "utilizar" nem ter paciência em atualizar o antivírus, inclusive quando se utilizam pen drives para realizar *backups*. Anteriormente no estudo, em relação à prática de *backup*, E2 mencionou utilizar esses dispositivos externos para realizar cópias de segurança de seus dados. Porém, ao declarar não fazer varreduras de antivírus em pen drives, a entrevistada torna suas cópias de segurança expostas a riscos de integridade (RAO; NAYAK, 2014; STEWART ET AL., 2015).

O aspecto da falta de interesse e paciência, citado novamente por E2 após ter sido mencionado no fator anterior, afasta ainda mais a participante das melhores práticas em segurança e da conscientização em SI, conforme o que observa Llorente-Barroso *et al*. (2018). Para as autoras, um reduzido interesse por parte do usuário em adquirir conhecimentos acerca da tecnologia digital dificulta a adaptação dos sêniores a seu uso seguro.

A também já comentada observação de incidentes de segurança originados pela usuária e verificados pela equipe de TI do órgão, trazem casos práticos à discussão que demonstram a que tipo de riscos E2 está exposta. Incidentes de infecção por malware, perdas de dados e descontinuidades operacionais são exemplos de consequências da negligência com o agente de segurança pela usuária com a segurança pode causar.

Por fim, os antivírus não foram citados por E6 e E7. Será feita na sequência a exposição gráfica dos posicionamentos dos entrevistados acerca do tema na Figura 18.

Figura 18 – Percepção dos usuários acerca de software antivírus.

Fonte: Dados da pesquisa (2023).

A Figura 18 realça o fato de que apenas 02 dos 07 participantes (E3 e E4, representando 29% dos entrevistados) apresentou familiaridade com o aspecto antivírus, agente de segurança fundamental à proteção da informação em ambientes organizacionais (GREEN; DOREY, 2016). O contato que os usuários em questão têm com a equipe de TI pode auxiliar na explicação a essa familiaridade, uma vez que recorrem aos especialistas com uma frequência maior do que os outros entrevistados. Verificou-se a exceção de E1, que apesar de não ter

mencionado de maneira espontânea, demonstrou a importância do antivírus em todos os dispositivos conectados à rede da empresa.

Do restante dos entrevistados, 02 afirmaram considerar importante a ação do antivírus, e compreendem satisfatoriamente os riscos que os vírus podem trazer à organização e a dados pessoais. Porém, também disseram não verificar se o programa está funcionando corretamente, ou se está atualizado, e outros dois participantes não mencionaram o aspecto, mesmo após estímulo do entrevistador.

4.1.1.5. Baixa autoeficácia, insegurança ou medo

Insegurança, medo e baixa autoeficácia foram outros aspectos citados pelos entrevistados, e sua análise foi agrupada em um só tópico por representarem o sentimento de insegurança, medo e baixa autoeficácia na operação de dispositivos computadores, tablets e *smartphones*. Abordada na literatura como aspecto importante na utilização de novas tecnologias digitais, a autoeficácia é também considerada fundamental à segurança da informação. Frik *et al*. (2019) e Mannheim *et al*. (2019) afirmam que quanto menos inseguro e mais autoeficaz o usuário se sente, maior capacidade de perceber e evitar ameaças de segurança da informação ele terá.

Soma-se à discussão a premissa de que os sêniores são vistos como um grupo com baixa sensação de autoeficácia no uso das recentes tecnologias, a exemplo da digitalização dos processos nas organizações e na vida cotidiana. Logo, parte-se à análise desse aspecto na organização estudada, de acordo com os relatos feitos pelos participantes (HARGITTAI; DOBRANSKY, 2017; MENG ET AL., 2019).

As conclusões dos autores supracitados vão de acordo com o cenário de baixa sensação de autoeficácia observado na organização, aspecto registrado pelo pesquisador no Script de Observação 04. Nesse documento, observa-se muitos sêniores se esquivam da operação de sistemas implementados na organização, mesmo que treinamentos sejam oferecidos. É comum ouvir declarações dos sêniores – inclusive por diretores e coordenadores – do tipo: “esse negócio de computador é complicado”, não “entendo nada de sistema” ou ainda “não tenho idade pra isso”. Tal percepção por vezes atrasa a operação/implementação de sistemas e/ou sobrecarrega empregados que têm mais habilidade, usualmente empregados mais jovens com maior aptidão ao uso de dispositivos digitais.

No que se refere à discussão acerca dos dados das entrevistas, os relatos de E2 são oportunos, pois a entrevistada mencionou expressamente essa faceta de sua relação com a tecnologia:

> Olha, eu vou lhe dizer francamente, eu me sinto bastante insegura até por uma série de motivos, aí que a gente vê em relação à questão da segurança, de proteção de informações. E eu me sinto até receosa de fazer qualquer coisa, passando qualquer tipo de informação para o computador, celular e esses aparelhos aí. Certo? (E2)

Para E2, a insegurança e baixa sensação de autoeficácia fazem sentir receio de fazer qualquer coisa que envolva inserir “qualquer tipo de informação para o computador”. Como já discutido anteriormente, Mannheim *et al*. (2019) observa que a autoeficácia na operação de dispositivos tecnológicos digitais é fundamental à produtividade das organizações, além de favorecer um uso mais seguro desses aparelhos. E2 continua comentando mais detalhes acerca do assunto:

> Não me sinto segura, mesmo porque... Porque eu me sinto insegura? Porque eu não tenho muita habilidade de tá colocando, é... Colocando esse tipo de informação e acesso mesmo. Eu não tenho muita habilidade e sou meio medrosa. (E2)

Observa-se que E2 associa sua insegurança à falta de habilidade técnica na operação dos dispositivos digitais, utilizando inclusive a palavra “medrosa” para descrever sua postura em relação às ameaças de segurança. No que se refere à pouca capacidade de lidar com a tecnologia digital, E2 descreve da seguinte forma:

> Eu sei o básico para trabalhar na empresa, esse negócio todo, assim, fazer algum documento... (E2)

Na prática, a entrevistada limita a sua capacidade técnica à utilização de editores de texto, planilhas e apresentações, além da navegação em websites. Recorre com frequência à equipe de suporte quando há necessidade de realizar algo diferente, a exemplo da conexão a videoconferências e alterações de configurações de rede para utilizar o computador em casa. Outra situação é citada na qual a entrevistada não se considera capaz de realizar é a atualização de sistema:

> Eu não tenho essa preocupação. Quando ele aparece [atualizações de sistema], eu sempre peço para alguém. Eu não avanço muito na questão de buscar as informações que eu quero, porque há um impedimento se eu não atualizo. Sim, para mim me dá muita dor de cabeça, porque sempre, sempre tão pedindo para atualizar. E eu sempre digo não. Mais tarde, agora não... (E2)

Dessa forma, a entrevistada afirmou não se sentir capaz de realizar a tarefa e que adia a atualização sempre que possível. A prática é considerada insegura, como já mencionado na pesquisa, uma vez que atualizações de software servem para corrigir vulnerabilidades e melhorar o desempenho do sistema (STEWART ET AL., 2015).

A insegurança afeta também E3, que afirmou não se sentir plenamente seguro ao utilizar dispositivos digitais, pois:

> Saber o que fazer [para se proteger contra as ameaças de SI], de fato, eu não sei muita coisa, mas eu vou dar pra você a minha percepção em relação a essa questão. Hoje em dia, com tudo que a gente está vivendo, que a gente está vendo, eu estou mais cético em relação à segurança da informação. Eu não sei exatamente qual o termo da internet do submundo internet, a deep web, né? Bom, então a gente acha que às vezes está num ambiente seguro, um ambiente de rede, por exemplo, mas lá no submundo eles conseguem ter acesso a essas informações. (E3)

O participante descreve seu ceticismo acerca da plena segurança da informação, pois afirmou crer que não se sente seguro em nenhum ambiente de rede. Justifica seu posicionamento ao dizer que criminosos podem conseguir ter acesso às informações armazenadas, tanto no dispositivo que utiliza, quanto nos dados que são enviados à internet. Confrontando a declaração com a literatura, os riscos estão, de fato, presentes em qualquer ambiente, mesmo nos mais restritos e potencialmente seguros. Green e Dorey (2016) e FBI (2023) afirmam que as técnicas de ataque estão evoluindo constantemente para contemplar os avanços nas defesas, sobretudo ao utilizar as já comentadas técnicas baseadas em engenharia social.

Logo, a sensação de insegurança relatada pelo usuário pode ser considerada como positiva, uma vez que o conduz a estado de conscientização acerca de que todo e qualquer usuário está exposto a riscos de segurança. Nesse sentido, a literatura, por meio de autores como Frik *et al*. (2019) e Masuch *et al*. (2021) afirma que tal estado de conscientização tende a levar o usuário a uma prática de cuidado e precauções na utilização de computadores, tablets e smartphones conectados à internet.

Observações acerca da sensação de segurança ao utilizar dispositivos digitais também foi um fator mencionado por E6, mas a participante revela uma percepção que vai em um sentido diferente às dos demais entrevistados. Quando perguntada se acreditava que corria riscos relacionados segurança da informação ao utilizar dispositivos digitais fornecidos pela empresa, afirmou:

> Não, porque não tem nada, nada assim, meu, sabe? Então... (E6)

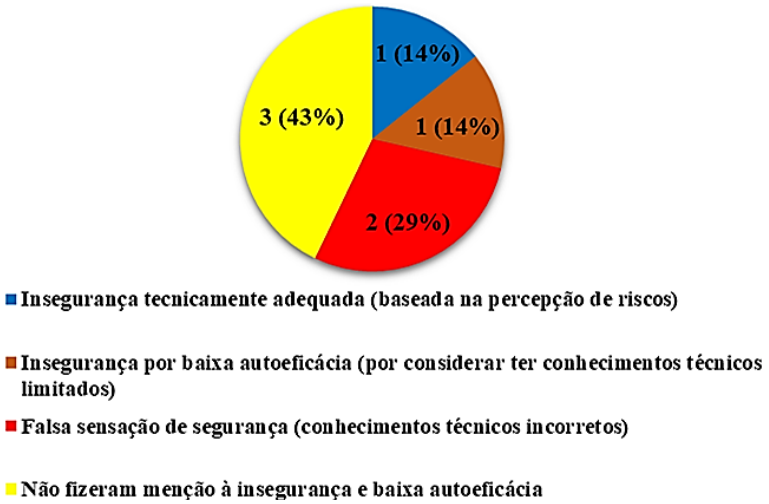
A resposta de E6 traz à discussão o que é observado por Green e Dorey (2016) e Hadnagy (2018): a indevida sensação por parte do usuário de que se está imune a ameaças de SI, ou que não corre riscos de ter seu dispositivo invadido, e seus dados acessados indevidamente. Thompson e Mayhorn (2012) ressaltam ainda que organizações devem tomar medidas para evitar que percepções desse tipo se desenvolvam em seu ambiente, uma vez que falhas de segurança podem levar a graves prejuízos. E7 também afirmou se sentir segura, uma vez que quando perguntada se a rede da organização pode ser invadida, respondeu:

> É possível, caso alguem de dentro passe o acesso. Se ocorrer de alguém aqui de dentro informar algo, aí entra. A atitude das pessoas pode colocar em risco. Não sei o que pode ocorrer se isso acontecer. (E7)

Ou seja, caso não haja a abertura de brechas de segurança por pelos próprios usuários, a usuária acredita que não há riscos de invasão à rede da organização. Apesar de afirmar que a atitude das pessoas pode colocar em risco a segurança da empresa, algo que encontra base técnica na literatura, o ambiente interno da EMDAGRO continua passível de invasões, mesmo que não haja falha técnica por parte dos usuários (GREEN; DOREY, 2016). Por fim, convém ressaltar que a entrevistada afirma não saber que consequências podem ocorrer caso isso ocorra.

Esse tópico é finalizado com a exposição da Figura 19, que apresenta graficamente os dados trazidos pelos participantes em suas entrevistas.

Figura 19 – Sensação de insegurança/medo e baixa autoeficácia percebida pelos participantes.



Fonte: Dados da pesquisa (2023).

Observa-se que apenas um usuário afirmou que sente algum grau de insegurança na utilização de dispositivos digitais, sobretudo no ambiente externo à organização, conforme mencionado no aspecto referente aos *hackers* e outros criminosos na internet – 4.1.1.3. Os demais que fizeram menção à sensação de insegurança apresentaram percepções tecnicamente divergentes às boas práticas de proteção à informação, seja por afirmar que não se sentem auto

eficazes no próprio uso dos dispositivos (E2), seja por declarar que se sentem seguros em um ambiente que está sujeito a riscos (E6 e E7).

4.1.1.6. *Websites*/aplicativos potencialmente inseguros

O sexto fator mencionado pelos participantes foi o acesso a websites e programas potencialmente inseguros. Esse aspecto da proteção à informação é debatido na literatura pela possibilidade de expor o usuário a diversos riscos de segurança, desde a captura de dados pessoais (por meio de *websites* falsos) a programas maliciosos que abrem portas lógicas no dispositivo que possibilitam o acesso de invasores, que passam a controlar silenciosamente o computador/*smartphone* (WHITMAN; MATTORD, 2017).

Partindo à discussão das menções dos entrevistados, percebe-se que de 06 citações acerca do tema, 04 foram feitas pelo participante E3. De maneira espontânea, ele menciona se preocupar com o acesso a websites, tema sobre o qual faz duas observações:

> Tem muita coisa que parece uma ovelha que nada mais é que na realidade, um lobo. Então é justamente você controlar o seu acesso no sentido ao que você acessa, que tipo de site você acessa, onde você vai buscar as informações. No caso de uso, nós como usuários. (E3)

> Estou falando principalmente daquelas máquinas que as pessoas têm acesso a outras redes, porque, por exemplo, tem sites aqui que você não consegue entrar de maneira nenhuma, porque a rede bloqueia. Não só a EMDAGRO, como a rede do Estado como um todo. Mas a partir do momento que chega na sua casa, que você sai da rede, do estado, você acessa o que você quiser, a máquina está com você. Então, se eu tentar entrar num site malicioso, vai funcionar. Isso vai. É isso que eu sei, porque eu já vi aqui jogos, brinquedos e etc. E outras coisas mais que você nem imagina. (E3)

O participante menciona o aspecto da utilização de dispositivos da empresa em redes públicas, que são posteriormente conectados à rede corporativa. Esse cenário é potencialmente perigoso à segurança tanto do próprio dispositivo quanto da rede da empresa, caso cuidados não sejam tomados pelo usuário. A atenção ao próprio aspecto do controle do acesso, seja no sentido de que sites são visitados quando conectado à rede externa, como também no ambiente da empresa, quando se vão buscar informações necessárias para o desenvolvimento de atividades diárias. Para E3, por vezes o website escolhido pode parecer uma "ovelha" e, na verdade, ser um "lobo". Tal preocupação também foi mencionada por E6, quando afirmou:

> Esse negócio de entrar em site... Eu entro. Mas aí eu vou olhar as opiniões de quem comprou. Se eu achar que a opinião está muito parecida uma com a outra, então eu não compro. (E6)

E6 é responsável pelo setor de compras da empresa. Logo, utiliza websites para realizar cotações de produtos e avaliação de preços. Dito isto, percebe-se que sua preocupação tange no sentido de fazer compras apenas de sites confiáveis, comparando as opiniões de pessoas que fizeram compras neles anteriormente. E6 também faz menção às *fake news* [notícias falsas – tradução nossa], sendo a única participante a trazer o tema ao debate:

> Você sabe que a internet tem muito *fake news*, né? Então sempre que tem uma coisa assim eu vou, eu vou em outros sites consultar para ver se tem a mesma notícia. Eu tenho certeza, porque uma notícia pode ocorrer, mas se for *fake news*, aí... (E6)

Os aspectos da navegação na internet mencionados pelos participantes podem ser considerados relevantes à discussão sobre SI no ambiente organizacional, já que tanto a

confidencialidade dos dados inseridos em sites quanto a segurança do próprio dispositivo e da rede interna da empresa podem ser ameaçados. A quantidade de *fake news* existente na internet também é considerada um problema pela literatura, pois pode levar à própria disseminação de notícias e informações falsas no ambiente organizacional. A preocupação pode ser considerada ainda maior quanto mais usuários sêniores fizerem parte da força de trabalho da organização, já que são apontados como um grupo especialmente vulnerável às *fake news* (FBI, 2023).

Acerca da instalação de programas, E3 menciona:

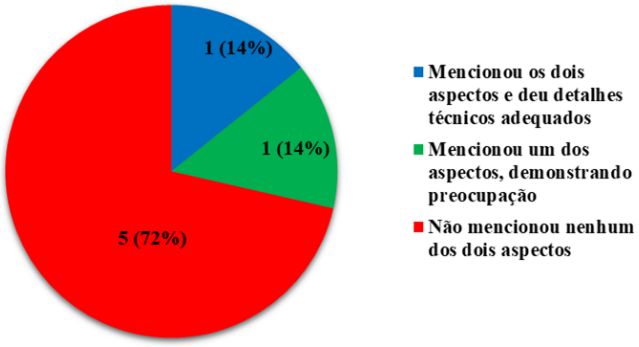
> Tem comportamentos aqui que coloca em risco esses dados. Você vê quantas vezes chegam na informática computadores com problemas, que você vai descobrir o porquê, vê que é justamente os acessos que foram dados através daquela máquina, os programas instalados, e as pessoas são muito imprudentes que acham que um programa é inocente, que isso é a mesma coisa que você tomar um doce de uma criança. (E3)

Os programas maliciosos são descritos pelo participante como fonte de problemas, ao mencionar que quando está no setor de informática, percebe que "chegam computadores com problemas". Para ele, o acesso administrativo dado ao usuário para instalar programas deve ser restringido, já que para o participante essa prática pode ser comparada a "tomar um doce de uma criança", no sentido de facilitar a infecção por malware ou a invasão de *hackers*.

A percepção de E3 encontra amparo teórico na literatura e nos fatos, pois além de suas falas corroborarem autores como Rao e Nayak (2014) e Green e Dorey (2016), observa-se no dia a dia da empresa que usuários possuidores de permissões administrativas por vezes instalam programas potencialmente inseguros em seus computadores.

Verifica-se na sequência a Figura 20, que faz apresenta detalhes das menções dos participantes da pesquisa à segurança na navegação de websites e a instalação de programas:

Figura 20 – Menções dos participantes acerca da navegação de websites/instalação de programas.



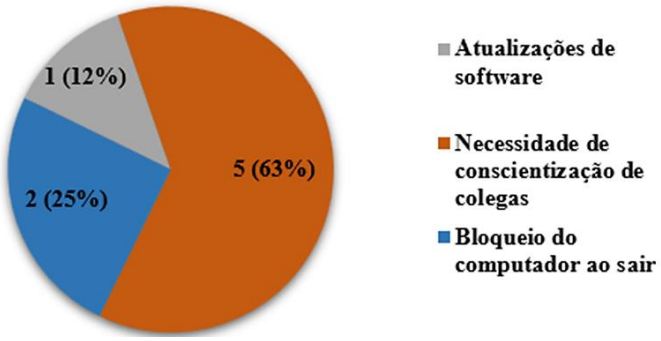
Fonte: Dados da pesquisa (2023).

Verifica-se ao analisar a figura que 02 entre 07 (28%) entrevistados mencionaram espontaneamente que evitar navegar e inserir dados em websites potencialmente perigosos é importante à SI, e 01 (14%) deles mencionou os dois aspectos: o cuidado com websites e programas maliciosos. Vale ressaltar que os outros 05 participantes não mencionaram o cuidado com essas práticas como importantes para a proteção à informação.

4.1.1.7 Outros fatores citados

Serão apresentados e discutidos agora os demais fatores de proteção à informação citados pelos entrevistados, mencionados em menor frequência do que os anteriores. Foram 03 fatores, distribuídos conforme a Figura 21, exposta na sequência.

Figura 21 – Demais fatores de proteção à informação mencionados pelos entrevistados.



Fonte: Dados da pesquisa (2023).

Iniciando a análise pelo aspecto do bloqueio do computador ao ausentar-se da estação de trabalho, essa prática foi mencionada por duas entrevistadas: E7, que afirmou que não tem tal hábito, e E5, que afirmou expressamente que costuma bloquear o computador ao sair:

> Agora... Eu não saio para deixar meu computador aberto. (E5)

De acordo com a literatura, as boas práticas de proteção à informação afirmam que em ambientes corporativos o computador deve ser bloqueado caso o empregado se ausente de seu posto de trabalho. Autores mencionam que algumas organizações possuem severas sanções em caso de mau uso de credenciais de acesso, o que pode ser representado por e-mails enviados sem consentimento, arquivos deletados e sites pornográficos visitados. Logo, aplica-se nesses casos o princípio do não-repúdio, que representa a incapacidade do responsável pelas credenciais de acesso de se eximir de qualquer responsabilidade em caso de mau uso por terceiros (HAEUSSINGER, 2017; MASUCH ET AL., 2021).

No tocante ao hábito de manter atualizados o sistema operacional e os programas utilizados nos dispositivos, 02 menções foram feitas por E2, a saber:

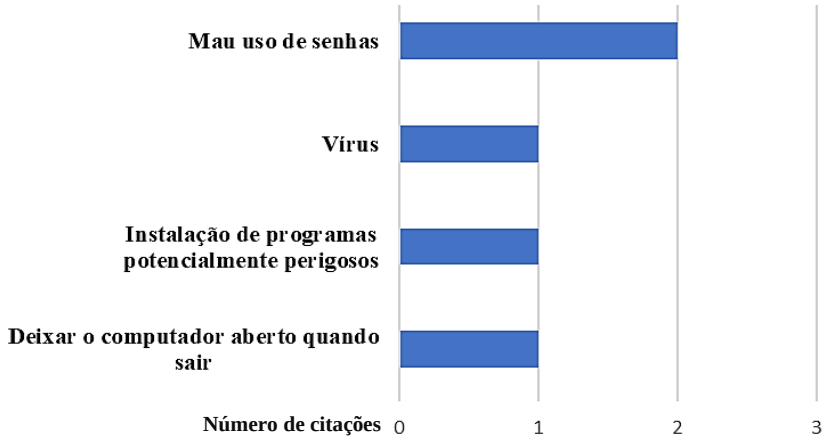
> Quando vem a questão da atualização para mim é um horror. De vez em quando eu atualizo, nem sempre eu não atualizo. (E2)

> Me causa alguns prejuízos, eu não avanço muito na questão de buscar as informações que eu quero, porque há um impedimento se eu não atualizo. Sim, para mim me dá muita dor de cabeça, porque sempre, sempre tão pedindo para atualizar. E eu sempre digo não. Mais tarde, agora não... E aí passa o tempo. Mas eu sei, que eu já ouvi falar que é um risco você não estar atualizado. (E2)

Como já mencionado no tópico referente ao aspecto da baixa sensação de autoeficácia, a participante afirma enfaticamente considerar incômodas as solicitações de atualização dos programas, sobretudo do sistema operacional. Declarou que apesar de ter ouvido falar que é um risco não fazer, tem baixa sensação de autoeficácia nesse sentido, e que adia as instalações sempre que possível. Todavia, atualizações fornecem correções de desempenho e segurança que reforçam a capacidade de defesa de todo o sistema, corrigindo falhas que são exploradas pelos *hackers* (HADNAGY, 2018).

