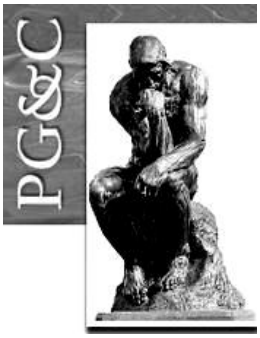



# SEGURANÇA DA INFORMAÇÃO ENTRE EMPREGADOS IDOSOS: ASPECTOS DE AFASTAMENTO A BOAS PRÁTICAS EM UMA ORGANIZAÇÃO PÚBLICA SERGIPANA

**Filipe Valença e Silva**
Mestre em Administração pela Universidade Federal de Sergipe, Brasil.
E-mail: filipevalenca.ti@gmail.com

**Jefferson David Araújo Sales**
Doutor em Administração pela Universidade Federal de Pernambuco, Brasil.
Professor da Universidade Federal de Sergipe, Brasil.
E-mail: profsales@hotmail.com

**Resumo**
O presente estudo tem como objetivo investigar a percepção dos idosos acerca das dimensões/aspectos da conscientização em segurança da informação em um ambiente corporativo, identificando fatores de afastamento dessas pessoas às melhores práticas de proteção à informação em uma empresa pública sergipana. Utiliza-se como estratégia 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 são analisados via análise de conteúdo. Dentre os fatores de afastamento às melhores práticas em segurança da informação, verificam-se: limitado contato com os especialistas de tecnologia da informação da empresa, que tende a proporcionar intercâmbio de conhecimentos técnicos aderentes a boas práticas em segurança da informação; 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 somente a prejuízos pessoais; comunicação deficiente por parte da gestão de tecnologia da organização; falta de envolvimento de gestores da organização; e baixa adesão a treinamentos, influenciada possivelmente por baixo interesse e sensação de baixa autoeficácia na operação de dispositivos digitais. A nível de pesquisas futuras, recomenda-se, que se conduzam estudos semelhantes em empresas privadas, avaliando possíveis diferenças nas percepções dos idosos nesses ambientes, sobretudo em aspectos comportamentais e de processos.

**Palavras-chave:** segurança da informação; idosos; ambiente organizacional; estudo de caso.

## *INFORMATION SECURITY AMONG ELDERLY EMPLOYEES: ASPECTS OF DISENGAGEMENT TO GOOD PRACTICES IN A PUBLIC ORGANIZATION IN SERGIPE*

***Abstract***
*The present study aims to investigate the perception of elderly individuals regarding the dimensions/aspects of information security awareness in a corporate environment, identifying factors that distance these individuals from best practices for information protection in a public company in Sergipe. A unique, embedded qualitative case study is conducted, with a descriptive and exploratory approach, using data collected through interviews guided by a semi-structured script and through observation of the company's activities. The data are analyzed using content analysis. Among the factors*


DOI: https://dx.doi.org/10.22478/ufpb.2236-417X.2024v14n3.69705
http://periodicos.ufpb.br/ojs2/index.php/pgc. ISSN: 2236-417X. 

*distancing