Trazendo à atenção a análise do fator mais mencionado - a percepção de que se faz necessário conscientizar colegas de trabalho - foram 05 menções distribuídas em fatores listados no Gráfico 01.

Gráfico 01 – Aspectos nos quais os participantes sugerem conscientizar colegas.



Fonte: Dados da pesquisa (2023).

Partindo para a análise do primeiro aspecto mencionado, o mau uso de senhas por colegas, os entrevistados fizeram os seguintes relatos:

> Então, se eu tentar entrar num site malicioso, vai funcionar. Isso vai. Às vezes, às vezes eu tenho impressão, sabe, Filipe, que as pessoas ainda não entenderam a responsabilidade que é quando receber uma senha daqui da empresa. Eu acho que não entenderam. E a gente tá vivendo no mundo, cara, que não dá pra você baixar a guarda pra nada. Infelizmente. (E3)

Ao comentar sobre os riscos à visitação de websites potencialmente perigosos, conforme exposto no tópico anterior, E3 chama à atenção de que colegas fazem acesso a sites dessa natureza, os quais ele chama de sites maliciosos. Comenta ainda acreditar que é necessário ter responsabilidade para possuir uma senha de acesso fornecida pela empresa, o que acredita não acontecer com muitos colegas, ao afirmar que as pessoas ainda não entenderam a responsabilidade que é receber uma senha da empresa.

Apesar da maioria das senhas fornecidas pela organização terem acesso limitado à rede interna e a websites externos, ainda concedem ao usuário a capacidade de excluir alguns arquivos armazenados em rede e acessar a internet. Faz-se necessário, assim, exercer o uso dessas credenciais de acesso com responsabilidade, de acordo com Thompson e Mayhorn (2012) e Green e Dorey (2016). E7 também tem a percepção de que, caso seja feito mau uso de senhas, fazendo com que elas cheguem a pessoas mal intencionadas, pode haver risco de invasão ao ambiente seguro da organização:

> É possível, caso alguém de dentro passe o acesso. Se ocorrer de alguém aqui de dentro informar algo, aí entra. A atitude das pessoas pode colocar em risco. E não sei o que pode acontecer nesse caso... (E7)

Apesar de mencionar que não sabe que implicações podem existir caso haja uma invasão por alguém mal intencionado, E7 acredita que os colegas devem estar conscientes de que perigos podem ocorrer diante de uma má gestão das senhas fornecidas pela organização. No que diz respeito à proteção contra vírus, E1 demonstra se preocupar com um possível mau uso dos computadores no ambiente da empresa, que pode culminar na ameaça à integridade de dados importantes do setor em que trabalha:

> Se um vírus entrar nesse arquivo e destruir [dados importantes – grifo nosso], como é que eu vou prestar conta à contabilidade? Vai, vai ficar o quê? A contabilidade vai

> ficar desprotegida? O setor vai ficar desprotegido pelo mau uso de informação, de vírus. (E1)

Para E1, o mau uso das informações aqui representado pela infecção por vírus do computador que um colega utiliza, que pode fazer com que a informação necessária ao setor de contabilidade seja destruída, deixando assim o setor de patrimônio (no qual o entrevistado trabalha) "desprotegido". Logo, para ele, deve haver maior conscientização da força de trabalho da empresa acerca do risco que os vírus trazem à organização. Além de já ter mencionado sua preocupação a respeito desse tipo de ameaça, a percepção de E1 encontra aderência técnica na literatura, pois vírus têm a capacidade de destruir dados e informações (WHITMAN; MATTORD, 2017).

Já no tocante à instalação de programas potencialmente perigosos, E3 menciona a necessidade de alinhamento dos empregados no que tange à instalação de programas nos computadores fornecidos:

> Tem comportamentos aqui que colocam em risco esses dados. Você vê quantas vezes chega na informática computadores que para você chega com problema que você vai descobrir qual o problema, mas justamente os acessos que foram dados através daquela máquina, os programas instalados e as pessoas são muito imprudentes que as pessoas acham que um programa é inocente, que isso é a mesma coisa que você dar um doce a uma criança. (E3)

Além de observar o uso indevido de computadores por parte dos usuários, o entrevistado menciona o fornecimento pelo setor de informática de credenciais com permissão administrativa a essas pessoas, que pode conduzir à instalação de programas maliciosos e trazer riscos à segurança da informação da organização. Por fim, o último aspecto mencionado pelos entrevistados foi relatado por E3, que tem a ver com a atenção ao bloqueio do computador ao ausentar-se da estação de trabalho:

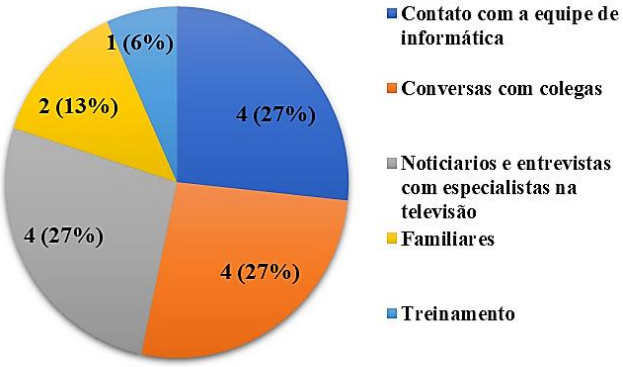
> As pessoas tem uma péssima mania aqui que é de deixar... Eles abrem e-mail e eles vão até embora e fica tudo aberto. Cara, saiu... Desliga o computador! Porque... O que tem aberto na tela... Você sabe que você acessa o computador, a empresa, por exemplo, isso não estou falando da empresa, mas isso se repete no dia a dia. Você abriu ali, você tinha uma senha inicial que você deu acesso à rede. Aí a pessoa dever sai e deixa ligado ali, cara. Então qualquer pessoa ali que quiser acessar o que imaginar através daquela senha de acesso, independentemente de ser, por exemplo: "Ah, mas eu não deixei a senha do Expresso [e-mail corporativo – grifo nosso] aberta". Mas você deixou a sua senha do computador de acesso à internet ligada. (E3)

Conforme já mencionado no início desse subtópico, é fundamental à SI organizacional manter o computador bloqueado ao ausentar-se da estação de trabalho, conforme Haeussinger (2017) e Masuch *et al*. (2019). Finalizando o bloco da compreensão acerca dos conhecimentos técnicos dos participantes, parte-se para a análise de suas respostas sobre o processo de construção dos conhecimentos declarados.

4.1.1.8. Processo de construção do conhecimento técnico dos participantes

Busca-se, nesse subtópico, apresentar e discutir o processo de construção do conhecimento técnico declarado pelos participantes em suas respostas às questões anteriores. Ressalta-se que em virtude da característica do instrumento de coleta de dados, os entrevistados estavam livres para expressar-se, podendo citar mais de uma fonte de conhecimento em suas respostas. Será exposta, na Figura 22, a representação gráfica das menções relatadas pelos entrevistados:

Figura 22 – Fontes de informação que os entrevistados utilizaram para construir seus conhecimentos técnicos acerca da SI.



Fonte: Dados da pesquisa (2023).

Observa-se assim que as fontes mais citadas foram o contato com a equipe de informática, conversas com colegas e noticiários e entrevistas com especialistas exibidos na televisão, com 04 menções cada uma. Acerca do contato com a equipe de informática, os entrevistados afirmaram:

> Eu não fiz curso de nada. Sobre informática eu vim a adquirir mais conhecimento estando lá, na informática. Trabalhei muito tempo na área administrativa, tive a oportunidade de ir para a informática, e sobre informática eu vim a adquirir mais conhecimento estando lá, na informática, que hoje eu não estou, certo? E isso foi pra mim foi fundamental a minha ida para a informática, vendo que tudo que é necessário dentro de uma empresa tem que ter um backup, tem que ter armazenamento de informações, e se tem armazenamento de informações é uma segurança para você e para a empresa, né? (E1)

O usuário afirma que não participou de cursos, e todo o seu conhecimento sobre boas práticas em segurança da informação são oriundos de sua experiência no setor de informática, onde trabalhou por 03 anos. Já E3, que apesar de não ter trabalhado na equipe de informática, tem bastante contato e afirmou que por vezes acompanha o dia a dia do setor:

> Convivência com o setor de TI, por meio de conversas com a equipe e acompanhamento do dia a dia. (E3)

E conforme mencionado anteriormente, E4 está sempre fazendo questionamentos técnicos e sanando dúvidas que tem na utilização dos dispositivos digitais que utiliza, sobretudo o computador:

> Vocês estão conversando aqui com a gente, vocês passam informação pra a gente. (E4)

E2 também menciona que tem o costume de ir ao setor de informática solicitar auxílio técnico e sanar dúvidas:

> Você vê que eu venho sempre aqui, né? Assim, na própria empresa não é o que é, mais especificamente, no setor de informática, há essa preocupação também de quando surge qualquer coisa eu corro pra cá. (E2)

Com efeito, autores como Hargittai e Dobransky (2017) e Hadnagy (2018) afirmam que a disponibilização de canais de comunicação eficientes é fundamental à conscientização de

usuários em direção à utilização mais segura da tecnologia digital. Convém frisar que Llorente-Barroso *et al*. (2018) e Frik *et al*. (2019) recomendam o mesmo, especialmente em organizações com a mão-de-obra envelhecida, já que os mesmos possuem maior resistência no aprendizado de novas tecnologias.

Outra fonte de conhecimento citada pelos participantes foi a conversas com colegas, sobre as quais mencionam:

> Conversando com colegas, pessoas até de outra instituição, entendeu? (E4)
>
> Surgiram do dia a dia. De conversas... (E5)
>
> Assim de outras pessoas caírem nesse...experiência dos outros. (E6)
>
> Só ouvi falar de conversas mesmo. (E7)

Observa-se aqui a importância declarada das conversas com colegas para a constituição do conhecimento sobre tecnologia segurança da informação dessas pessoas. Green e Dorey (2016) mencionam que assim como uma fofoca, o conhecimento técnico ao ser transmitido de maneira informal, especialmente por pessoas leigas, usualmente é difundido com inconsistências e podem não condizer com as melhores práticas.

Outro dado trazido sob o prisma da formação de conhecimento dos participantes foi a importância da televisão e seus noticiários, citada por exibir notícias e entrevistas de especialistas na área de tecnologia da informação. Nesse contexto, os entrevistados mencionaram:

> A mídia alerta a gente, a televisão alerta a gente pra gente já ficar meio atento, como é o caso de fraude bancário, de conta bancária, a gente já fica ligada. (E5)
>
> Eu ouvi mais isso... Noticiário de televisão, conversando com colega, pessoa até de outra instituição, entendeu? Na televisão de vez em quando sai... Tal instituição tá fora do ar, perde os dados... A televisão cansa muito de falar isso. Você às vezes tá conversando com colegas... Então foi mais noticioso, noticiário, e informação conversando com colegas. (E4)
>
> Noticiários... (E3)
>
> Noticiário, tem entrevistas sobre segurança da informação. (E2)

Li e Luximon (2016) mencionam a influência que a mídia televisiva tem sobre os sêniores, e afirmam que esse grupo de cidadãos é o que mais consome esse tipo de conteúdo dentre todas as faixas etárias. A pesquisa também trouxe o dado de que familiares, usualmente os mais jovens por terem maior habilidade na operação de aparelhos digitais, também servem como fonte de conhecimento e auxílio para os entrevistados:

> Meus sobrinhos são mais novos, sabem e entendem dessa questão aí, e eu estou sempre os procurando. (E2)
>
> Tiro dúvidas com meu filho... (E7)

Llorente-Barroso *et al*. (2018) citam que os sêniores tendem a buscar ajuda com familiares mais jovens quando têm dúvidas na operação dos aparelhos. As autoras afirmam ainda que a presença dessas pessoas pode acelerar o aprendizado na operação de *smartphones* e seus aplicativos, auxiliando no aumento da sensação de autoeficácia e independência dos mais

velhos. Por fim, o último aspecto citado como fonte de informações para os usuários sêniores entrevistados foram os treinamentos, mencionados por E5:

> Treinamento, que sempre nos treinamentos que a gente faz, é falado sobre a segurança da informação no ambiente de trabalho dedicado da gente. O conselho mesmo é um, que quando dá curso, sempre questiona esse lado de segurança (E5)

Convém frisar, a partir da declaração de E5, que o treinamento mencionado é focado em questões contábeis, e que nesses eventos também são transmitidas informações sobre proteção à informação. Treinamentos são apontados por diversos autores como mitigadores de riscos à SI em ambientes corporativos, pois assegura a transferência de conhecimento fidedigno e tende a gerar engajamento e conscientização na força de trabalho, segundo Lyra (2015), Haeussinger (2017) e Stelzer *et al*. (2019).

Todavia, autores como Friedberg (2001) e Gardner e Thomas (2014) trazem ao debate que empresas com uma mão-de-obra envelhecida por vezes tendem a investir menos em treinamentos para os sêniores, uma vez que estão próximos à aposentadoria, e, ao mesmo tempo, os sêniores perdem interesse em serem treinados pelo mesmo motivo.

Findada a exposição e discussão de aspectos cognitivos verificados na pesquisa, parte-se à análise dos aspectos comportamentais mencionados e observados no ambiente organizacional.

4.2. Aspectos Comportamentais

Conforme exposto anteriormente, os aspectos comportamentais em proteção à informação são apoiados em aspectos cognitivos, uma vez que o comportamento do usuário em segurança é baseado em seus conhecimentos acerca dos riscos e de procedimentos de defesa (HAEUSSINGER, 2017; ISO, 2022). Dito isto, são apresentados e discutidos os dados relacionados a essa etapa, obtidos principalmente por meio da definição das Questões 04, 05 e 06 do roteiro de entrevistas com o objetivo de conhecer a percepção dos usuários acerca de seu comportamento de proteção à informação. Adicionalmente, serão trazidos à discussão as observações realizadas pelo o autor da pesquisa, quando do acompanhamento das atividades diárias da organização.

A discussão é assim iniciada com a exposição dos aspectos comportamentais citados, que podem ser visualizados no Quadro 10.

Quadro 10 – Aspectos comportamentais, aspectos mencionados e respectivas frequências de citações.

Dimensão	Fator	Nº de citações	Citações espontâneas
Aspectos Comportamentais	Busca por informações sobre potencial risco	10	10 (100%)
	Cautela diante de potencial risco percebido	10	8 (62%)
	Contato frequente com o setor de TI	7	4 (50%)
	Preocupação com possíveis prejuízos que podem advir de um uso não seguro	6	3 (50%)

Fonte: Dados da pesquisa (2023).

A partir do Quadro 10 podem ser visualizados os aspectos relacionados ao comportamento de proteção à informação mencionados pelos participantes, juntamente com a quantidade e proporção de citações espontâneas de cada fator. No Quadro 11, exposto a seguir, são apresentadas as definições de cada aspecto citado e suas respectivas bases teórica.

Quadro 11 – Definições gerais dos aspectos comportamentais mencionados.

Aspecto comportamental	Definição	Base teórica
Cautela diante de risco percebido	Usuário(a) declara ser cauteloso(a) em face de uma situação de risco percebido.	Lohani (2019)
Busca por informações sobre potencial risco	Entrevistado(a) declara costumar buscar informações sobre potencial ameaça percebida, antes de realizar ação que considera de risco.	Masuch *et al*. (2021)
Contato frequente com o setor de TI	Participante recorre frequentemente ao setor de TI da empresa para obter suporte e informações sobre a utilização de dispositivos digitais	Hadnagy (2018)
Preocupação com possíveis prejuízos que podem advir de um uso não seguro	Entrevistado(a) declara que possíveis prejuízos o(a) influenciam a buscar utilizar dispositivos de maneira mais segura.	Green; Dorey (2016)

Fonte: Dados da pesquisa (2023).

Uma vez apresentados os fatores e suas respectivas definições, parte-se à análise das menções dos participantes. A apresentação será ordenada de acordo com o número de citações de cada fator, e esses serão discutidos em respectivos subtópicos, assim como foi feito na exposição dos aspectos cognitivos. Dito isto, inicia-se a análise dos aspectos comportamentais com a discussão acerca da cautela diante de potencial risco percebido declarada pelos participantes.

4.2.1. Cautela diante de potencial risco percebido

De acordo com Whitman e Mattord (2017) e Lohani (2019), é preciso que o usuário utilize dispositivos digitais de maneira cautelosa, ciente de que possíveis riscos e ameaças podem advir de uma ação a ser executada. Nesse ínterim, a literatura recomenda ao usuário seguir o que se recomenda nas boas práticas de SI, evitando assim danos à confiabilidade, integridade e disponibilidade de dados e informações pessoais ou corporativos.

Com efeito, os entrevistados declararam exercer um comportamento cauteloso quando deparados com situações que julgam potencialmente perigosas. Isso significa, nesse contexto, não executar arquivos desconhecidos, não enviar de dados sensíveis a desconhecidos nem os inserir em websites não confiáveis, fazer download e executar anexos de e-mail não reconhecidos dentre outras práticas (WHITMAN; MATTORD, 2017; FBI, 2023).

Em suma, diz respeito à cautela diante de uma situação que o usuário julga potencialmente perigosa. Os primeiros exemplos de menções a esse respeito são declarações de E1, que apresentam a preocupação do usuário no cuidado na execução de arquivos desconhecidos em computadores:

> Olha, quando eu, quando eu vejo cada informação que eu não tenha conhecimento certo, eu jamais abro aquele arquivo porque corro o risco de ser uma fraude, certo? (E1)

O usuário afirma condicionar a execução de arquivos à possessão de “conhecimento certo”, ou seja, há por parte dele a necessidade de saber da procedência do arquivo e de sua finalidade. Percebe-se, ao final da fala do participante, que a execução do arquivo pode culminar na facilitação a uma fraude, e por isso considera necessária a cautela. Adicionalmente, o entrevistado diz pensar que tal cuidado também se faz importante na navegação e inserção de dados em websites:

> Você tem que ter muita cautela no caso de você abrir qualquer site que é designado a você fazer isso, porque você corre o risco de em um acesso desse dar informações

> indevidas. Essa informação é prejudicial a você mesmo você sofrer vários danos, vários danos a si próprio, e você ser altamente auto prejudicado. (E1)

Após mencionar que prejuízos podem advir de ações descuidadas nesse sentido, mesmo sem detalhar de que ordem tais prejuízos seriam, E1 diz que tanto ele quanto a empresa podem ser prejudicados, caso informações sensíveis forem inseridas em websites não confiáveis ou enviados via mensagens de e-mail sem a cautela necessária:

> Ou dar informação errada, se eu fornecer qualquer informação que não esteja dentro do meu conhecimento, eu vou ser prejudicado. Para mim, responder aquela informação que veio para mim eu não abro, jamais eu faço isso porque, como eu acabei de citar, pode ser uma fraude. Posso me prejudicar, prejudicar a empresa, certo? (E1)

Green e Dorey (2016) e Whitman e Mattord (2017) mencionam que a falta de percepção de riscos por parte dos usuários é o principal motivo para incidentes de segurança. Diante disso, o cuidado declarado por E1 e por outros entrevistados com a manipulação de dados e informações corrobora as boas práticas de proteção à informação, em se tratando da exposição a ameaças de segurança:

> Você tem que ter muita cautela no caso de você abrir qualquer site que é designado a você fazer isso, porque você corre o risco de em um acesso desse dar informações indevidas. Essa informação é prejudicial a você mesmo você sofrer vários danos, vários danos a si próprio, e você ser altamente auto prejudicado. (E1)

> Diante das informações que já tive, escuto noticiários, pessoas que já foram e sofreram, vamos dizer assim, com esse tipo de informação eu não mexo ou deleto. (E2)

Verifica-se que tanto E1 como E2 afirmam terem cuidado quando deparados com mensagens de e-mail, tanto em sua abertura quanto no ato de respondê-las. Vale ressaltar a menção de E2 às experiências relatadas de outras pessoas, que segundo sua fala, a faz ter cuidado quando percebe estar em situações semelhantes.

> Dependendo do conteúdo, se eu receber um arquivo ou e-mail, seja o que for, que for totalmente assim, distante do que eu trabalho, vamos supor, vou dar um exemplo que eu recebi: “sua senha do Itaú precisa ser alterada” ... Pô, eu nunca tive conta no Itaú. Eu nem vou lá. Por exemplo, recebi algum informe sobre treinamento da área de geoprocessamento. Eu vejo mais ou menos de quem é e vou por fora, eu não abro aquele arquivo. Vamos supor, recebi da empresa Filipe e companhia, eu vou fazer uma pesquisa sobre quem é Filipe e companhia. Entendeu? Então assim, não é por que é relativo à minha área de trabalho que eu abro. Ah, se foi alguém que eu fiz contato anterior e vem em forma de resposta, até sim, mas aleatoriamente... Eu nem abro, em caso de dúvida. Primeiro que eu não sei como eles chegaram até mim. Então, se eles chegaram de alguma maneira, não sou eu que vou dar mais informações além das que eles já têm. (E3)

> Geralmente não abro. Não abro, geralmente. Dificilmente eu abro. Meu computador particular o procedimento também é o mesmo, é coisa desconhecida, assim, não abro. No telefone, deleto. Justamente por causa dessas coisas. Hoje em dia, tem que ter cuidado. (E4)

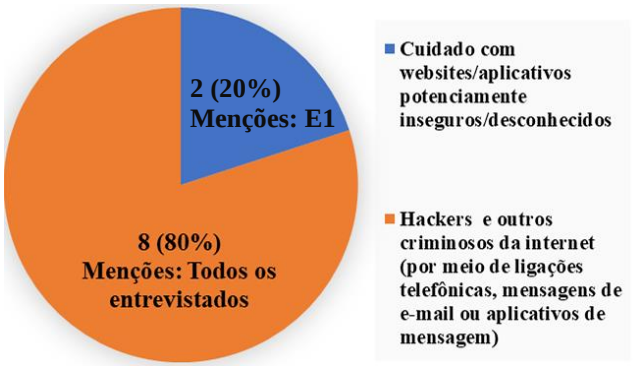
Os relatos de E3 e E4 aqui também dizem respeito a práticas recomendadas trato com e-mails de fontes desconhecidas, demonstrando preocupação inclusive com possíveis danos a computadores da organização.

> Não abro. Olha, estão efetuando uma compra na loja Bahia, não sei o que... Vários... Não abro. (E5)
>
> Eu não atendo, faço de conta que não estou, que não recebi. Uma vez não atendo, mas se for duas vezes sim, mas se for uma vez só, não deve passar, sabe? Mas se persistir, aí sim. (E6)
>
> É só você não passar seus dados, se passar seus dados, já era... Eu bloqueio [números estranhos e e-mails desconhecidos – grifo nosso]. No telefone mesmo, vem esses números estranhos pedindo os dados, eu bloqueio. No computador também, eu não abro, porque se você abrir você vai tá facilitando. (E7)

Percebe-se que as entrevistadas E5, E6 e E7 demonstram preocupações sobretudo com ameaças a dados e dispositivos pessoais, seja em portais de compras ou ligações telefônicas que consideram possivelmente fraudulentas. Segundo Lyra (2015), essas práticas são de fato recomendadas, embora seja possível notar uma maior preocupação de alguns participantes com danos que podem ser causados à organização por meio desses tipos de ameaça.

Os pressupostos teóricos apontados no estudo apontam que um usuário só tem a capacidade de reconhecer uma ameaça se houver algum nível de conhecimento sobre ela (FRIK ET AL., 2019; ISO, 2022). Dessa maneira, pode-se traçar um paralelo de aspectos cognitivos que influenciam os participantes a exercer um comportamento cauteloso em situações de potencial risco, de acordo com as boas práticas de segurança da informação. Tal paralelo pode ser observado na Figura 23.

Figura 23 – Relação de aspectos cognitivos que foram mencionados como influenciadores da cautela dos participantes no uso da tecnologia digital.



Fonte: Dados da pesquisa (2023).

A cautela na navegação de websites e execução de aplicativos foi mencionada apenas por E1, citada 02 vezes pelo entrevistado em sua resposta à Questão 05. O participante também menciona ser cauteloso quando considera mensagens de e-mail, websites e arquivos potencialmente inseguros. Quanto aos outros entrevistados, mencionam serem cautelosos apenas ao ler e clicar em anexos de e-mails, enviar dados pessoais para desconhecidos e inseri-los em websites.

Autores como Green e Dorey (2016) e Masuch *et al*. (2021) afirmam que, além de evitar as ameaças por ter cautela no uso da tecnologia, a busca por informações pelo usuário quando exposto a situações de risco é fundamental à proteção à informação. Esse aspecto foi mencionado também pelos entrevistados, e será analisado na sequência.

4.2.2. Busca por informações sobre potencial risco ou ameaça

Em face de situações de risco, boas práticas de proteção recomendam que os usuários busquem informações acerca de potenciais ameaças com que se deparam em sua utilização de

dispositivos digitais, conforme Green e Dorey (2016), Haeussinger (2017) e Masuch *et al*. (2021). Proceder dessa maneira, segundo os autores, torna possível ao usuário identificar as causas e consequências da possível ameaça, evitando assim danos à segurança dos dados. A busca por informações diante de ameaças, segundo Llorente-Barroso *et al*. (2018) também tende a auxiliar no desenvolvimento da autoeficácia nos usuários, sobretudo dos sêniores.

Nesse sentido, a maioria dos participantes da pesquisa demonstraram ter o hábito de buscar informações sobre como proceder quando deparados com ameaças reconhecidas, conforme os relatos de 06 dos 07 participantes:

> Bem, dessa forma eu vou primeiro, vou dar, vou ligar para ver se esse site é verdadeiro ou é mentiroso. Eu vou tomar um caminho... Qual o caminho? Fazer várias pesquisas, perguntar a um, perguntar a outro que já teve essa informação para me informar, para dar fornecimento a pessoas confiáveis e não a pessoas indevidas, que ele faz uma pergunta, eu vou e abro o site, ele vai ter acesso à minha conta e vai me prejudicar na frente ou a empresa que eles estão querendo esse acesso. Jamais eu faço isso. (E1)

> [Quando perguntado se costuma buscar informação quando deparado com possível ameaça – grifo nosso] Depende. Depende do tipo de informação que chega até mim. É como eu tô te dizendo, se for algo que me desperte a atenção, mas não tenho convicção que devo abrir, eu vou buscar informação com vocês lá [equipe de suporte], caso contrário eu deleto e nem abro. (E3)

Percebe-se que os participantes E1 e E3 dizem consultar pessoas técnicas e vistas como confiáveis, além de fazerem pesquisas por conta própria acerca de possíveis situações de risco. Tal prática consiste em um comportamento recomendado pela literatura, pois evita a execução de programas maliciosos, o fornecimento de dados sensíveis e de outras ameaças de SI (WHITMAN; MATTORD, 2017).

> E aí eu procuro informação... Já com vocês, por exemplo, já teve caso do Banese (Banco do Estado de Sergipe). Eu já fui no Banese, entendeu? Pegar a informação com o cara. Aí disse: não abra, não abra não porque é vírus, é não sei o que. Quando é de banco, então, eu procuro me informar. Eu só tenho praticamente com o Banese, então, qualquer coisa, vou ali no bigodinho [caixa do Banese – grifo nosso]. (E4)

> Sobre o caso da invasão do CRC [Conselho Regional de Contabilidade – grifo nosso]: Eles fizeram contato com outros órgãos de segurança da informação e disseram até que tem um protocolo. Eu estou com toda a documentação que eu imprimi para poder ter, que o amanhã a gente não sabe, né, Filipe... O que pode, porque a gente tem tudo lá, a nossa vida. De maneira geral eu procuro informação. Procuro informação de alguém que entenda, que saiba mais do que eu que possa me ajudar. Eu vou pro site que me mandou [a mensagem possivelmente fraudulenta – grifo nosso]. (E5)

Ressalta-se aqui o relato mencionado pela entrevistada E5 sobre seu conhecimento acerca da citada invasão aos sistemas do CRC, e uma consequente busca por informações sobre como evitar problemas semelhantes em outros ambientes, a exemplo da própria EMDAGRO.

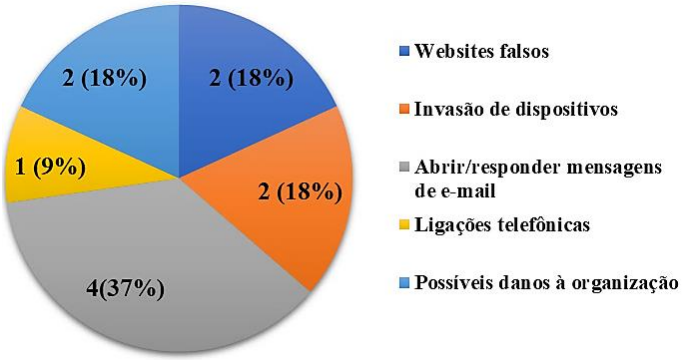
> Eu consulto muito quando eu faço compra, consulto muito com o Reclame Aqui. Se eu acho que aquele site é muito bom de reclamação, então eu consulto. Quando recebo mensagem de banco, eu vou consultar o banco que me mandou, e se for uma empresa que eu comprei alguma coisa, eu vou lá pra ver, pra ter certeza mesmo. Agora pagar um boleto sem ter certeza eu não pago nada. (E6)

> Quando aparece alguma coisa eu pergunto a pessoas que entendem mais, a vocês [do setor de informática – grifo nosso], pergunto a meu filho... Ele manda recusar ou bloquear esse número... Porque se bloquear não vem mais. (E7)

Mais uma vez, percebe-se que alguns participantes, apesar de mencionarem exercer práticas tecnicamente adequadas, demonstram que suas preocupações são voltadas a evitar consequências de ordem pessoal, a exemplo de perdas financeiras ou o acesso a dados pessoais.

A Figura 24, exposta na sequência, apresenta as potenciais ameaças percebidas pelos entrevistados que os fazem buscar informações.

Figura 24 – Situações de potenciais ameaças percebidas pelos usuários que os fazem buscar informações.

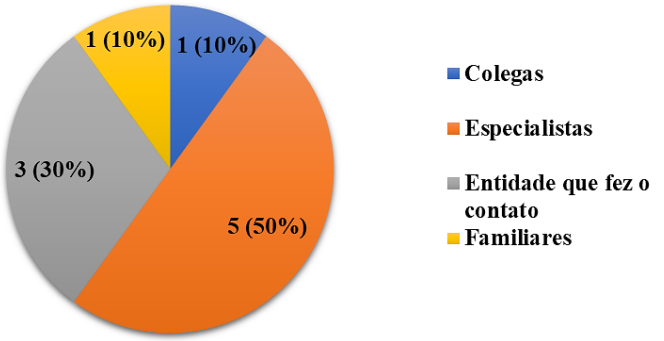


Fonte: Dados da pesquisa (2023).

Percebe-se que a preocupação dos usuários nesse sentido é voltada a situações nas quais são percebidos riscos de prejuízos financeiros, perpetrados por meio do furto de dados pessoais via websites falsos, invasões de dispositivos ou mensagens de e-mail. Tentativas de fraude por ligações telefônicas também são citadas como motivo para buscar informações, conforme mencionado por E7. A preocupação com possíveis prejuízos de tais ameaças à organização foi relatada apenas por dois entrevistados (E1 e E5), que se referem à necessidade de buscar informações sobre como utilizar dispositivos de maneira segura.

No tocante à fonte de informação que é recorrida nas situações relatadas, observa-se que a maioria consulta especialistas, a exemplo da equipe de TI da organização e websites especializados na internet. Os participantes também mencionaram fazer consultas a colegas e a familiares, às entidades que supostamente tentaram contato por meio de ligações telefônicas ou e-mails, fraudes conhecidas como *phishing*, que simulam portais e aplicativos de bancos, lojas virtuais ou outras empresas. Esse cenário pode ser observado na Figura 25.

Figura 25 – Fontes de informação consultadas pelos entrevistados quando deparados com situações que consideram de risco.



Fonte: Dados da pesquisa (2023)

As boas práticas em proteção à informação sugerem que se busquem informações com especialistas, sobretudo quando em face de potenciais ameaças. Para autores como Whitman e Mattord (2017) e Llorente-Barroso *et al*. (2018), fontes de informações confiáveis no sentido técnico são fundamentais à conscientização com vias à utilização segura de dispositivos digitais. Logo, as práticas mais frequentemente declaradas pelos entrevistados, com 05 menções

de consultar a equipe de suporte de TI e outras fontes de conhecimento técnico especializado é conforme ao recomendado pelos autores.

03 entrevistados também declararam consultar bancos e empresas acerca de mensagens recebidas por e-mail, ligação telefônica ou mensagem de texto. O hábito de sanar dúvidas com a própria entidade que fez o contato para inquirir acerca da legitimidade da mensagem também é recomendada, de acordo com Green e Dorey (2016) e FBI (2023). As demais menções dizem respeito a consultas feitas a colegas e familiares que os participantes consideram mais tecnicamente capacitados.

4.2.3. Contato frequente com o setor de TI

Outro aspecto mencionado pelos entrevistados foi a prática de manter contato frequente com a equipe de TI da organização, que segundo a literatura especializada, aproxima usuários das melhores práticas em SI (HADNAGY, 2018; FRIK ET AL., 2019). Para Green e Dorey (2016) e FBI (2023), a transferência de conhecimento que é proporcionada pela interação entre especialistas e usuários, juntamente com o desenvolvimento de políticas de segurança, são fundamentais à conscientização em SI em organizações, bem como contribuir ao aumento da sensação de autoeficácia dos usuários.

Dito isso, alguns participantes declararam exercer esse comportamento, sobretudo por meio da presença física no setor de informática:

> Trabalhei muito tempo na área administrativa, tive a oportunidade de ir para a informática, e sobre informática eu vim a adquirir mais conhecimento estando lá, na informática, que hoje eu não estou, certo? E isso foi pra mim foi fundamental a minha ida para a informática, vendo que tudo que é necessário dentro de uma empresa tem que ter um backup, tem que ter armazenamento de informações, e se tem armazenamento de informações é uma segurança para você e para a empresa, né? (E1)

E1 considera, de acordo com seu relato, que o desenvolvimento de seus aspectos cognitivos em relação à SI se deu em virtude de sua experiência no setor de TI, mesmo declarando nunca ter feito cursos na área, conforme mencionado em sua resposta à Questão 04:

> Eu não fiz curso de nada. Eu fui adquirindo no tempo de trabalho um certo? Passei o período lá na informática e vi a muito isso a preocupação do pessoal da informática com dados que nós, que nós vemos a ser perdidos que são, são segurança de trabalho, são segurança de informações que você vai adquirir no dia a dia, né? (E1)

O relato descreve prática semelhante à declarada por E3 em sua resposta à mesma questão, ao dizer que não busca informação sobre conhecimentos de proteção à informação:

> Eu não, eu não busco informação. Dificilmente eu busco informação. Chega até mim, eu não vou, eu não vou buscar a informação. (E3)

É possível observar que E3, apesar de ter declarado ao responder à Questão 04 que não costuma buscar conhecimento espontaneamente sobre SI, menciona que a informação “chega” até ele. Sua resposta à Questão 06 traz informações sobre como seu conhecimento é construído:

> Mas a partir do momento que chega na sua casa, que você sai da rede, do estado, você acessa o que você quiser, a máquina está com você. É isso que eu sei, porque eu já vi aqui jogos, brinquedos e etc. E outras coisas mais que você nem imagina. Coisas mais que você nem imagina. Eu digo porque eu ando muito na informática, eu vejo. (E3)

Após mencionar alguns de seus aspectos cognitivos acerca dos perigos sobre o acesso a redes externas, o participante diz que “anda muito na informática”. Tal relato corrobora o que

é observado pelo autor da pesquisa, descrito no Apêndice A, no relatório de observação 01. As declarações de E4 ao responder à Questão 04 também descrevem um relacionamento próximo com o setor de TI. Essa prática auxiliou o usuário a desenvolver seus aspectos cognitivos observados anteriormente no estudo:

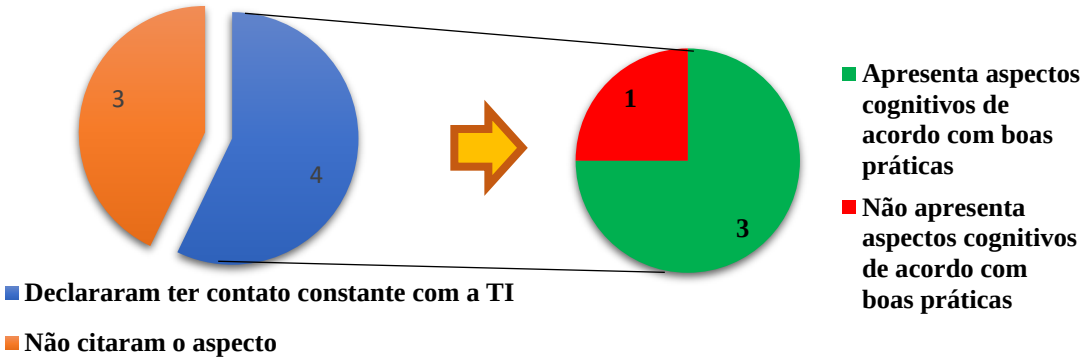
> Então foi mais noticiário, e informação conversando com colegas, até de vocês mesmo. Vocês estão conversando aqui com a gente, vocês passam informação pra a gente. Entendeu? (E4)

A Entrevistada 02 também afirma ter contato constante com a equipe de informática, o que também traz benefícios à construção de seu conhecimento. Todavia, suas visitas limitam-se ao sanamento de dúvidas recorrentes na utilização do computador portátil que utiliza. Suas solicitações mais frequentes dizem respeito à alteração de configurações de rede para conectar-se à rede da empresa, arquivos deletados acidentalmente ou dúvidas na operação do Microsoft Word. O cenário declarado pela participante pode ser observado no relatório de observação 02 (Apêndice B), e no relato feito na resposta da usuária à Questão 03:

> Você vê que eu venho sempre aqui, né? Assim, na própria empresa não é o que é, mais especificamente, no setor de informática, há essa preocupação também de quando surge qualquer coisa eu corro pra cá. (E2)

O comportamento de E2 em sua relação com a tecnologia, apesar de marcado por visitas constantes ao setor de informática, não compartilha do mesmo desenvolvimento de aspectos cognitivos e comportamentais de compliance às políticas de segurança de outros entrevistados, a exemplo de E1, E3 e E4. Nesse sentido, observa-se que dos 07 participantes da pesquisa, 04 afirmaram ter contato constante com a TI. Vale ressaltar que desses últimos, 03 apresentaram conhecimentos técnicos suficientes para uma utilização segura de dispositivos, sobretudo no ambiente da organização. Dito isto, traça-se a Figura 26 para exposição do cenário do contato constante com a TI como possível influenciador do comportamento dos usuários em relação à sua conscientização em SI.

Figura 26 – Influência do contato constante com a TI em relação à conscientização em segurança da informação.



Fonte: Dados da pesquisa (2023).

Ao se analisar a Figura 26, pode-se verificar que dentre os 04 participantes que declararam ter contato constante com a equipe de TI, 03 relataram possuir aspectos cognitivos próximos às boas práticas durante suas entrevistas. Apenas 01 entrevistada (E2) demonstrou baixa sensação de autoeficácia em sua relação com a SI, apresentando poucos aspectos cognitivos em seus relatos e durante a observação por parte do autor da pesquisa.

Com efeito, autores mencionam que o desenvolvimento da CSI depende não só da importante interação entre técnicos e usuários, vista como fundamental à transferência de

conhecimentos, e sim da junção dessa prática com aspectos de processos da organização. Tais aspectos regulamentam a utilização dos dispositivos e estimulam a execução de treinamentos e o compartilhamento de boas práticas em SI (KAMARIZA, 2017; MASUCH ET AL., 2021).

4.2.4. Preocupação com possíveis prejuízos que podem advir do uso não seguro

O roteiro de entrevistas buscou também questionar os participantes acerca dos motivos pelos quais consideram que cuidados são necessários no uso de dispositivos digitais. Com efeito, os entrevistados declararam perceber prejuízos que podem ocorrer caso a utilização não esteja de acordo com as melhores práticas em SI, e o presente estudo pretende lançar olhar a que ordem de prejuízos mencionaram se preocupar e estar conscientes.

Nesse sentido, E1 inicia seu relato mencionando preocupação com sanções administrativas que podem ocorrer caso faça mal uso dos dispositivos digitais no ambiente de trabalho:

> Você tem que ter muita cautela no caso de você abrir qualquer site, porque você corre o risco de, num acesso desse, inserir informações indevidas. Você pode sofrer vários danos, e você ser altamente auto prejudicado. Como eu posso ser prejudicado? Pegar uma suspensão... De trabalho. Ser demitido, por falta de informações... Aí por isso que você tem que ter cautela ao responder qualquer ato desse. Muita cautela, com informações indevidas. (E1)

Mesmo não existindo sanções administrativas previstas no regimento interno da organização, o usuário direciona sua preocupação ao risco de receber suspensões ou até mesmo de ser demitido caso seja responsabilizado pelo mau uso do dispositivo. Apesar de ter apresentado conhecimentos técnicos satisfatórios acerca da proteção à informação em outros pontos da entrevista, E1 não faz menção a riscos de segurança à informação da empresa, a exemplo de destruição ou acesso não autorizado.

Ainda no contexto da responsabilização administrativa, referindo-se indiretamente ao princípio descrito por Haeussinger (2017) do não-repúdio de uma ação indevida, E3 cita preocupação com prejuízos que podem advir de má utilização de credenciais de acesso fornecidas pela organização. Para ele, o mau uso nesse sentido pode causar prejuízos ao usuário:

> Como você trata uma senha de banco, uma senha de e-mail. Isso é sua, É responsabilidade sua também. Qualquer coisa que saia do seu e-mail, não importa quem escreveu, não importa quem mandou, é você. A senha é sua, vai sair em seu nome. (E3)

Posteriormente, tanto o próprio E3 quanto E4 citam situações nas quais prejuízos são possíveis, abordando situações que podem culminar em destruição/alteração/acesso indevido a dados e informações sigilosas:

> Então, se qualquer movimento que você faça, que fuja dentro daquela margem de segurança que o sistema permite, cara, você pode abrir caminho a um invasor. Você pode estar disponibilizando um banco de dados gigante [referindo-se a dados existentes na organização sobre produtores rurais de Sergipe – grifo nosso] que pode ser utilizado das piores formas possíveis. (E3)

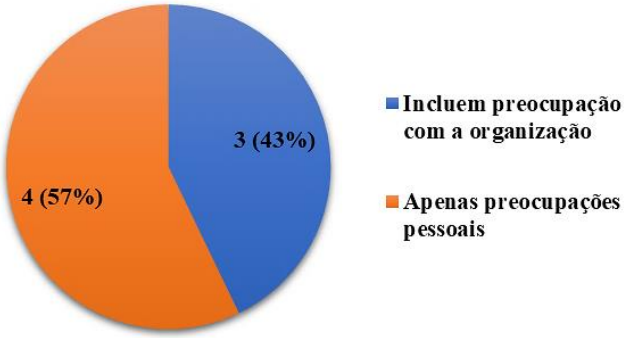
> Pode ser um vírus... Pode ser alguma coisa que... pá! Aí eu prefiro demorar um pouquinho, procurar ver... Até ligar pra o local se for o caso, pra saber. É justamente o medo que você tem de causar algum dano no computador, vírus. Porque já teve de perder dados. Eu perdi tudo ou quase tudo aqui da empresa. (E4)

Conforme já mencionado, tanto o acesso não autorizado ao ambiente seguro da organização quanto a infecção por vírus podem causar sérios danos à integridade dos dados sigilosos da organização, bem como o correto funcionamento dos serviços da empresa (STEWART ET AL., 2015). Outros participantes mencionaram prejuízos de ordem pessoal, sem referência a problemas que podem ser causados à organização:

> Acesso não autorizado a dados pessoais (CPF, dados de cartão, senhas e fotos) e da organização, a exemplo de documentos sigilosos e declarações de imposto de renda. (E5)
>
> Além do financeiro? Porque isso é só prejuízo financeiro. Às vezes você também tem. Um problema de privacidade, também, né? Assim como também é isso que eu quero da minha privacidade, porque você vai afetar um bocado de coisa, né? Seu nome, no caso, não é seu CPF, seu nome, entendeu? Aí você já tá em jogo seus dados. (E6)
>
> Esses aplicativos de celular, de banco, pix... Tem que ter muito cuidado. Tem que tomar cuidado com outros dados também, não só financeiro, como também com dados pessoais. (E7)

É possível perceber que os usuários E5, E6 e E7 citam preocupações com fraudes que visam a subtração de dinheiro e de dados pessoais, sobretudo CPF e números de cartão de crédito. Apesar de se observar que a frequência de crimes dessa ordem contra sêniores estar crescendo anualmente, conforme PWC (2022) e FBI (2023), é possível verificar que não houve preocupação por parte desses empregados com prejuízos à organização. A Figura 27 expõe, na sequência, a situação encontrada.

Figura 27 – Motivos pelos quais os participantes declararam se preocupar com a segurança da informação.



Fonte: Dados da pesquisa (2023).

Observa-se, portanto, que mais da metade dos entrevistados (04, ou 57%) não demonstraram exercer um comportamento de preocupação com possíveis prejuízos à SI da organização. Segundo Kamariza (2017), é importante às organizações delinear políticas para desenvolver a conscientização em segurança da informação, e Green e Dorey (2016) afirmam que políticas tendem a incrementar o conhecimento técnico e a contribuição dos usuários às metas definidas pelos gestores. A limitada observância da organização nesse sentido pode auxiliar na percepção acerca da proporção de entrevistados que não declararam se preocupar com possíveis riscos à segurança da informação da organização.

Parte-se agora à apresentação e discussão dos dados que foram coletados acerca da percepção dos participantes aos aspectos de processos na organização.

4.3. Aspectos de Processos

Como já mencionado, aspectos de processos são medidas tomadas pela organização no sentido de incrementar a segurança da informação em seu ambiente. Para Lim *et al*. (2010), fatores como o reforço a práticas adequadas de utilização por meio de lembretes e avisos, treinamentos, atribuição de responsabilidades no uso de dispositivos e na manipulação de dados e informações, investimentos em segurança e envolvimento do corpo gerencial são maneiras de desenvolver a conscientização em empregados.

Dito isto, a presente etapa do trabalho fará a exposição e discussão da percepção dos participantes acerca de aspectos dessa natureza que porventura existam na organização, ou que os entrevistados considerem importantes, mesmo que não implementados na empresa. Serão discutidas menções a esses aspectos feitas durante as respostas às Questões 07 e 08 do roteiro, além de citações em respostas anteriores e dados da observação no ambiente organizacional.

Parte-se então à exposição de aspectos relacionados a processos percebidos e citados pelos participantes, feita no Quadro 12.

Quadro 12 – Aspectos de processos, aspectos mencionados e respectivas frequências de citações.

Dimensão	Aspecto	Nº de citações	Citações espontâneas
Aspectos de Processos	Envolvimento dos gestores	3	2 (100%)
	Investimento em tecnologia e segurança	2	1 (100%)
	Comunicação da TI com os usuários	7	1 (17%)
	Política de atribuição de responsabilidades	3	2 (100%)
	Políticas de segurança	11	5 (55%)
	Treinamento	6	4 (100%)

Fonte: Dados da pesquisa (2023).

No Quadro 12 estão expostos os aspectos relacionados ao comportamento de proteção à informação mencionados pelos participantes, juntamente com a quantidade e proporção de citações espontâneas de cada um. O Quadro 13, visualizado na sequência, apresenta as definições de cada aspecto e suas respectivas bases teóricas.

Quadro 13 - Definições gerais dos aspectos de processos mencionados.

Aspecto de processos	Definição	Base teórica
Envolvimento dos gestores	Usuário(a) declara considerar importante o envolvimento da chefia na implementação de práticas seguras na organização.	Gardner; Thomas (2014)
Investimento em tecnologia e segurança	Participante pensa que são necessários investimentos financeiros em tecnologia e para incrementar a segurança da informação no ambiente.	Whitman; Mattord (2017)
Comunicação da TI com os usuários	Entrevistado(a) considera importante que sejam utilizados lembretes, avisos ou mensagens de texto/e-mail para comunicar alertas e boas práticas em SI.	Masuch *et al*. (2021)
Política de atribuição de responsabilidades	Usuário(a) pensa que a definição de uma política de atribuição de responsabilização do empregado pelo mau uso de dispositivos é importante à SI da organização.	Gardner; Thomas (2014)
Políticas de segurança	Participante afirma que políticas de segurança são importantes para a manutenção da segurança da informação. Referem-se à disponibilização de recursos de segurança, como antivírus, *backup*, senhas seguras e controle de acesso à internet	Green; Dorey (2016)
Treinamento	Entrevistado(a) considera que treinamentos podem auxiliar a empresa a conscientizar usuários com vias a boas práticas de SI.	Frik *et al*. (2019)

Fonte: Dados da pesquisa (2023).

Apresentados os aspectos e suas definições, inicia-se na sequência a análise dos relatos dos entrevistados, abordando primeiramente as políticas de segurança, implementadas a partir de recursos técnicos utilizados pela equipe de TI da organização.

4.3.1. Políticas de segurança (senhas seguras, antivírus, *backup* e controle de acesso à internet)

O aspecto de processos mais comentado pelos participantes diz respeito a políticas de segurança implementadas pela organização, a exemplo das regras de senha, de software antivírus instalado nos computadores e do controle de acesso a websites. Os relatos destacam inicialmente, no que diz respeito à política de senhas da organização, duas de suas características: a imposição de troca mensal da senha de acesso ao e-mail corporativo/internet e a utilização de senha comum para acesso aos computadores da empresa.

Acerca do primeiro, E5 afirmou no sentido de considerar a política importante à SI no ambiente:

> São importantes as senhas seguras, devido a isso [política de troca mensal], ser sempre alterada, mudada. (E5)

Ainda sobre a necessidade de troca de senhas para reforçar a segurança, E1 também traz a sua percepção:

> As senhas, no caso de senhas de computadores e dos sistemas da empresa, são sempre restritas aos responsáveis pelo setor, ela é restrita. Eu acredito que devia não permanecer muito tempo com essas senhas. Sempre renovando a senha, por que é uma alta segurança tanto para a empresa como pra pessoa. Sei que sou responsável, no meu caso, que sou responsável pelo setor, deveria estar sempre renovando essa senha, pois sempre no decorrer do tempo você termina cedendo a senha. (E1)

O participante vincula assim os dois aspectos: considera importante a troca constante de senhas e vê com preocupação a utilização de uma senha comum para acesso aos computadores e à maioria dos sistemas internos, a exemplo do utilizado no setor do usuário (setor de patrimônio). Referindo-se ao segundo, outros participantes demonstraram ter um misto de percepções:

> A senha é uma só. Aqui todo mundo, a gente não tem senha. É emdagro. (E6)

> Assim. Veja bem, porque cada um tem a sua senha, né? Embora seja uma só, pelo menos aqui. Aqui com a gente tudo é “emdagro”. AÍ Eu posso entrar no computador ali do meu colega, ele pode entrar no meu assim, entendeu? Qualquer um acessa. Por um lado, é bom por que é prático, né? Porque às vezes o colega tá viajando, eu tenho de acessar o computador dele. Preciso de uma informação dele. Olhando por esse lado é bom, já por outro... Se o camarada quiser fazer alguma coisa, ele faz... Ele abre, entra aqui no meu, deleta... Salvo se eu tivesse a dele, ele tivesse a própria, mas é geral. (E4)

Como mencionado anteriormente, apesar de cada empregado utilizar seu próprio usuário de rede, não há diferenciação das senhas dessas contas, que servem para acesso ao computador. Logo, se uma pessoa sabe o login do colega, sabendo que a senha é sempre a mesma, é possível que faça o login com sucesso. Uma vez autenticado, o usuário pode acessar pastas da rede interna e apagar dados locais do perfil do titular, o que tecnicamente dificulta a apuração de responsabilidades (STEWART ET AL., 2015).

Com efeito, utilização de senha comum é vista pela literatura como prática potencialmente insegura. Porém, trata-se de medida tomada pela gestão de TI para reduzir a dificuldade dos usuários sêniores em conciliar a diferenciação entre a senha de acesso ao computador da de acesso ao e-mail corporativo/internet, que sofre incidência de outra política imposta pela EMGETIS, conforme mencionado anteriormente. A partir disso, diversas solicitações de falta de acesso aos serviços eram registradas na EMDAGRO, pois os usuários sêniores apresentavam dificuldade de efetuar o procedimento.

Outro fator das políticas de segurança da organização que foi citado pelos participantes é a política de atualização do antivírus, mencionada por E3 e E4:

> E para isso também tem que ter uma coisa que seja sempre atualizado o antivírus, que nos lembra da importância de estar atentos. (E3)

> Por exemplo, dessa questão do antivírus que você viu agora mesmo apareceu [agente solicitando atualização]. Sim, eu não sei qual é a frequência que vocês disponibilizam lá, a atualização. Se fazem toda hora. Eu acho que essa questão do antivírus é importante sim. (E4)

A gestão de TI da organização implementou política de atualização do antivírus, que determina que o agente de segurança solicita confirmação ao usuário sempre que uma nova versão crítica está disponível. Dito isto, os participantes mencionaram a política como importante, relatando inclusive o alerta ao uso seguro que as solicitações de confirmação das atualizações do agente representam. É possível observar também que a comunicação da equipe de TI pode tornar a prática mais clara aos empregados, pois o próprio E4 mencionou não saber detalhes sobre o procedimento.

O fator da política de *backup* em vigor na organização também foi citado. A empresa disponibiliza uma área de armazenamento em rede que sofre *backup* diário, permitindo aos usuários que restaurem versões anteriores em caso de necessidade. Adicionalmente, a área de rede, armazenada em servidor, evita que falhas locais no computador utilizado pelo empregado afetem a integridade e disponibilidade dos dados. A importância de disponibilização de recurso semelhante foi mencionada por E4, que diz não saber que o serviço existe na organização:

> Tem a questão do *backup*, essas coisas. Mas não pela empresa, pela empresa não tem nada. Quero dizer... Pode ter, mas aqui não chega. (E4)

Além da menção clara do participante, outros usuários mencionaram durante as respostas a questões anteriores a prática de *backups* por meios próprios, utilizando dispositivos pessoais. Esses relatos surgem, inclusive, de participantes que perderam dados por não terem conhecimento da existência de áreas para cópias de segurança disponibilizadas pela organização:

> A única coisa que eu uso é o pen drive, para salvar os dados. Só. Eu já perdi muitos arquivos assim, porque eu não sei, assim, mas eu já perdi. A partir dessas perdas eu comecei a usar pen drive, assim, não tem muita segurança, nem pen drive nem HD externo, nada disso tem. Eu perdi dados importantes e alguns dados eu protejo nesse sentido, de botar pendrive, de ter uma cópia, tenho uns dois ou três pen drives q eu faço isso. (E2)

> Por exemplo, eu não tive o cuidado de passar antivírus nos arquivos. Eu sei que quando eu baixei as plantas que eu recebi de um trabalho lá de cima, um dia o computador deu uma pane que eu não conseguia acessar nada aqui. Tudo o que os programas que eu abri, topografia, AutoCAD, não conseguia ser sanado, não conseguia produzir nada, não conseguia salvar nada. O que é que me salvou? O

> *backup*, o *backup* que eu tinha que eu tinha nos HDs. Então, além da nuvem, eu tenho dois HDs onde eu guardo meus arquivos. (E3)

Outro fator citado em relação às políticas de segurança vigentes na organização é o controle do acesso a websites. A empresa exerce vigilância e proibição a tipos específicos de páginas da internet, a exemplo de redes sociais, sites de download de programas piratas, jogos eletrônicos, plataformas de *stream*, a exemplo do Netflix e HBO+. Websites marcados como potencialmente perigosos também são detectados pelo *firewall* instalado na organização, o que também reduz a exposição do ambiente organizacional a ameaças.

Nesse sentido, participantes mencionam o controle como importante à proteção contra perigos existentes na internet:

> Essas informações, no caso o site que pede que uma informação, eu acho necessário você se proteger, a empresa proteger, ter confiança se aquele site é verdadeiro. (E1)

> Tem sites aqui que você não consegue entrar de maneira nenhuma, porque a rede bloqueia. Não só a Emdagro, como a rede do Estado como um todo. Mas a partir do momento que chega na sua casa, que você sai da rede, do estado, você acessa o que você quiser, a máquina está com você. (E3)

Llorente-Barroso et al. (2018) e FBI (2023) afirmam que os usuários sêniores são especialmente vulneráveis a técnicas de utilizadas pelos *hackers* em páginas web, usualmente baseadas em engenharia social. Nesse sentido, Kamariza (2017) e Whitman e Mattord (2017) citam o controle do acesso a websites uma ferramenta importante à proteção do ambiente organizacional, sobretudo contra roubo de dados sensíveis.

4.3.2. Comunicação da TI com os usuários

Os participantes também expressaram considerar necessário que a organização incremente sua comunicação de informações sobre SI com os usuários. A análise desse fator, mencionado pelos participantes principalmente em respostas à Questão 07 do roteiro de entrevistas (percebido também ao longo de relatos em outras questões), é iniciada trazendo menções à deficiência da comunicação realizada pela empresa no tocante à disponibilização de serviços que poderiam auxiliar usuários a protegerem a informação:

> A única coisa que eu uso é o pen drive, para salvar os dados. Só. Eu já perdi muitos arquivos assim, porque eu não sei, assim, mas eu já perdi. (E2)

> Tem a questão do backup, essas coisas. Mas não pela empresa, pela empresa não tem nada. Quero dizer... pode ter, mas aqui não chega. (E4)

> Sim, eu não sei qual é a frequência que vocês disponibilizam lá, a atualização. Se fazem toda hora. Eu acho que essa questão do antivírus é importante sim. (E4)

Tais relatos retratam um possível ponto de atenção da organização à melhoria de sua comunicação com os usuários, sobretudo no que se refere à recursos de proteção à informação. Exemplifica-se a situação com a existência de área específica para *backup* e recomendações acerca do antivírus em funcionamento nos computadores da empresa, que foram citados como aspectos pouco conhecidos pelos sêniores entrevistados.

Adicionalmente, quando perguntados sobre como a empresa poderia incrementar a conscientização nos empregados, os participantes declararam que a comunicação por meio de avisos, lembretes e mensagens de e-mail podem auxiliar nesse processo, conforme menções citadas na sequência:

> Acho que essas coisas têm um efeito positivo, quando a empresa faz lembretes [pelo e-mail, no site do expresso, mensagens de texto – grifo nosso]. (E7)

> Influencia, influencia... Alerta, né? Alerta de vez em quando você está meio esquecido, mas esses e-mails alertam que aí você troca de senha, tem a questão do *backup*, essas coisas. "Banese informa" ... Não atenda isso. Não, faça não sei o quê, sabe? Tem esse lado. Assim, alerta... Alerta bastante. (E4)

> Pra mim tem, porque tá alertando, e é importante por que tem que ter... Gera um efeito, porque alerta, chama atenção, deixa as pessoas ligadas. (E5)

Observa-se, ao analisar os relatos dos participantes, que a comunicação realizada por meio dos recursos mencionados exerce influência positiva nos usuários, como lembretes de práticas de boas práticas de segurança ou alertas enviados por mensagens de e-mail, mensagens de texto ou avisos fixados na parede. Com efeito, Kamariza (2017) e Frik *et al*. (2019) consideram que políticas de comunicação da equipe de TI com os usuários exerce efeito positivo em seu comportamento, no que se refere à transmissão de conhecimento técnico e interesse em contribuir com a proteção da informação no ambiente.

> Eu nunca pensei em questões práticas de como estimular, mas poderiam começar pela própria TI, inicialmente sendo fundamental por parte deles a exposição por meio de mensagens dos riscos de um uso não conforme com as melhores práticas. (E3)

> Aqui não se fala de segurança. De como você se proteger melhor. Eu acho que precisa ainda fazer isso... Poderia ser por meio de mensagens de texto... (E2)

> É importante esse tipo de coisa e que esse é um alerta que a gente sempre tem... Você está sempre usando o computador...Pra você não ficar sem a informação [pelo mau uso – grifo nosso] ... Esses alertas ajudam você a ter a informação na hora que precisa. (E6)

Para Llorente-Barroso *et al*. (2018) e Masuch *et al*. (2021), cabe às organizações desenvolver alternativas às abordagens tecnicistas dominantes em programas de conscientização à SI, trazendo à discussão aspectos que abranjam crenças e limitações específicas dos empregados sêniores. Para autores como Cattell (1998) e Schelini (2006), programas de transferência de conhecimento e conscientização devem levar em consideração os tipos de inteligência e capacidades de retenção de conhecimento dos indivíduos, que se transformam com o avançar da idade.

Nesse sentido, E6 menciona sua percepção de que quando se trata de usuários de faixas etárias mais avançadas, medidas como as abordadas nesse subtópico são mais eficientes do que treinamentos formais para transferir conhecimentos e conscientizar:

> Só se for o lembrete na parede. Porque aqui... Pra fazer curso ninguém mais faz não. Um lembrete eu acho que é mais fácil, sabe porque as pessoas aqui do trabalho já estão numa idade que não comporta mais não. Você ensina uma coisa hoje e amanhã já não sabe. (E6)

Treinamentos também foram apontados pelos participantes como determinantes à disseminação de informações sobre boas práticas em SI. A percepção dos entrevistados sobre o tema será discutida na sequência.

4.3.3. Treinamento

Apontado pela literatura como fundamental qualquer política de segurança da informação, o treinamento foi mencionado por alguns entrevistados como ferramenta à conscientização em SI da força de trabalho não explorado pela organização (GREEN; DOREY, 2016; HAEUSSINGER, 2017; MASUCH ET AL., 2021). E2 e E7 expõem sua percepção nesse sentido ao responder às Questões 07 e 08 do roteiro de entrevistas:

> Eu acho que a gente precisa ainda ter alguns cursos sobre essa questão, sabe? Porque eu lembro que eu fiz um apenas um curso aqui, que foi quando eu tinha aqui um projeto de informática. E de lá para cá que não, não fez mais. Eu acho que a empresa precisa estar nivelando, vamos dizer, atualizando os servidores em alguns aspectos da tecnologia importantes. (E2)

> Atualizar [o conhecimento dos empregados – grifo nosso] ... Tem sempre que tá atualizando... É importante. É importante ter palestras sobre esses riscos... Em geral, tem que ter uma palestra pra todo mundo. Em grupo era bom, viu? (E7)

Após demonstrarem ter dificuldades na utilização de tecnologias digitais, as participantes consideram importante por parte da organização a atualização dos empregados em segurança da informação ou em aspectos da tecnologia importantes, conforme mencionado por E2. E3 corrobora tal preocupação, também considerando que a empresa deve treinar os empregados e relata que a administração estatal até disponibiliza treinamentos, mas que os colegas não demonstram interesse suficiente nesses programas:

> Quando necessário, buscam acessar o de outras pessoas [e-mail corporativo – grifo nosso], ou não buscam conhecimento sobre como utilizar. Talvez haja necessidade de uma política por parte da empresa para conscientizar os usuários sobre como utilizar os recursos tecnológicos. (E3)

> O próprio E-DOC [sistema de protocolo eletrônico utilizado pela administração estadual – grifo nosso], não é nem utilizado. A empresa disponibilizou treinamento e quantas pessoas aqui utilizam e sabem utilizar? A empresa também é culpada por não cobrar e estimular a força de trabalho na utilização desses recursos. (E3)

O treinamento formal em E-DOC é fornecido pela Escola do Estado, organizado pela Secretaria de Administração (SEAD). Em se tratando de um sistema implementado na esfera estadual, mas não mandatório na organização, o protocolo eletrônico se apresenta como recurso importante na agilidade, economia e segurança dos processos das empresas da administração direta e indireta do Estado de Sergipe, mas encontra baixa adesão pelos setores da EMDAGRO. Observa-se, durante as atividades, que há resistência da força de trabalho sênior ra empresa à implementação do sistema, justamente pela baixa sensação de autoeficácia desses empregados em sua operação.

Com efeito, treinamentos no E-DOC foram disponibilizados em turmas bimestrais desde sua implementação desde 2010, mas apenas a presidência da organização faz utilização regular do recurso. Há previsão da nova diretoria da empresa que o sistema entre em vigor ainda esse ano (2023), com adesão total de todos os setores da organização. Nesse sentido, conforme mencionado no fator anterior, E6 corrobora o que se observa na organização, pois acredita que treinamentos poderiam não ser eficientes, e os motivos consistem na dificuldade dos sêniores em assimilar conhecimentos em virtude de fatores relacionado à idade:

> Só se for o lembrete na parede. Porque aqui... Pra fazer curso ninguém mais faz não. Um lembrete eu acho que é mais fácil, sabe porque as pessoas aqui do trabalho já

> estão numa idade que não comporta mais não. Você ensina uma coisa hoje e amanhã já não sabe. (E6)

A percepção mencionada pela entrevistada encontra amparo na literatura. Conforme Thompson e Mayhorn (2012) e Kraiger (2017), sêniores apresentam maior resistência à obtenção e retenção de novos conhecimentos, especialmente no que se refere a novas tecnologias. Além disso, os autores descrevem características particulares a esse grupo de pessoas que dificultam a aprendizagem, a exemplo de aspectos cognitivos, como reduzido nível de atenção e capacidade de memorização.

Também são citados aspectos motivacionais, que segundo Kanfer e Ackerman (2004), são afetados pela redução da quantidade de inteligência fluida dos sêniores. Os autores citam esse tipo de inteligência como importante à análise de novos problemas, detecção de padrões e assim por diante, atividades comuns em muitos programas de treinamento. Assim, os trabalhadores mais velhos podem perceber o treinamento como novo e exigente e, portanto, ter menor motivação para participar (KANFER; ACKERMAN, 2004).

4.3.4. Outros fatores de aspectos de processos

Os seguintes fatores de aspectos de processos foram mencionados pelos participantes: envolvimento dos gestores, investimento em tecnologia e segurança e atribuição de responsabilidades pelo mau uso de dispositivos digitais. A exposição e análise dessas menções serão iniciados pelo fator envolvimento dos gestores, citado por 03 participantes que se referiram à participação da gestão na conscientização dos empregados:

> Sei que é responsável, no meu caso, que sou responsável pelo setor, deveria estar sempre renovando essa senha. Por isso, por ser chefia do setor, deve-se dar exemplo. (E1)

> E de lá para cá que não, não fez mais. Eu acho que a empresa precisa estar nivelando, vamos dizer, atualizando os servidores em alguns aspectos da tecnologia importantes. Aqui não se fala de segurança. De como você se proteger melhor. Eu acho que precisa ainda fazer isso. (E2)

> A empresa também é culpada por não cobrar e estimular a força de trabalho na utilização segura desses recursos. (E3)

O relato de E1 refere-se à sua experiência como gestor do setor de patrimônio (atual, na qual acessa com senha um sistema de gestão patrimonial) e serviços gerais (anterior, onde acessa programas como editores de texto, planilhas e navegadores de internet). E2, por sua vez, pensa que os gestores da empresa devem trazer o assunto da SI para o ambiente da organização, sobretudo sobre como os usuários podem se proteger. Por último, E3 acredita que os gestores da empresa têm responsabilidade por um possível mau uso da informação por parte dos empregados, pois pensa que a chefia deve estimular seus usuários a utilizar de forma segura os dispositivos digitais.

Dito isto, percebe-se pela fala dos participantes que eles não acreditam que supervisores e diretores da organização estimulem a conscientização em SI nos empregados. Essa percepção é corroborada pelo autor da pesquisa em suas observações, registradas no Script de Observação 04. Nesse registro, é possível verificar que alguns gestores da empresa que são sêniores fazem declarações para seus subordinados no sentido de que tecnologias digitais “complicam” ou que “não têm mais idade pra isso [aprender a operar sistemas – grifo nosso]”, o que pode desestimular empregados a observarem o assunto da mesma maneira.

Nesse ínterim, Lim *et al*. (2010) consideram que o comprometimento e exemplo dos gestores da empresa na proteção à informação é vital à promoção de usuários atentos e conscientes em segurança da informação. Green e Dorey (2016) corroboram, afirmando que a diretoria e os supervisores devem demonstrar apoio à conscientização por participar ativamente em atividades de segurança.

A ausência de uma política de atribuição de responsabilidades também foi mencionada pelos participantes. Como já abordado anteriormente, a responsabilização em caso de mau uso é uma das metas da segurança da informação, conforme Haeussinger (2017) e Masuch *et al*. (2021). Nesse sentido, os relatos de E1, E3 e E7 descrevem suas percepções acerca do tema:

> Eu sou responsável hoje pelo setor de patrimônio. Eu tenho a minha responsabilidade por todos os dados que são manipulados. Por isso que é necessário ter esse cuidado. Se não tivéssemos essa responsabilização, vai virar um caos. Pode prejudicar a empresa também. (E1)

E1 acredita que a responsabilização é necessária, pois o uso não cuidadoso pode causar problemas à organização como um todo, mesmo não especificando que tipos de danos podem advir de tal situação. E3 traz, mais uma vez, a preocupação com a questão da auditabilidade em uma possível má utilização do e-mail corporativo:

> Eu sou meio radical em relação a algumas coisas. Primeiro o seguinte: eu acho que essa política de conscientização, né, mas não é só conscientização... Não é só sobre em relação ao uso, mas também à responsabilização do não uso. O que é o mau uso? Por exemplo, outra pessoa solicita que eu abra o meu expresso para mandar uma informação através da minha conta de e-mail. Para que a gente carregue em cima dessa pessoa um peso maior em relação à responsabilidade de ele ter aberto esse e-mail para que outra pessoa mande a informação. Que eles tenham consciência de que serão cobrados caso aquela informação seja mal utilizada. O reflexo que vai ter lá na frente, não importa se a conta era de Fred e Filipe mandou o e-mail e assinou, a responsabilidade é de Frederico que abriu o e-mail para que Filipe mandasse. (E3)

Uma vez que o entrevistado observa que há pratica de compartilhamento de senhas de acesso à internet e e-mail corporativo, E3 relata preocupação com possíveis consequências do mau uso desses recursos. Nesses casos, o entrevistado acredita que o usuário deve ser responsabilizado pela organização, por meio de política ativa nesse sentido. O relato é semelhante ao feito por E7:

> Os empregados devem ser responsabilizados, até porque tem muitos terceirizados aqui que não têm noção ainda dos riscos que possam passar, né? (E7)

A entrevistada menciona que, além de considerar necessária responsabilização dos usuários em caso de mau uso de dispositivos digitais, que há diferenciação no comprometimento em SI entre empregados próprios da organização e os terceirizados. Tal cenário apontado pela participante encontra amparo na literatura especializada, pois autores como Herath e Rao (2009) e Prislan *et al*. (2020) afirmam que há fatores que podem afetar o comprometimento dos empregados a políticas de proteção à informação. Comportamentos de segurança podem ser influenciados por ambos motivadores intrínsecos e extrínsecos, e o vínculo legal dos empregados é citado como um dos fatores extrínsecos trazidos pelos autores (HERATH; RAO, 2009; PRISLAN ET AL., 2020).

O último aspecto mencionado pelos participantes é a percepção de que há necessidade de maior investimento em segurança por parte da organização. Acerca do tema, E3 menciona:

> Por exemplo, quando eu me referi à Emdagro, eu sei que a gente tem um trabalho, tem uma rede segura, mas o Estado não investe nisso e a EMGETIS está sucateada.

> Essa é a verdade. E não é de agora, não é desse governo. Já vem de quantos anos isso? Então não investe. Então você chega, por exemplo, numa empresa privada que de tecnologia de informação, eles estão num patamar muito acima. O esforço da empresa é inegável, só que eles não têm as ferramentas necessárias para que eles tenham uma condição melhor de proteger os dados do Estado. (E3)

E3 afirma reconhecer o interesse da organização e da EMGETIS em proteger o ambiente de rede da empresa, e considera que maiores investimentos em tecnologia são oportunos. Ao mencionar que a administração estadual não possui as ferramentas necessárias para proteger os dados utilizados na empresa, apesar do esforço que enxerga por parte da organização em fazer isso. No caso de E4, seu relato refere-se ao direcionamento dos investimentos feitos pela empresa:

> Uma reunião aí no auditório, né? Lembretes, tipo uma mensagem, né? Reuniões... cursos mesmo, se fosse o caso. Eu acho que o *backup*. Eu não sei se o *backup* pode ser coletivo, não sei bem como é esse sistema. Vai ser um *backup* coletivo, *backup* individual, ou seja, às vezes a gente gasta dinheiro com tanta coisa. (E4)

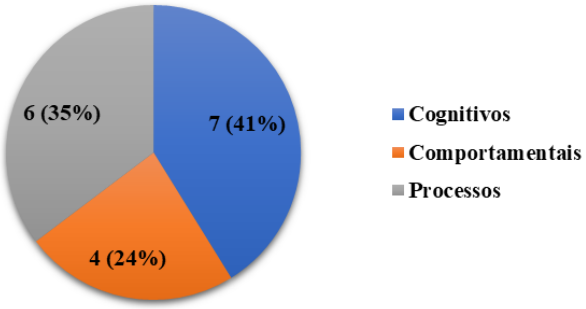
O usuário acredita que apesar da organização investir recursos em outras áreas, poderia fazer investimentos tecnologia e segurança, a exemplo de treinamento aos empregados e tecnologia de *backup*. Investimento em segurança é prática recomendada pela literatura, inclusive quando se refere a treinar a força de trabalho em SI e em recursos de proteção à informação, como os *backups* (RAO; NAYAK, 2014; STEWART ET AL., 2015).

Finalizada a exposição dos aspectos da CSI mencionados pelos participantes nas entrevistas, parte-se à discussão acerca do agrupamento dos entrevistados em relação a seus níveis de conscientização em SI observados, bem como dos modelos mentais relacionados aos aspectos da CSI de cada grupo.

4.4. Agrupamento dos participantes em relação ao nível de CSI e seus respectivos mapas mentais

Como já mencionado, buscou-se identificar a percepção dos usuários sêniores em relação aos aspectos da conscientização em segurança da informação. Com efeito, foram mencionados pelos participantes 17 fatores relacionados à proteção à informação no ambiente organizacional, distribuídos nos 03 aspectos componentes da conscientização em segurança da informação: cognitivos, comportamentais e de processos. A distribuição dos fatores em cada aspecto pode ser visualizada na Figura 28.

Figura 28 - Distribuição de aspectos mencionados nos componentes da CSI.



Fonte: Dados da pesquisa (2023).

Os participantes foram divididos em dois grupos, de acordo com a sua aproximação às boas práticas em SI. O critério de agrupamento foi frequência de possessão de aspectos

cognitivos e de comportamento, além da atenção a processos conduzidos pela organização relacionados a boas práticas em SI (HAEUSSINGER, 2017). Participantes que apresentam aproximação a boas práticas em 50% ou mais dos aspectos citados foram classificados no Grupo 01, e os demais foram listados no Grupo 02.

Dito isto, os agrupamentos dos participantes foram feitos conforme pode ser observado no Quadro 14, apresentado na sequência.

Quadro 14 – Contagem e frequência de menções a percepções tecnicamente adequadas/comportamentos seguros à organização entre os 17 aspectos citados.

Sêniores com maior grau de CSI (Grupo 01)	**Sêniores com menor grau de CSI (Grupo 02)**
E1 - 11 (65%)	**E2** - 7 (41%)
E3 - 15 (89%)	**E5** - 7 (41%)
E4 - 12 (71%)	**E6** - 7 (41%)
	E7 - 6 (35%)

Fonte: Dados da pesquisa (2023).

Serão expostos em seguida os mapas mentais desenvolvidos a partir da análise das citações feitas pelos grupos, organizados de acordo com os 17 fatores mencionados nas entrevistas. Uma vez que a presente pesquisa buscou lançar luz à percepção de como os sêniores da organização enxergam os três aspectos da conscientização em segurança da informação, foram delineados dois mapas por aspecto: um referente ao Grupo 01, e outro que diz respeito ao Grupo 02. Pretende-se auxiliar na visualização da percepção dos entrevistados, destacando possíveis distinções entre os grupos, lançando luz a fatores de afastamento dos sêniores da organização estudada a uma atitude mais segura.

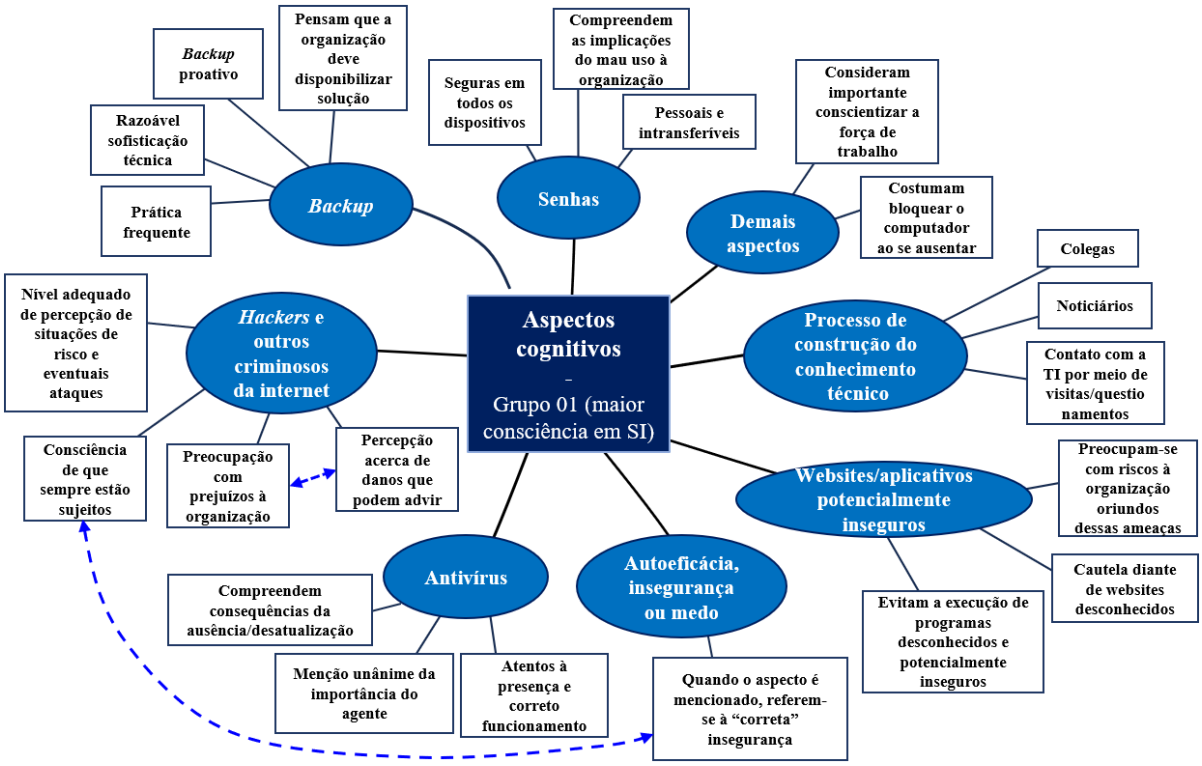
Parte-se, então, à apresentação dos modelos mentais referentes aos aspectos cognitivos dos participantes.

4.4.1. Mapa mental relacionado a aspectos cognitivos

No tocante aos aspectos cognitivos citados pelos participantes em suas entrevistas, observou-se que há significativa diferença entre os grupos definidos. Os entrevistados do Grupo 01 apresentaram respostas às questões com maior segurança e espontaneidade, trazendo informações técnicas referentes aos aspectos citados. Embora alguns detalhes importantes da proteção à informação não tenham sido lembrados de maneira unânime pelo grupo, a exemplo da atenção à correta manutenção do antivírus e a execução de *backup* proativo, a percepção do grupo acerca dos riscos e ameaças a que estão sujeitos e das maneiras de mitigá-los é tecnicamente adequada.

O Script de Observação 01 reforça o cenário verificado nas declarações do grupo, pois retrata situações nas quais os participantes exercem um comportamento mais consciente acerca da mitigação a riscos à proteção à informação. Dito isto, a Figura 29 apresenta o mapa mental do Grupo 01.

Figura 29 – Mapa mental de aspectos cognitivos do Grupo 01.



Fonte: Elaborado pelo autor (2023).

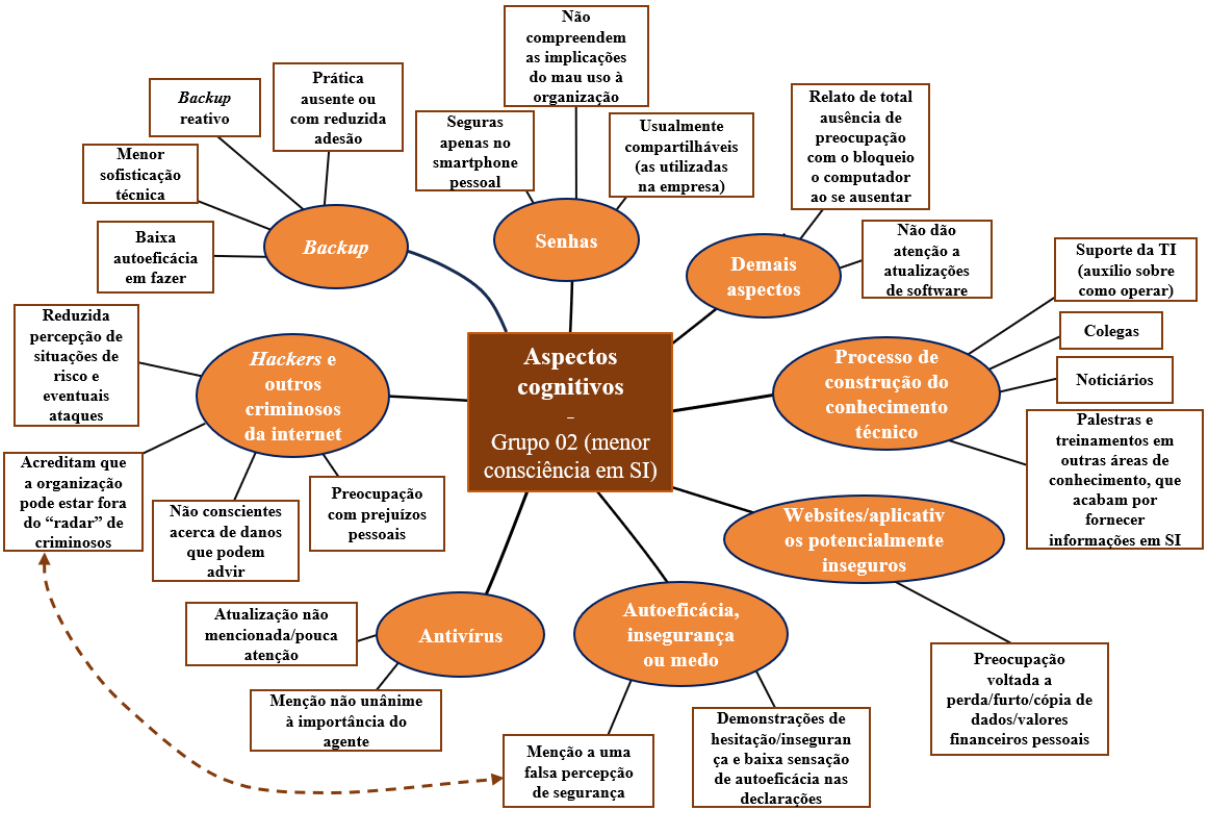
Observa-se que os participantes do Grupo 01 declaram, quase que em todos os aspectos citados, ter consciência e preocupação com o fato de que ameaças podem prejudicar também a organização, não trazendo só prejuízos pessoais. Essa atenção a possíveis prejuízos à empresa é representada em aspectos cognitivos anteriormente citados.

Também vale ressaltar que o aspecto Autoeficácia, insegurança ou medo é mencionado pelos participantes do grupo, mas referindo-se apenas ao que a literatura apresenta como uma preocupação tecnicamente adequada. Isso ocorre no sentido de o usuário compreender que está sempre exposto a riscos à integridade, confiabilidade e confidencialidade de dados e informações pessoais e da organização (HADNAGY, 2018).

Tal sensação de insegurança relaciona-se diretamente à capacidade do usuário de perceber situações de risco, quando se observa a ligação no mapa mental entre os dois aspectos citados, apresentando assim noções acerca de técnicas e caminhos utilizados pelos criminosos para terem acesso a dados e ambientes restritos. Percebe-se também que esses participantes são capazes de enxergar e sugerir soluções técnicas à organização, sobretudo no que diz respeito ao aspecto *backup*. O participante E3, por exemplo, citou o recurso das cópias de segurança em nuvem, e E4 considera que a empresa pode disponibilizar área de armazenamento de arquivos em rede com serviço de *backup*.

Adicionalmente, observa-se que o Grupo 01 mantém contato constante com a equipe de TI da organização, seja por prévias experiências profissionais no setor, como pela frequente presença no local que os técnicos exercem suas funções. Mesmo declarando não terem sido formalmente treinados em programas com este fim, atribuem a esse contato a sua percepção técnica acerca da segurança da informação. Em contrapartida, as respostas e observações referentes ao Grupo 02 tendem a uma preocupação mais voltada a ameaças a dados pessoais, e não a riscos à segurança do ambiente e de informações da organização. Dito isto, a Figura 30 apresenta o mapa mental referente aos aspectos cognitivos mencionados pelas participantes E2, E5, E6 e E7.

Figura 30 - Mapa mental de aspectos cognitivos do Grupo 02.



Fonte: Elaborado pelo autor (2023).

Os entrevistados do Grupo 02 demonstram menor sensação de autoeficácia em diversos aspectos citados, a exemplo de *backups*, da ação de *hackers* e outros criminosos da internet e atualizações de software. Porém, alguns participantes do grupo citaram, ao contrário do mencionado pelo Grupo 01, uma falsa sensação de proteção e invulnerabilidade a ataques de criminosos digitais por considerarem que estão fora do raio de ação dessas pessoas ou grupos, o que não encontra amparo na literatura especializada. Autores como Green e Dorey (2016) e Whitman e Mattord (2017) associam a baixa autoeficácia, ou uma indevida sensação de segurança à baixa capacitação técnica.

Como já mencionado, apesar de afirmarem tomar cuidados com seus dispositivos no âmbito particular, os dados da pesquisa trazem à tona de que são poucos momentos nos quais os participantes do Grupo 02 demonstram preocupações com possíveis prejuízos à organização. Esse cenário se faz perceptível em aspectos importantes à proteção à informação, como quando estão diante de possíveis invasões a sistemas e dispositivos, da navegação a websites ou em seu gerenciamento de senhas, marcado pelo compartilhamento com colegas e armazenamento físico em papéis.

A atenção e preocupação dos empregados com a segurança da informação no ambiente organizacional é visto como premissa básica da conscientização em SI (HAEUSSINGER, 2017; MASUCH ET AL., 2021). Conhecimentos técnicos limitados, sobretudo acerca dos riscos e possíveis prejuízos causados for incidentes de segurança, são vistos pela literatura como contribuidores à baixa conscientização de uma força de trabalho (LLORENTE-BARROSO ET AL., 2018).

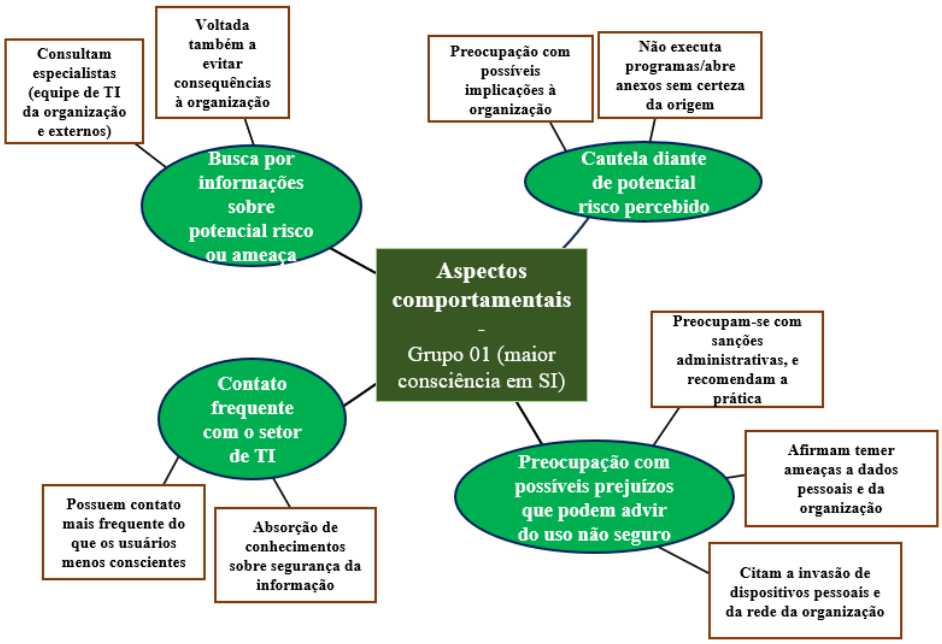
Por fim, os entrevistados que compõem o Grupo 02 afirmaram que seu conhecimento sobre SI é construído sobretudo por conversas com colegas e noticiários, e que consultas aos especialistas em TI da organização são voltadas ao auxílio na realização de tarefas, a exemplo do percebido no Script de Observação 02. É também citado por uma participante (E5)

informações que são obtidas em treinamentos que dizem respeito a outras áreas de conhecimento, que por vezes trazem conhecimentos acerca de SI, como cursos de contabilidade e finanças.

4.4.2. Mapa mental relacionado a aspectos comportamentais.

Os aspectos comportamentais mencionados pelo Grupo 01 tendem a expor um maior comprometimento e atuação prática no sentido de contribuir aos objetivos da segurança da informação na organização. A Figura 31 expõe o modelo mental genérico desenvolvido a partir dos relatos de seus participantes.

Figura 31 – Mapa mental de aspectos cognitivos do Grupo 01.



Fonte: Elaborado pelo autor (2023).

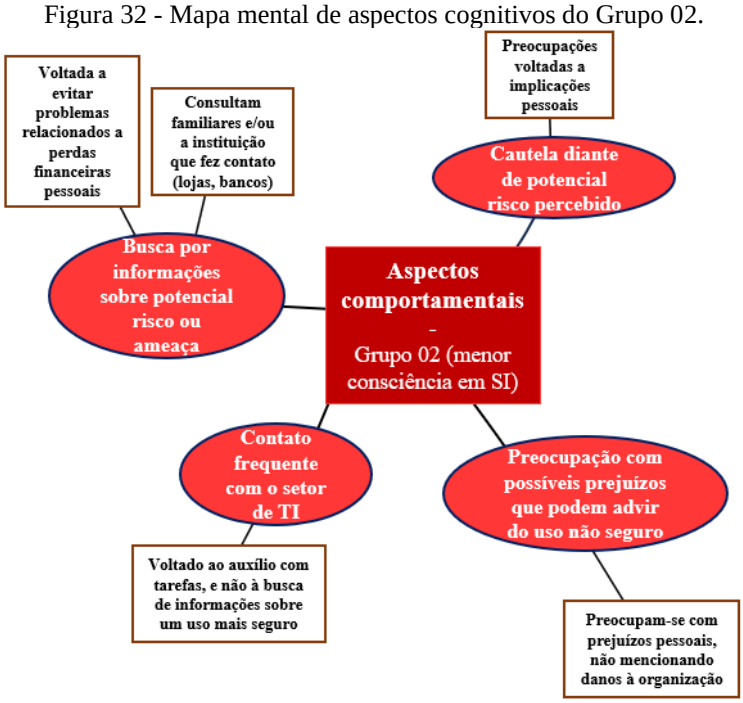
Assim como nos aspectos cognitivos, os participantes mencionam estarem atentos a possíveis prejuízos à empresa. Declararam que, em face de situações de risco percebido tendem a utilizar de cautela e buscar informações sobre potenciais ameaças, levando em consideração que um possível incidente causaria danos à integridade, disponibilidade e confiabilidade dos dados e informações da organização, além do correto funcionamento de seus sistemas. Baseiam sua preocupação e cuidado no uso dos dispositivos em informações técnicas usualmente corretas, a exemplo de consequências de uma possível invasão ao ambiente de rede da empresa e da inserção de dados e informações em websites fraudulentos.

Os participantes também consideram que a responsabilização pelo mau uso, mediante sanções administrativas, contribui para que utilizem de maneira mais segura e responsável os dispositivos no ambiente da organização. Embora sanções administrativas sejam vistas como processos da organização que buscam desenvolver conscientização em empregados, os participantes afirmam que possíveis punições afetam seu comportamento, mesmo que não formalmente implementadas na organização estudada.

Adicionalmente, é mencionada a prática de contato constante com os especialistas em TI da empresa, o que os permite adquirir conhecimentos sobre segurança da informação, seja diante de situações de possível risco quanto para solicitar o ajuste de agentes de segurança, como observado no Script de Observação 01.

No que se refere aos sêniores com menor grau de consciência em SI, mais uma vez as percepções acerca dos aspectos são direcionadas a prejuízos de ordem pessoal, não comprometidos com os objetivos da segurança da informação da organização. Esse cenário pode ser observado na Figura 32, apresentada na sequência.

Figura 32 - Mapa mental de aspectos cognitivos do Grupo 02.



Fonte: Elaborado pelo autor (2023).

Observa-se que os entrevistados do Grupo 02, apesar de demonstrarem preocupação com as ameaças que estejam sujeitos, seu comportamento de evitar prejuízos é voltado a perdas financeiras e ao acesso indevido a fotos e senhas em dispositivos pessoais. Apesar da segurança da informação envolver a proteção a dados e dispositivos particulares, a consciência e atenção dos empregados a possíveis prejuízos à organização é necessária para que o ambiente se mantenha seguro, uma vez que os usuários são apontados como o elo frágil na cadeia de proteção à informação (GREEN; DOREY, 2016; HADNAGY, 2018).

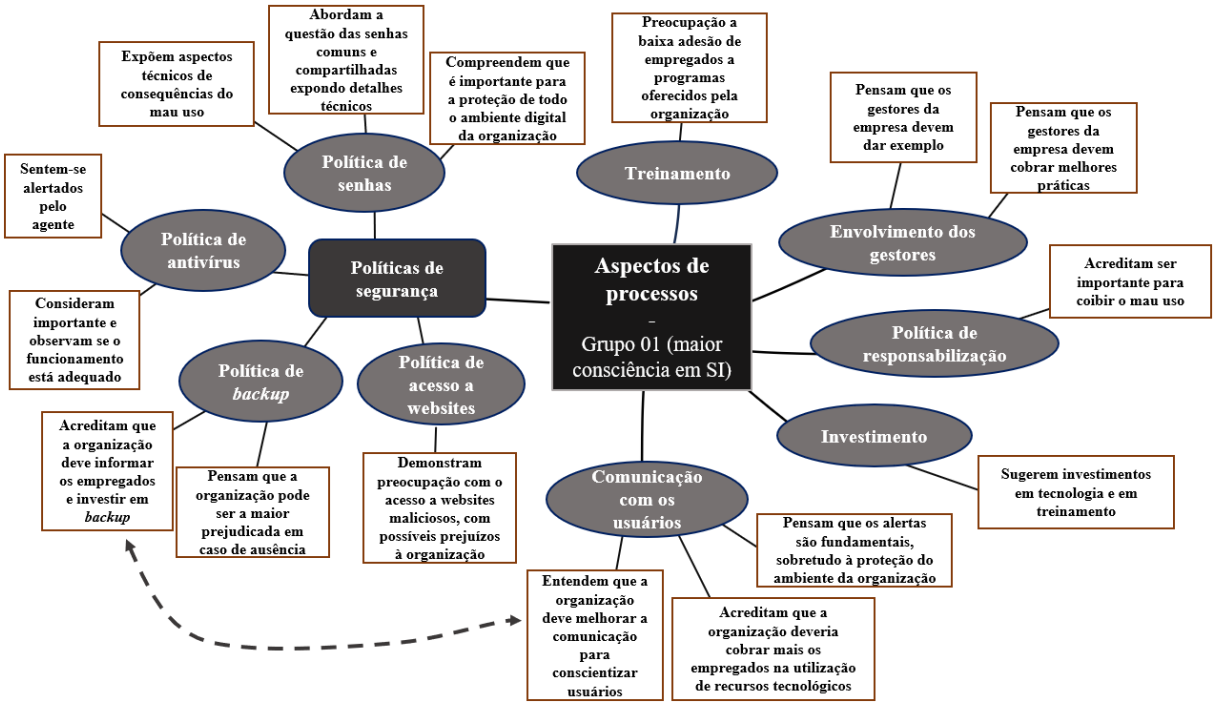
Outra característica percebida no Grupo 02 é que o contato com a equipe de especialistas em TI da organização é frequente apenas para o auxílio sobre como operar os dispositivos, a exemplo do que foi observado no Script de Observação 02. Esse hábito também pode ser verificado no aspecto da busca por informações numa situação de potencial risco, na qual costumam consultar a própria empresa/instituição que, em teoria, está entrando em contato ou hospedando uma oferta em websites, por exemplo. Algumas situações que ocorreram com esses participantes foram mencionadas ao longo do estudo, como e-mails de varejistas conhecidos ou bancos.

Todavia, apesar de ser recomendado tecnicamente buscar instituições oficiais para sanar dúvidas relacionadas a possíveis fraudes, a consulta à equipe de TI é recomendada, pois evita a consulta a fontes não fidedignas, a exemplo de falsos serviços de call center e websites (FBI, 2023). No tocante ao intercâmbio proporcionado pelo contato com os especialistas da empresa, Kamariza (2017) menciona que o contato constante favorece não só a transmissão de conhecimentos técnicos de qualidade, mas também informações acerca de políticas e práticas recomendadas no âmbito da empresa. Cenários apontados durante a pesquisa, a exemplo do desconhecimento de alguns participantes de áreas de *backup* disponibilizadas pela TI, podem auxiliar na demonstração dessa situação.

4.4.3. Mapa mental relacionado a aspectos de processos.

Em se tratando de aspectos de processos, os participantes de Grupo 01 apresentam compreensões tecnicamente adequadas a diversos processos a serem conduzidos pela organização, a exemplo de políticas de segurança, envolvimento de gestores e treinamento. Esse cenário pode ser observado na Figura 33.

Figura 33 - Mapa mental de aspectos de processos do Grupo 01.



Fonte: Elaborado pelo autor (2023).

Os participantes E1, E3 e E4 comentaram aspectos relevantes das políticas de segurança que são levadas a cabo pela EMDAGRO. Foram observadas as políticas de senhas, antivírus, *backup* e acesso a websites, sobre as quais houve, novamente, menção à preocupação com a integridade da organização.

No que diz respeito à política de senhas, são citados detalhes técnicos de consequências por possíveis maus usos de credenciais. Foram mencionados prejuízos severos à organização, como a invasão por usuários mal intencionados do ambiente de rede da empresa e da destruição e cópia de dados e informações sigilosos. O mesmo ocorre quando o tema é *backup*, pois creem que a empresa seria a maior prejudicada caso dados e informações importantes sejam perdidas, em detrimento a preocupações com perdas pessoais.

Nesse ínterim, os participantes do Grupo 01 traçam um paralelo entre o aspecto da, por eles percebida, ausência de investimentos em tecnologias de *backup* com uma deficiente comunicação da gestão com os empregados, pois desconhecem que o recurso é disponibilizado pela equipe de TI. Com efeito, consideram que uma comunicação mais eficiente dos técnicos e gestores de tecnologia com os demais empregados pode contribuir a uma maior conscientização desses últimos, o que encontra aderência na literatura especializada (RAO; NAYAK, 2014).

Além disso, o Grupo 01 afirma crer que uma política de cobrança à adesão a sistemas digitais é importante, pois consideram que a maioria da força de trabalho sênior da empresa não adere à utilização de sistemas eletrônicos, a exemplo do protocolo eletrônico (E-DOC). Compreendem, assim, os benefícios oriundos da digitalização de processos, mesmo fazendo

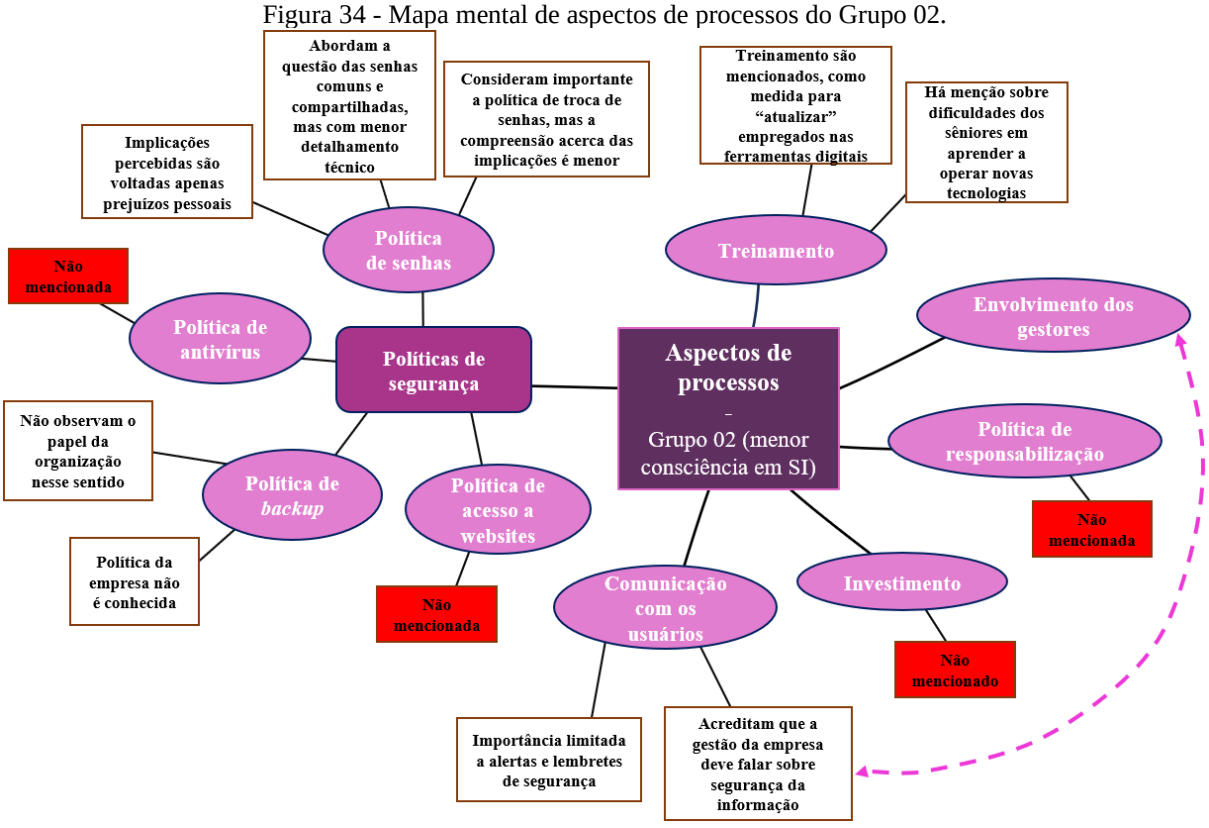
parte de um recorte social mais resistente à adoção de tecnologias digitais, pensamento que vai em sentido contrário ao cenário observado por Adamczyk e Betlej (2020). Consideram também que a responsabilização em caso de mau uso é importante e que a EMDAGRO carece desse tipo de diretriz, bem como de investimentos financeiros na aquisição de recursos tecnológicos, como equipamentos, software e qualificação e treinamento para a força de trabalho.

Por fim, é citado o aspecto do envolvimento da gestão, apontado por autores como fundamental à conscientização de empregados (STEWART *ET AL*., 2015; STELZER *ET AL*., 2019). Nesse contexto, o Script de Observação de número 04 faz menção a uma realidade pouco presente, pois diversos coordenadores e até diretores da empresa não exercem um comportamento de estímulo às melhores práticas em SI. Esses gestores por vezes expressam uma visão de afastamento deliberado à tecnologia orientado por uma baixa sensação de autoeficácia, descrevendo os avanços tecnológicos na área digital como sendo potenciais complicadores à realização de atividades.

Em contrapartida, os integrantes do Grupo 01 declaram ter uma percepção diferente, pois enxergam vantagens na adoção de recursos tecnológicos e até sugerem possíveis pontos de melhoria em processos que possam contribuir ao aumento da produtividade e da CSI na força de trabalho.

No que diz respeito ao Grupo 02, a consciência acerca das políticas e processos da organização com vias ao desenvolvimento de CSI nos empregados reduzida, quando comparada à do Grupo 01. Esse cenário pode ser observado na Figura 34, exposta na sequência.

Figura 34 - Mapa mental de aspectos de processos do Grupo 02.



Fonte: Elaborado pelo autor (2023).

Todavia, cabe trazer à discussão que os participantes dos grupos dos menos conscientes, apesar de demonstrarem possuir menor conhecimento técnico acerca da existência ou das implicações de não se seguir políticas estabelecidas, consideram importantes as diretrizes definidas no que se refere a senhas. Abordam, inclusive a questão da utilização de uma senha

comuns em diversos computadores da empresa, mas não foi mencionado detalhamento técnico como foi feito pelos integrantes do Grupo 01.

Em relação às políticas de *backup*, antivírus e controle acesso a websites, não foram mencionadas ou são desconhecidas pelo Grupo 02. Adicionalmente, a prática da comunicação com os usuários por parte da organização foi citada, e foi considerado insuficiente o envolvimento dos gestores na conscientização. Essa percepção corrobora com o mencionado pelo Grupo 01, que também pensa que a gestão da empresa deve ser mais ativa no incentivo e no exemplo de boas práticas em SI. Os participantes consideram também que lembretes de segurança por mensagens de texto ou e-mail podem ser úteis para alertar os empregados a riscos de SI.

Traz-se à discussão também a percepção desses participantes ao aspecto do treinamento, por eles considerado importante para "atualizar" os empregados sêniores às novas tecnologias e em boas práticas de SI. Ao mesmo tempo, E6 afirma considerar que esse tipo de prática não funcionaria na organização, pois em virtude da idade avançada de muitos dos empregados a retenção de novos conhecimentos é dificultada. A entrevistada justifica sua afirmação por citar fatores como o decaimento dos níveis de atenção, capacidade de memorização e do próprio interesse dos empregados sêniores em treinamentos. O relato da entrevistada corrobora o cenário de desinteresse causado pela sensação de baixa autoeficácia observada em sêniores da organização, inclusive diretores e coordenadores, que por vezes expressam desinteresse em tecnologias digitais. Tal aspecto foi registrado pelo pesquisador no Script de Observação 04 durante suas atividades diárias na empresa, e citado na discussão do tópico voltado à baixa autoeficácia, insegurança ou medo (tópico 4.1.1.5).

A percepção de E6 vai de encontro ao que é mencionado pelo Grupo 01, que observa uma baixa adesão de treinamentos que são oferecidos pela organização. Esse cenário encontra aderência na literatura por autores como Li e Luximon (2016) Llorente-Barroso *et al*. (2018), que afirmam que o interesse do usuário sênior em adquirir conhecimentos acerca da tecnologia digital é reduzido em relação a faixas etárias mais jovens, o que dificulta a adaptação dessas pessoas a um uso mais autoeficaz e confiante de dispositivos digitais.

Finalizando à análise dos aspectos de processos sob a percepção das entrevistadas do Grupo 02, ressalta-se a ausência de menção a diversos aspectos observados pelo Grupo 01: políticas de antivírus e controle de acesso a websites, investimentos e responsabilização em caso de mau uso.

Parte-se, em seguida, à exposição das considerações finais da pesquisa.

5. CONSIDERAÇÕES FINAIS

O presente estudo é norteado pelo seguinte problema: como a percepção dos usuários sêniores da organização acerca dos aspectos da CSI os afasta das melhores práticas em segurança da informação? A resposta a esse questionamento, constituído no objetivo principal da pesquisa, iniciou-se pela investigação acerca dos aspectos componentes da conscientização em segurança da informação.

Com isso, o atendimento ao objetivo foi permeado pelo entendimento de que o recorte social dos sêniores, inseridos no ambiente organizacional estudado, apresentou dois grupos de percepções distintas: o primeiro, constituído por 03 dos 07 participantes (Grupo 01), mostrou-se mais consciente quanto a riscos e ameaças que permeiam o uso de dispositivos digitais, além de possuir mais conhecimentos técnicos necessários para evita-los. Esses participantes também exercem um comportamento comprometido com os objetivos de segurança da organização, e são mais atentos a processos conduzidos pela empresa para incrementar a conscientização nos empregados. Em outras palavras, maior consciência em segurança da informação, sendo mais atentos e comprometidos com os objetivos da SI na organização.

Observou-se, também, um grupo composto por 04 sêniores (Grupo 02), que apresentou menor consciência em relação aos aspectos da CSI. Isso significa que sua percepção acerca de aspectos cognitivos, comportamentais e de processos são reduzidos em relação aos participantes do Grupo 01. Esse cenário sinaliza que mais da metade dos entrevistados apresentam conhecimentos, comportamentos e percepções acerca de processos conduzidos pela empresa não atentos e alinhados às boas práticas de proteção à informação, com menor comprometimento com os objetivos da organização em relação aos componentes do Grupo 01.

No ínterim da busca ao atendimento do primeiro objetivo específico da pesquisa, a discussão acerca dos aspectos cognitivos dos entrevistados mostrou características que apontam os participantes do Grupo 01 como mais conscientes do que os demais. A primeira característica observada é o contato mais frequente dessas pessoas com especialistas em tecnologia da organização. Seja por experiência no setor de informática (E1), pela utilização intensa de recursos fornecidos pela TI, e por isso se estabeleceu troca de conhecimentos (E3) ou por constantes questionamentos acerca de melhores práticas em segurança e sobre como operar de maneira mais eficiente os dispositivos que utiliza (E4). Dessa maneira, foi construído pelo Grupo 01 um conhecimento tecnicamente adequado.

Paralelamente, o Grupo 02 exerce um contato menos frequente e usualmente reativo com os especialistas da organização. Essa interação consiste, majoritariamente, em solicitações sobre como operar programas para a execução de tarefas básicas, a exemplo do Microsoft Word e navegadores de internet, além da solução de dúvidas acerca de possíveis riscos à segurança apenas quando esses se manifestam, uma prática de todos os componentes do grupo.

Ressalta-se, adicionalmente, que o comprometimento aos objetivos da SI na organização se destaca em diversos aspectos cognitivos mencionados, citados tanto no sentido da atenção a possíveis prejuízos à empresa, quanto na menção a sugestões de melhorias à organização e estímulo à conscientização de colegas. Com efeito, segundo as declarações obtidas pelo Grupo 01, a preocupação com a empresa exerce influência sobre esses usuários, uma vez que os estimula a adoção de diversos comportamentos seguros, a exemplo da execução de *backups*, cuidados no gerenciamento de senhas e cautela no acesso a websites.

Outra característica observada durante a investigação aos aspectos cognitivos dos participantes é a declaração de sensação de segurança e autoeficácia percebida no uso de tecnologias digitais. Dentre os entrevistados do Grupo 01, declarações explícitas e a firmeza e espontaneidade das respostas representam o aspecto, que é apontado como determinante à aproximação à tecnologia. É também vinculado usualmente à possessão de conhecimentos técnicos relacionados à utilização de tecnologia.

Em contrapartida, esse aspecto é inversamente percebido pelos participantes do Grupo 02, exemplificado pela ausência de firmeza e confiança nas respostas, feitas majoritariamente de maneira estimulada. A insegurança e o medo chegam a ser expressamente citados por E2, que afirma que esse sentimento cria barreiras para o seu aprendizado na utilização de dispositivos digitais. Dito isto, organizações devem estar atentas ao desenvolvimento de interesse/inclusão tecnológica e à redução da insegurança em usuários sêniores por meio de políticas que considerem as suas limitações e habilidades, a exemplo das características das inteligências dos mais velhos. Conforme mencionado durante a pesquisa, esses fatores podem ajudar no incremento da autoeficácia de empregados de idade avançada.

Ainda na seara dos aspectos cognitivos, o processo de construção do conhecimento técnico dos entrevistados é marcado por noticiários como fonte de informação sobre SI é verificada nos dois grupos, trazendo à discussão a necessidade de planejamento quanto à escolha da abordagem na conscientização dos empregados sêniores. Tal cenário torna-se mais oportuno numa conjuntura de envelhecimento populacional e predomínio da abordagem tecnicista de treinamento e conscientização de usuários de tecnologia.

Também chama a atenção o aspecto da transmissão de conhecimento via conversas informais com colegas, citado pelos dois grupos de entrevistados. Green e Dorey (2016) afirmam que essa maneira de difundir informações assemelha-se a uma fofoca, sobretudo quando disseminada por pessoas leigas, usualmente transmitida com inconsistências. A própria pesquisa trouxe diversos exemplos de declarações dos participantes que consistiam em conceitos técnicos incorretos, mostrando-se como ponto de atenção à organização no tocante à qualificação técnica em SI da força de trabalho.

O segundo objetivo específico diz respeito aos comportamentos efetivos dos usuários. Mais uma vez percebe-se discrepância entre os grupos, no que se refere à consciência acerca de possíveis prejuízos à organização em caso do exercício de comportamento inseguro. O Grupo 01 demonstrou comprometimento com a proteção à SI na organização em todos os aspectos relacionados a riscos que foram mencionados: cautela e busca por informações quando diante de riscos e ameaças. Em paralelo, o Grupo 02 traz como principal motivo para evitar riscos a perda de dados pessoais e recursos financeiros.

Há também a menção dos participantes de suas percepções acerca de como consequências em caso de mau uso os estimulam a buscar exercer um comportamento adequado. O cenário observado nos aspectos cognitivos foi mantido aqui: o Grupo 01 demonstrou maior comprometimento e maior detalhamento técnico ao expor as preocupações com as consequências, exemplificando cenários de risco com os quais costumam se deparar e maneiras de evita-los, a exemplo da execução de programas e na abertura de mensagens de e-mail. Para esses participantes, a preocupação com possíveis sanções administrativas também foi citada, indicando uma possível eficiência de uma política de responsabilização.

Ainda no ínterim dos aspectos comportamentais, chega à discussão a busca dos usuários por informações quando deparados em situações de risco, nas quais os entrevistados do Grupo 02 citaram buscar familiares e a própria instituição remetente da mensagem de texto/e-mail, ou do website que anunciou a oferta ou forneceu determinada informação. Percebe-se, dessa maneira, que os especialistas da organização não são a fonte primária de conhecimento sobre SI para esse grupo. Cabe assim, à organização, a discussão acerca de como estimular e estreitar o relacionamento entre seus empregados sêniores e a equipe de TI.

A percepção dos entrevistados acerca dos aspectos de processos também trouxe reflexões acerca do papel da organização no desenvolvimento da CSI em seus empregados sêniores. Observou-se que as políticas conduzidas pela empresa são observadas pelos participantes do Grupo 01, mas que há campo para melhoria do seu papel em proteger a informação e conscientizar esses usuários.

Nesse sentido, inicialmente foram observadas as questões relacionadas à política de senhas da empresa, que em virtude da dificuldade observada na memorização e compreensão do processo de troca mensal por parte dos empregados sêniores, definiu uma senha comum para a maioria dos computadores dos escritórios. Tal política é vista pelos entrevistados com maior grau de consciência como uma possível falha de segurança, percepção que tem amparo técnico na literatura. Em face desse cenário, cabe à organização ajustar suas políticas para contemplar as limitações dos empregados de idades mais avançadas, que estimule a memorização e conscientize os usuários à importância dessa prática.

A limitada adesão à prática de *backup* entre sêniores também foi observada, pois apenas 04 dos 07 participantes afirmaram fazê-lo. Além da reduzida sensação de autoeficácia na realização das cópias declarada por E2, E6, e E7, a maioria dos entrevistados desconhece a área de rede que passa por *backups* diários disponibilizada pela organização. O desconhecimento desse recurso faz com que os que aderem à prática busquem soluções particulares menos seguras, como discos rígidos externos e pen drives, que apesar de se constituírem em cópias de segurança, potencialmente expõem a riscos dados e informações importantes da organização armazenados nesses dispositivos.

Logo, pode-se perceber a que a comunicação da empresa com os empregados, sobretudo os sêniores, pode auxiliar esses usuários a exercerem um comportamento mais seguro. Além de ter sido citado como importante por esses próprios trabalhadores, ao mencionarem que alertas e lembretes podem ajudá-los na conscientização, o que pode ser potencializado pelo declínio de suas capacidades de memorização e inteligência fluida. Verifica-se que há campo para melhorias pelo fato de que o recurso da área de armazenamento fornecida pela organização é, por vezes, desconhecido, mesmo havendo histórico de perdas de dados importantes de empregados por falta de *backup*.

Com efeito, observa-se a importância de incrementar a comunicação acerca dos recursos tecnológicos disponibilizados, a exemplo da já citada área de *backup* e do sistema de protocolo eletrônico (E-DOC), e envolver os gestores no auxílio à conscientização e cobrança da utilização desses recursos. Uma vez que usuários sêniores são particularmente resistentes à adoção de tecnologias digitais, medidas como essas podem contribuir em sua adaptação.

Ainda no contexto do envolvimento dos gestores na implementação de medidas que conduzam os empregados a um comportamento mais seguro, a própria responsabilização em caso de mau uso foi citada por participantes. Políticas de responsabilização fazem parte da lista de procedimentos recomendados pela literatura para uma gestão de segurança da informação eficiente, principalmente num ambiente de mão de obra envelhecida e com dificuldades técnicas. Uma vez que sanções podem advir de um mau uso de ativos informacionais, usuários podem exercer um comportamento mais cauteloso.

Finalizando as discussões acerca dos aspectos de processos, foi avaliada a importância dos treinamentos na transferência de conhecimentos para os sêniores, já que o incentivo à qualificação formal e a disponibilidade de cursos e programas de desenvolvimento técnico em tecnologia e SI são escassos na organização. Em se tratando de segurança da informação não há nenhum programa de treinamento, estando ausente do planejamento da empresa a qualificação dos empregados nesse sentido. Adicionalmente, participantes da pesquisa citam a preocupação com a baixa adesão dos empregados aos já escassos treinamentos, e há relatos e observações que demonstram que a baixa sensação de autoeficácia pode estar contribuindo ao desinteresse em qualificação técnica.

Em face do exposto, observou-se na pesquisa que os principais fatores de afastamento dos usuários sêniores da organização às melhores práticas em SI são:

- O limitado contato com os especialistas de TI da empresa, que tende a proporcionar um maior intercâmbio de conhecimentos técnicos de qualidade;

- A reduzida percepção técnica das ameaças à segurança da informação, não tendo consciência do alcance dos danos de um comportamento inseguro;
- Um menor grau de comprometimento com os objetivos de segurança da informação da organização, representado pela ausência de preocupação com possíveis prejuízos à empresa (preocupações voltadas apenas a prejuízos pessoais);
- Comunicação deficiente por parte da gestão de tecnologia da organização, pela ausência do envio de alertas e lembretes aos empregados;
- Falta de envolvimento de gestores por parte da organização, seja no incentivo, atitude de exemplo ou cobrança/responsabilização em caso de comportamento inseguro;
- Baixa adesão a treinamentos, influenciada possivelmente por baixo interesse e sensação de baixa autoeficácia na operação de dispositivos digitais;

Como limitações do estudo podem-se mencionar tanto a limitação temporal, que não tornou possível a criação de mapas mentais individuais dos participantes, o que proporcionaria uma análise ainda mais didática e profunda de como percebem os sêniores da organização as dimensões da CSI. As restrições também tangem à condução de um estudo que se baseia na fala de participantes de uma pesquisa. Isto é, alguns entrevistados demonstraram estar pouco à vontade com o teor da entrevista, pela percepção aparente de que estariam sendo testados ou avaliados pela gestão da organização, aspecto observado por diversos autores que conduzem estudos que utilizam técnicas semelhantes de coletas de dados (YIN, 2019).

Por fim, no que se refere a sugestões a respeito de pesquisas futuras, entende-se que seriam oportunos à área acadêmica da Administração e gestão de empresas estudos voltados à compreensão de fatores de estímulo a empregados sêniores, voltado à qualificação e comprometimento a políticas de segurança à informação em organizações. Adicionalmente, lançar o olhar científico a temas da relação dos sêniores com a tecnologia da informação, sobretudo a segurança de dados e informações em ambientes organizacionais, contribuiria à inclusão tecnológica e social de indivíduos de idades mais avançadas, no sentido de auxiliar no desenvolvimento de políticas públicas que desenvolvessem uma maior sensação de autoeficácia nesses cidadãos. Recomenda-se, também, que se conduzam estudos semelhantes em empresas da iniciativa privada, avaliando possíveis diferenças nas percepções dos sêniores nesses ambientes, sobretudo em aspectos comportamentais e de processos.

Isto é, compreender cada vez mais a relação dos sêniores com as mais recentes tecnologias digitais, para auxiliar a torná-los cada vez mais digitalmente relevantes em um mercado de trabalho tão dependentes dessas ferramentas.

REFERÊNCIAS BIBLIOGRÁFICAS

ADAMCZYK, M.; BETLEJ, A. Social determinants of digital exclusion in an ageing society. The case of Poland. **Entrepreneurship and Sustainability Issues**, v. 8, n. 3, 2021.

ALVES-MAZZOTTI, A. J. Usos e abusos do estudo de caso. **Cadernos de Pesquisa**, v. 36, n. 129, p. 637-651, set./dez. 2006. Disponível em: www.scielo.br/pdf/cp/v36n129/a0736129.pdf. Acesso em: 10 jun. 13.

BANERJEE, C. *et al*. An Improvised Software Security Awareness Model. **International Journal of Information, Communication and Computing Technology**, [*s. l.*], v. 1, ed. 2, p. 1-5, 15 jan. 2013. DOI: JIMS 8i-Int'l J. of Inf. Comm. & Computing Technology (IJICCT). Disponível em: https://www.jimsindia.org/8i_journal/volumeii/an_improvised_software_security_awareness.pdf. Acesso em: 1 mar. 2022.

BBC NEWS - BBC. How to hack people. Reino Unido, 26 jun. 2002. Disponível em: http://news.bbc.co.uk/1/hi/technology/2320121.stm. Acesso em: 16 mar. 2022.

BARDIN, L. **Análise de conteúdo**. Lisboa: Edições 70, 2009

BELLUZZO, R. O uso de mapas conceituais e mentais como tecnologia de apoio à gestão da informação e da comunicação: uma área interdisciplinar da competência em informação. Revista de Biblioteconomia e Documentação, São Paulo, v. 2, n. 2, p. 78-89, dez. 2006. Disponível em: http://www.febab.org.br/rbbd/ojs2.1.1/index.php/rbbd/article/view/19/7. Acesso em: 11 abr. 2022.

BONNER, L. **Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches**. Washington University Journal of Law & Policy, Washington, v. 40, ed. 257, p. 257-277, 2012. DOI 1943-0000. Disponível em: https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1581&context=law_journal_law_policy. Acesso em: 20 mar. 2019.

BUZAN, T. **Dominando a técnica dos mapas mentais: guia completo de aprendizado e o uso da mais poderosa ferramenta de desenvolvimento da mente humana**; tradução Marcelo Brandão Cipolla. São Paulo: Cultrix, 2019.

CARLSON, E. **Phishing for Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting Them Follow**. Illinois University. 2015. Disponível em: http://publish.illinois.edu/elderlawjournal/files/2015/02/Carlson1.pdf. Acesso em 10 de jan. 2019.

CARROLL, J. **Human cognitive abilities: a survey of factor-analytic studies**. Nova York: Cambridge University Press, 1993.

CATTELL, R. **Where is intelligence? Some answers from the triadic theory**. J. J. McArdle & R. W. Woodcock. Human cognitive abilities in theory and practice. 1998. (pp. 29-38). New Jersey: Erlbaum.

CERVO, A; BERVIAN, P. **Metodologia científica**. 4 ed. São Paulo: Makron Books, 2002.

CHERDANTSEVA, Y.; HILTON, J. A Reference Model of Information Assurance & Security. **8th International Conference on Availability, Reliability and Security (ARES),** Reino Unido, 2 set. 2013. Disponível em: https://users.cs.cf.ac.uk/Y.V.Cherdantseva/RMIAS.pdf. Acesso em: 13 abr. 2022.

CHUA, C.; MYERS, M. Social control in Information Systems Development: a Negotiated Order Perspective. **Journal of Information Technology**, Vol. 33, No. 3, pp-173–187. 2017. DOI: https://doi.org/10.1057/s41265-017-0048-4

CÓDIGO FONTE. Artigos. In: SILVA, Carlos. **7 golpes de engenharia social que você precisa evitar**. [S. l.], 16 jul. 2018. Disponível em: https://www.codigofonte.com.br/artigos/7-golpes-de-engenharia-social-que-voce-precisa-evitar. Acesso em: 25 maio 2022.

CRESWELL, J. **Projeto de pesquisa:** métodos qualitativo, quantitativo e misto. Porto Alegre: Bookman, 2010.

CSIRO (Austrália). Cybertaipan. Module 3: Principles of cyber security. *In*: **Cybertaipan**: Australian Youth Cyber Defence Competition modelled on the US Air Force Association's CyberPatriot program. Austrália, 2018. Disponível em: https://www.csiro.au/en/education/programs/digital-careers/ctaipan. Acesso em: 17 maio 2023.

DEBERT, G. **A reinvenção da velhice: Socialização e Processos de Reprivatização do Envelhecimento**. 1ª ed. São Paulo: Editora da Universidade de São Paulo: Fapesp, 2004.

DEPARTAMENTO INTERSINDICAL DE ESTATÍSTICA E ESTUDOS SOCIOECONÔMICOS - DIEESE (Brasil). ANFIP. **Previdência: reformar para excluir?** Contribuição técnica ao debate sobre a reforma da Previdência Social brasileira. Brasília: ANFIP/DIEESE, 2017. Disponível em: https://www.dieese.org.br/evento/2017/reformarParaExcluirCompleto.pdf. Acesso em: 8 dez. 2021.

DIAS, I. O uso das tecnologias digitais entre os seniores: motivações e interesses. **Sociologia, Problemas e Práticas**, Lisboa, v. 68, ed. 68, p. 51-77, 2012. DOI 2182-7907. Disponível em: http://spp.revues.org/686. Acesso em: 11 fev. 2019.

ERNST AND YOUNG. **Global Information Security Survey 2021**. Nova Iorque**,** 2021. Disponível em: https://assets.ey.com/content/dam/ey-sites/ey-com/en_vn/topics/cybersecurity/ey-global-information-security-survey-2021.pdf?download Acesso em: 05 de jul. 2021.

ESTEVES, J.; GOMES, J. A contrarreforma da previdência, crise do capital e da previdência privada. **Revista Direito e Praxis**, Rio de Janeiro, v. 11, n. 4, p. 2572-2608, 2020. DOI 10.1590/2179-8966/2020/50102. Disponível em: https://www.scielo.br/j/rdp/a/BxrCgLcydPgHc8b9StwcZ4K/abstract/?lang=pt. Acesso em: 15 mar. 2022.

ESTEVES, P. **Uso da internet pelo consumidor da terceira idade: influências do risco percebido e impacto na intenção de compra online**. 2014. Tese (Doutorado) – Escola de Administração, Universidade Federal do Rio Grande do Sul, Programa de Pós-Graduação em Administração, Porto Alegre.

FARIVAR, S. *et al*. Wearable device adoption among older adults: A mixed-methods study. **International Journal of Information Management**, v. 55, 2020.

FEDERAL BUREAU OF INVESTIGATION - FBI. **Elder Fraud Report 2022**. EUA, 2023. Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf. Acesso em: 10 maio 2023.

FELIX, J. O idoso e o mercado de trabalho. *In*: ALCÂNTARA, Alexandre; CAMARANO, Ana; GIACOMIN, Karla. **Política Nacional do Idoso: velhas e novas questões**. Rio de Janeiro: Ipea, janeiro 2016. cap. 9, p. 241-265. ISBN 978-85-7811-290-5.

FRANÇA, W. **Criptografia**. 2005. Disponível em: http://www.ucb.br/sites/100/103/TCC/22005/WaldizarBorgesdeAraujoFranco.pdf Acesso em: 26 de fev. 2019.

FRIEDBERG, L. **The impact of technological change on older workers: evidence form data on computers**. 2001, NBER Working Paper 8297.

FLICK, U. **Introdução à pesquisa qualitativa**. 3 ed. Porto Alegre: Bookman, 2009.

FÓRUM ECONÔMICO MUNDIAL – FEM. **Understanding the impact of digitalization on society**: In the face of huge societal challenges, how can digital transformation make a positive contribution? 2022. Disponível em: https://reports.weforum.org/digital-transformation/understanding-the-impact-of-digitalization-on-society/. Acesso em: 19 abr. 2022.

FRANCO, M. **Análise do conteúdo**. Brasília: Liber Livro, 2008.

FREITAS, W.; JABBOUR, C. Utilizando Estudo De Caso(S) Como Estratégia De Pesquisa Qualitativa: Boas Práticas E Sugestões. Estudo & Debate, Lajeado, v. 18, ed. 2, p. 07-22, 2011. Disponível em: http://www.meep.univates.br/revistas/index.php/estudoedebate/article/view/560/550. Acesso em: 4 jul. 2023.

FRIK, A. *et al*. **Privacy and Security Threat Models and Mitigation Strategies of Older Adults**. 2019.

GARDNER, B.; THOMAS, V. **Building an information security awareness program: Defending against social engineering and technical threats**, 1st ed. Waltham: Elsevier, 2014.

GOVERNO DO ESTADO (Sergipe). Empresa de Desenvolvimento Agropecuário de Sergipe. **A Emdagro**. [S. l.], 2023. Disponível em: https://emdagro.se.gov.br/a-empresa/. Acesso em: 17 out. 2023.

GREEN, J.; DOREY, P. **The Weakest Link**, 1ª ed. Londres: Bloomsbury, 2016.

HADNAGY, C. **Social Engineering. The art of Human Hacking**. Indianapolis: Wiley Publishing, 2018.

HAEUSSINGER, F. *In*: HAEUSSINGER, F. **Studies on Employees' Information Security Awareness**. Orientador: Prof. Dr. Lutz M. Kolbe. 2015. Tese (Doutorado), Munique, 2015. p. 200. DOI http://dx.doi.org/10.53846/goediss-5137. Disponível em: https://ediss.uni-goettingen.de/bitstream/handle/11858/00-1735-0000-0022-6021-8/Dissertation_Haeussinger_FINAL.pdf?sequence=1&isAllowed=y. Acesso em: 15 fev. 2022.

HAIR JR.; J. *et al.* **Fundamentos de métodos de pesquisa em administração**. Porto Alegre: Bookman, 2007.

HARGITTAI, E.; DOBRANSKY, K. Old dogs, new clicks: Digital inequality in skills and uses among older adults. **Canadian Journal of Communication**, [*S. l.*], v. 42, p. 195-212, 14 mar. 2017. Disponível em: http://doi.org/10.22230/cjc.2017v42n2a3176. Acesso em: 12 abr. 2022.

HELLQVIST, F. *et al*. Getting their Hands Stuck in the Cookie Jar: STUDENTS' SECURITY AWARENESS IN 1:1 LAPTOP SCHOOLS. **International Journal of Public Information Systems**, Suécia, v. 2013, n. 1, 2013. Disponível em: http://www.ijpis.net/ojs/index.php/IJPIS/article/download/102/pdf_1. Acesso em: 12 abr. 2022.

HERATH, T; RAO, H. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. **Decision Support Systems**, Buffalo, v. 47, p. 154-165, 27 fev. 2009. DOI https://doi.org/10.1016/j.dss.2009.02.005. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167923609000530. Acesso em: 19 abr. 2023.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA – IBGE. **Projeção da população. Projeções da População do Brasil e Unidades da Federação por sexo e idade: 2010-2060**. 2019. Disponível em: ftp://ftp.ibge.gov.br/Projecao_da_Populacao/Projecao_da_Populacao_2018/projecoes_2018_populacao_idade_simples_2010_2060.xls. Acesso em: 05 jul 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27000:2022: Information security, cybersecurity and privacy protection — Information security controls, Suíça, ano 5, 15 fev. 2022. Disponível em: https://www.iso.org/standard/75652.html. Acesso em: 27 maio 2022.

KAMARIZA, Y. **Implementation of information security policies in public organizations: Top management as a success factor**. Orientador: May Wismen, Christina Keller. 2017. 165 p. Tese (Doutorado) - Jönköping University - International Business School, Jönköping, 2017.

KANFER, R; ACKERMAN, P. Aging, Adult Development, and Work Motivation. **The Academy of Management Review**, [*s. l.*], v. 29, ed. 3, p. 440-458, jul. 2004. DOI https://doi.org/10.2307/20159053. Disponível em: https://doi.org/10.2307/20159053. Acesso em: 11 abr. 2023.

KASPERSKY. **Older and wiser? A look at the threats faced by over-55s online**. 2017. Disponível em: https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2017/05/10084116/Report_Over-55s_Online_ENG_UPD.pdf Acesso em 08 de jan. 2019.

KRAIGER, K. Designing Effective Training for Older Workers. In: PARRY, E; MCCARTHY, J. The Palgrave Handbook of Age Diversity and Work. 1. ed. Menphis: Palgrave Macmillan London, 2017. p. 639-667. ISBN 978-1-137-46781-2. Disponível em: https://link.springer.com/book/10.1057/978-1-137-46781-2. Acesso em: 8 jun. 2023.

KRAISIG, Â.; BRAIBANTE, M. MAPAS MENTAIS: INSTRUMENTO PARA A CONSTRUÇÃO DO CONHECIMENTO CIENTÍFICO RELACIONADO À TEMÁTICA “CORES”. **South American Journal of Basic Education, Technical and Technological,** *[S. l.]*, v. 4, n. 2, 2017. Disponível em: https://periodicos.ufac.br/index.php/SAJEBTT/article/view/1273. Acesso em: 18 jul. 2023.

LIEBSCHER, P. Quantity with quality? Teaching quantitative and qualitative methods in a LIS Master’s program. **Library Trends**, v. 46, n. 4, 1998, p. 668-680.

LI, Q.; LUXIMON, Y. Older Adults and Digital Technology: A Study of User Perception and Usage Behavior. **Advances in Physical Ergonomics and Human Factors**: Advances in Intelligent Systems and Computing, Hong Kong, p. 155-163, janeiro 2016. DOI DOI 10.1007/978-3-319-41694-6_16. Disponível em: http://encurtador.com.br/prwKZ. Acesso em: 2 mar. 2022.

LIM, J. *et al*. Embedding Information Security Culture Emerging Concerns and Challenges. **Association for Information Systems**: AIS Electronic Library (AISeL), Pacific Asia Conference on Information Systems (PACIS), v. 43, ed. PACIS 2010 Proceedings, p. 463-474, 2010.

LLORENTE-BARROSO, C. *et al*. Administración electrónica y trámites online: hacia la autonomía y el empoderamiento de las personas mayores. **El Profesional de la información**. v. 26 n. 1, p. 34-14 42, 2018. Disponível em: http://encurtador.com.br/cqzQ7. Acesso em: 10 set. 2018.

LOHANI, S. Social Engineering: Hacking into Humans. **Special Issue based on proceedings of 4th International Conference on Cyber Security (ICCS)**, Índia, 5 fev. 2019. Disponível em: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3329391_code3240942.pdf?abstractid=3329391&type=2. Acesso em: 16 fev. 2022.

LYRA, M. **Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro: Ciência Moderna, 2015.

MAMEDOVA, N. *et al*. Social engineering in the context of ensuring information security. **Current Issues of Linguistics and Didactics: The Interdisciplinary Approach in Humanities and Social Sciences**, Rússia, ano 2019, v. 69, n. 73, 25 out. 2019. DOI https://doi.org/10.1051/shsconf/20196900073. Disponível em: https://www.shs-conferences.org/articles/shsconf/pdf/2019/10/shsconf_cildiah2019_00073.pdf. Acesso em: 12 abr. 2022.

MANNHEIM, I. *et al*. Inclusion of Older Adults in the Research and Design of Digital Technology. **International Journal of Environmental Research and Public Health**, [*S. l.*], ano 3718, n. 16, p. 1-17, 2 out. 2019. DOI doi:10.3390/ijerph16193718. Disponível em: https://www.researchgate.net/publication/336226875_Inclusion_of_Older_Adults_in_the_Research_and_Design_of_Digital_Technology/fulltext/5d9543a9299bf1c363f2c3f6/Inclusion-of-Older-Adults-in-the-Research-and-Design-of-Digital-Technology.pdf. Acesso em: 23 nov. 2021.

MARCON, S.; ELSEN, I. Estudo qualitativo utilizando observação participante - análise de uma experiência. Acta Scientiarum, v.22, n.2, p.637-647. 2000.

MARTINS, G. Estudo de caso: uma reflexão sobre a aplicabilidade em pesquisa no Brasil. **Revista de Contabilidade e Organizações**, São Paulo, v. 2, ed. 2, p. 8-18, 11 abr. 2008. DOI https://doi.org/10.11606/rco.v2i2.34702. Disponível em: https://www.revistas.usp.br/rco/article/view/34702/37440. Acesso em: 5 jan. 2022.

MASUCH, K. *et al*. The Impact of Threat and Efficacy on Information Security Behavior: Applying an Extended Parallel Process Model to the Fear of Ransomware. **Hawaii International Conference on System Sciences**, Havaí, p. 6691-6700, 2021. Disponível em: https://scholarspace.manoa.hawaii.edu/bitstream/10125/71423/1/0654.pdf. Acesso em: 9 mar. 2022.

MAXWELL, J. **Qualitative research design: An interactive approach**. 2ª Edição. Thousand Oaks, Reino Unido: Sage. 2005.

MELO NETO, P. ARAÚJO, W. Segurança da informação: uma visão sistêmica para implantação em organizações – João Pessoa: Editora da UFPB, 2019.

MENG, F. *et al.* Investigating the adoption of mobile health services by elderly users: Trust transfer model and survey study. **JMIR mHealth and uHealth**, v. 7, n. 1, 2019.

MENTLIK, G. *et al*. **Aposentadoria e Mercado de Trabalho: uma Análise Usando Regressão Descontínua**. Policy Paper, [s. l.], ed. 37, 2 jan. 2019. Disponível em: https://www.insper.edu.br/wp-content/uploads/2019/01/Aposentadoria-Mercado-Trabalho-Regressao-Descontinua.pdf. Acesso em: 13 ago. 2019.

MICHAELIS. **Moderno Dicionário da Língua Portuguesa**. 1. ed. [*S. l.*]: Melhoramentos, 2004. 2268 p. ISBN 8506027594.

MINAYO, M. **Pesquisa Social: teoria, método e criatividade**. Petrópolis: Vozes, 1994.

OLANIRAN, B. *et al*. A Gamer's Nightmare: An Analysis of the Sony PlayStation Hacking Crisis. **Journal of Risk Analysis and Crisis Response**, Estados Unidos, v. 4, ed. 3, p. 151-159, setembro 2014. Disponível em: https://jracr.com/index.php/jracr/article/view/107. Acesso em: 18 fev. 2022.

ONTORIA PEÑA, A. *et al*. **Potencializar a capacidade de aprender e pensar: o que mudar para aprender e como aprender para mudar**. São Paulo: Madras, 2004.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS - ONU. **Young or old, UN calls for 'digital equality' for all**. [*S. l.*]: UN Affairs, 30 set. 2021. Disponível em: https://news.un.org/en/story/2021/09/1101882. Acesso em: 19 set. 2023.

PETER, K. A Virtue Ethics Analysis of the 2011 PlayStation Network Data Breach. **STS Research Paper**, Virgínia, p. 1-14, 10 abr. 2020. Disponível em: https://libraetd.lib.virginia.edu/downloads/9k41zf25d?filename=Peter_Kyle_STS_Research_Paper.pdf. Acesso em: 23 mar. 2022.

PRAWOBO, H.; TJONG, Y. Benefits to implementing IT governance in higher education: (Systematic literature review). **International Conference on Information Management and Technology (ICIMTech)**, Indonésia, p. 35-38, 2017. DOI 10.1109/ICIMTech.2017.8273507. Disponível em: https://www.researchgate.net/profile/Yanti-Tjong-3/publication/322877453_Benefits_to_implementing_IT_governance_in_higher_education_Systematic_literature_review/links/5c5a7664299bf1d14caf3a90/Benefits-to-implementing-IT-governance-in-higher-education-Systematic-literature-review.pdf. Acesso em: 15 mar. 2022.

PRISLAN, K *et al*. A real-world information security performance assessment using a multidimensional socio-technical approach. **PLOS ONE**, Slovenia, 8 set. 2020. DOI https://doi.org/10.1371/journal.pone.0238739. Disponível em: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0238739. Acesso em: 13 abr. 2023.

PSAFE. Dfndr Blog: Ciberataques. In: BIANCAMANO, Paula. **Spear phishing: o que é e como se proteger? Conheça essa ameaça que se esconde em e-mails para roubar dados pessoais e corporativos**. [S. l.], 3 dez. 2021. Disponível em: https://www.psafe.com/blog/spear-phishing-o-que-e-e-como-se-proteger/. Acesso em: 19 maio 2022.

PWC. A global state of information security. 22. ed. Disponível em: https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2021/global-digital-trust-insights-survey-2022.html. Acesso em: 20 de setembro de 2022.

QUEIROZ, R. *et al*. OBSERVAÇÃO APLICADA À PESQUISA QUALITATIVA. In: ESTUDOS QUALITATIVOS: Enfoques Teóricos e Técnicas de Coleta de Informações. Sobral: [s. n.], 2018. cap. 15, p. 257-267. ISBN 978-85-9539-016-4. Disponível em: https://portais.univasf.edu.br/medicina-pa/pesquisa/producao-cientifica/experiencias-qualitativas-ebook. Acesso em: 17 maio 2023.

RAO, U.; NAYAK, U. **The InfoSec Handbook: An Introduction to Information Security**. 1. ed. New York: Apress Media, 2014. 376 p. ISBN 978-1-4302-6382-1.

RICHARDSON, R. **Pesquisa social.** 3. ed. São Paulo: Atlas, 1999.

SAFETYDETECTIVES. O que é engenharia social e por que é uma ameaça em 2022? O que é um ataque de engenharia social? [S. l.], 2022. Disponível em: https://pt.safetydetectives.com/blog/o-que-e-engenharia-social-e-por-que-e-uma-ameaca-tao-grande/. Acesso em: 24 maio 2022.

SALES, J. **Ações Coletivas Suportadas pela Tecnologia da Informação em Comunidades de Prática: os efeitos indutores à configuração dos coletivos inteligentes**. Orientador: Dr. Jairo Simião Dornelas. 2012. 174 p. Tese (Doutorado) - Universidade Federal de Pernambuco, Recife, 2012.

SAMPIERI, R. *et al*. Metodologia da pesquisa. 5ª ed. Porto Alegre (RS): AMGH, 2013.

SANTIAGO, P. **De la expression corporal a la comunicación interpersonal**. Madrid: Narcea, 1985.

SCHELINI, W. **Teoria das inteligências fluida e cristalizada: início e evolução**. Estudos. Psicológicos. (Natal), Natal, v. 11, n. 3, p. 323-332, Dec. 2006. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-294X2006000300010&lng=en&nrm=iso. Acesso em 01 jul 2020.

SILVA, M. **Mapas mentais**: uma ferramenta para o desenvolvimento da competência em informação. 2010. Trabalho de conclusão de curso (Graduação em Biblioteconomia) – Curso de Biblioteconomia e Gestão de Unidades de Informação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2010.

SOH, P. *et al*. Perception, acceptance and willingness of older adults in Malaysia towards online shopping: a study using the UTAUT and IRT models. **Journal of ambient intelligence and humanized computing**, 2020.

SPEARS, J.; BARKI, H. User participation in information Systems Security Risk Management. **MIS Quarterly**, Chicago, v. 34, n. 3, p. 503-522, SETEMBRO 2010. Disponível em: https://misq.umn.edu/skin/frontend/default/misq/pdf/appendices/2010/SpearsBarkiAppendices.pdf. Acesso em: 12 abr. 2022.

STELZER, J. *et al*. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E OS DESAFIOS DAS INSTITUIÇÕES DE ENSINO SUPERIOR PARA A ADEQUAÇÃO. **Colóquio Internacional de Gestão Universitária**: Universidade e Desenvolvimento Sustentável: desempenho acadêmico e os desafios da sociedade contemporânea, Florianópolis - SC, 25 nov. 2019. Disponível em: https://repositorio.ufsc.br/handle/123456789/201939. Acesso em: 19 abr. 2022.

STEWART, J. *et al*. **ISC Certified Information Systems Security Professional**: Official Study Guide. 7. ed. atual. Indianapolis: Sibex, 2015. 1561 p. ISBN 978-1-119-04275-4.

THOMPSON, L.; MAYHORN, C. **Aging workers and technology**. Oxford handbook of work and aging. NY: Oxford University Press. 2012.

TRANSPARÊNCIA SERGIPE. **Servidores por Órgão**. 2023. Disponível em: http://www.transparenciasergipe.se.gov.br/TRS/Pessoal/PorOrgao.xhtml. Acesso em: 05 jul. 2022.

TSOHOU, A. *et al*. Investigating Information Security Awareness: Research and Practice Gaps. **Information Security Journal A Global Perspective,** Grécia, v. 17, n. 6, ed. 5, p. 207-227, dezembro 2008. DOI 10.1080/19393550802492487. Disponível em: https://www.researchgate.net/profile/Spyros-Kokolakis/publication/220449896_Investigating_Information_Security_Awareness_Research_and_Practice_Gaps/links/0912f50be002093bf3000000/Investigating-Information-Security-Awareness-Research-and-Practice-Gaps.pdf. Acesso em: 7 mar 2022.

VERGARA, Sylvia C. **Métodos de pesquisa em administração**. São Paulo: Atlas, 2005.

VOSS, C. *et al*. Case research in operations management. **International Journal Of Operations & Production Management**, v. 22, n. 2, 2002, p. 195-219.

ZANELLI, J. C. Pesquisa qualitativa em estudos da gestão de pessoas. **Estudos da Psicologia**, n. 7, 2002, p.79-88.

WALSHAM, G. Doing interpretive research. **European Journal of Information Systems**, Vol.15, pp.320-330. 2006.

WHITMAN, M.; MATTORD, H. **Principles of Information Security: Fourth Edition**. 6. ed. atual. Boston, MA: Cengage Learning, 2017. 658 p. ISBN 978-1337102063.

ZANELLI, J. Pesquisa qualitativa em estudos da gestão de pessoas. Estudos de Psicologia (Natal), v. 7, n. spe, p. 79–88, 2002.

YIN, R. **Case Study Research and Applications: Design and Methods** (English Edition). 6th Edição. Califórnia: SAGE Publications, 2019.

APÊNDICE A - Roteiro de entrevista semiestruturado

Categoria COG - Aspectos cognitivos

1 - A Segurança da Informação é colocada em prática pela utilização segura de celulares, computadores e tablets, bem como o uso consciente dos serviços de rede fornecidos pela empresa. Na sua opinião, que ações podem ser tomadas no dia a dia para proteger a informação?

2 – Que tipo de prejuízos você acha que podem ocorrer caso dados e informações sigiloso e o ambiente de rede da empresa sejam acessados por pessoas não autorizadas?

3 – De onde surgiram as percepções que você mencionou acerca da segurança da informação?

Categoria COM - Aspectos comportamentais

4 - Você costuma buscar informações acerca dos riscos à segurança da informação? Se sim, como faz isso (por exemplo: vídeos, leituras, consulta ao setor de TI)?

5 – Como você costuma proceder em caso de uma situação de potencial risco, ou dúvida sobre algo potencialmente perigoso? (exemplo: e-mail duvidoso de fonte desconhecida ou ligação/mensagem de aplicativo pedindo dados pessoais sensíveis)

6 – Quais os principais motivos pelos quais você toma cuidados com a segurança da informação?

Categoria PRO - Aspectos de processos

7 – A empresa toma algumas precauções para aumentar a segurança da informação, a exemplo de instalar antivírus, definir trocas de senhas mensais e exibir lembrete no expresso sobre a importância de proteger a informação. Qual sua opinião sobre elas?

8 – De que maneiras você acha que a empresa poderia estimular mais a segurança da informação?

APÊNDICE B – Scripts de observação

Script de observação 01

Evento	Visita do Entrevistado 03 ao setor de informática.
Local	Setor de informática - EMDAGRO
Data	09/03/2023
Pauta	Solicitar instalação de antivírus

Quadro 1 – Aspectos da Conscientização em Segurança da Informação observados

ASPECTOS OBSERVADOS	
Aspectos Cognitivos	Noção dos riscos, ao afirmar espontaneamente que entende a necessidade da instalação do agente de segurança em seu computador;
	Percepção da importância do agente, por dizer que não poderia "ficar sem" ele no computador que utiliza;
	Capacidade técnica de observar que o agente está ausente.
Aspectos Comportamentais	Demonstrou comprometimento com a busca pela segurança da informação ao apresentar-se espontaneamente ao setor de informática para a instalação do agente de segurança;
	Exerce o comportamento que descreveu em respostas às Questões 04 e 06 do roteiro de entrevistas, ao dizer que costuma visitar o setor de informática em busca de informações e suporte técnico;
Aspectos de Processos	Participante exerce comportamento de contribuição à proteção do computador que utiliza, dos dados que estão nele armazenados e do ambiente de rede da organização por observar a presença e correto funcionamento do antivírus em sua estação de trabalho (política de segurança vigente na empresa).

Script de observação 02

Evento	Visita da Entrevistada 02 (E2) ao setor de informática.
Local	Setor de informática - EMDAGRO
Data	10/04/2023
Pauta	Solicitar auxílio na operação do computador (conectividade de rede e Microsoft Word)

Quadro 1 – Aspectos da Conscientização em Segurança da Informação observados

ASPECTOS OBSERVADOS	
Aspectos Cognitivos	Ausência de conhecimentos necessários para o ajuste da conexão de rede do computador, mesmo após diversas solicitações de suporte para realização do referido ajuste (visitas em (14/12/2022 e 06/02/2023);
	Usuária visita o setor de informática trazendo o seu computador portátil ao setor de informática sem executar a atualização do antivirus que está sendo solicitada via janela;
	Entrevistada visita o setor de informática de maneira recorrente com programas potencialmente perigosos instalados em seu computador, a exemplo de jogos eletrônicos e extensões de navegador de fontes não oficiais. Tais programas podem ser fonte de problemas de segurança, segundo Kaspersky (2017) e FBI (2022b);
	Apesar da presente visita ter como objetivo solucionar falta de conectividade à internet e prestar consultoria na utilização do Microsoft Word do computador da usuária, é possível observar a dificuldade que a usuária encontra para assimilar conhecimentos técnicos. É possível observar o cenário após outras visitas para sanar as mesmas dúvidas, o que corrobora os relatos da participante nas Questões 01, 02 e 04 do roteiro de entrevistas.
Aspectos Comportamentais	Usuária confirma, ao trazer o computador portátil ao setor de informática, que não tem preocupação com o antivírus, pois não executa a atualização do agente mesmo quando solicitada;
	Mesmo após prévias orientações e desinstalações dos softwares potencialmente perigosos instalados pela usuária, demonstra-se, ao verificar que tais programas estavam instalados novamente, pouca contribuição da participante no sentido de exercer um comportamento não seguro;
Aspectos de Processos	Participante exerce comportamento de pouca conscientização com a política de utilização de computadores portáteis, pois instala programas potencialmente perigosos e mantém o equipamento em péssimo estado de conservação (teclas arrancadas e tela rachada). Ressalta-se que a participante deixou de ter permissão administrativa no dispositivo após esse atendimento.

Script de observação 03

Evento	Operações no dia a dia da organização – Setor de convênios
Local	EMDAGRO – Setor de convênios
Data	Junho de 2022
Pauta	Solicitação de atendimento a computador que sofreu ataques de *ransomware*.

Quadro 1 – Aspectos da Conscientização em Segurança da Informação observados

ASPECTOS OBSERVADOS	
Aspectos Cognitivos	O usuário sênior, gestor do setor de convênios da organização, executou um anexo fraudulento de uma mensagem de e-mail, demonstrando desconhecimento acerca dos riscos desse tipo de ação.
	A vítima alegou que a mensagem mencionava uma situação relacionada a um suposto débito do usuário com a Receita Federal, e por isso se preocupou e decidiu executar o anexo. Vale ressaltar que o empregado é contador e envia anualmente as declarações de imposto de renda de diversos outros usuários da organização, o que demonstra um ataque direcionado por parte dos criminosos que enviaram o e-mail fraudulento. Tal situação consiste em uma demonstração da eficácia da Engenharia Social nos sêniores, pois o atacante utilizou de tática dessa área do conhecimento para "convencer" a vítima com uma abordagem crível à mesma.
	Percebe-se, adicionalmente, que o usuário além de não ter consciência acerca do risco de sua ação, não possuía *backup* dos dados sensíveis existentes no computador que utilizava, o que resultou na perda dos mesmos arquivos.
Aspectos Comportamentais	O empregado não demonstrou cautela nem buscou informações acerca do e-mail possivelmente fraudulento, não demonstrando condições de agir em conformidade com os objetivos da SI na organização. Alem disso, a ausência de backup pôs em grave risco dados importantes da organização.
Aspectos de Processos	O usuário desconhece o ambiente de rede destinado ao backup de dados importantes, situação que é agravada por falhas na comunicação da equipe de tecnologia da informação.

Script de observação 04

Evento	Operações no dia a dia da organização – Setores de Defesa Animal e Coordenadoria de Geoprocessamento
Local	EMDAGRO – Diversos setores da empresa
Data	Junho de 2022 a setembro de 2022
Pauta	Observação da utilização de dispositivos digitais pelos usuários sêniores da organização

Quadro 1 – Aspectos da Conscientização em Segurança da Informação observados

ASPECTOS OBSERVADOS	
Aspectos Cognitivos	Verifica-se que diversos sêniores da empresa apresentam baixa percepção de autoeficácia na operação de computadores e sistemas, aspecto que se manifesta em diversas declarações durante as atividades no dia a dia da organização. Apesar da alta capacidade técnica em suas funções, a exemplo de empregados das coordenações de defesa animal e geoprocessamento, e possível ouvir declarações autodepreciativas feitas pelos trabalhadores, incluindo gestores (coordenadores de programas, de divisão e diretores): “não entendo nada de sistema”, “deixa isso pros mais jovens”, “não tenho idade pra isso”.
	A materialização da ausência de autoeficácia e baixo comprometimento em relação à tecnologia de alguns sêniores se reflete na transferência de tarefas relacionadas a sistemas, que usualmente são assumidas pela equipe de TI (há um “consenso” por parte de gestores e até de diretores da empresa de que, por serem executadas em computadores e sistemas, essas tarefas tendem a ser “supervisionadas” ou “acompanhadas” de perto por especialistas em tecnologia). A nível de exemplo, tarefas relacionadas à documentos de trânsito animal, operação do sistema de geração de títulos fundiários e assinatura digital de documentos são frequentemente transferidas a técnicos de TI.
	Observa-se ainda a sensação de baixa autoeficácia nos sêniores pela solicitação de acompanhamento de técnicos da equipe de informática durante reuniões virtuais de setores não relacionados à área de TI. É comum ouvir a justificativa de que a presença se faz necessária em caso de alguma dúvida tecnológica ocorrer ou algum problema técnico advir, o que reduz a produtividade da equipe técnica e impede atendimentos urgentes de serem feitos.
Aspectos Comportamentais	Diversos usuários sêniores da organização, sobretudo no setor de defesa animal e coordenadoria de geoprocessamento, demonstram pouco interesse e comprometimento no aprendizado da operação de sistemas que são disponibilizados. Nesse sentido, outros profissionais são sobrecarregados (sobretudo terceirizados mais jovens e a própria equipe de tecnologia da informação) e a organização tende a perder em produtividade.

Aspectos de Processos	A conivência da gestão da empresa (que por vezes apresenta as mesmas percepções acerca da tecnologia) a esse tipo de comportamento, tanto da diretoria como da assessoria de TI, acaba por transferir a execução dessas tarefas à equipe de tecnologia. Tal prática, além de desestimular o aprendizado dos usuários originalmente responsáveis por essas atividades, atribui possível responsabilização em caso de falhas a outros empregados. Muitos gestores e diretores da empresa, por enxergarem diversas barreiras na utilização da tecnologia digital, percepção causada por uma baixa sensação de autoeficácia, exercem um comportamento contrário ao recomendado pela literatura especializada. Podem estar atuando, dessa maneira, por desencorajar os empregados à incrementar sua autoeficácia na relação com a tecnologia.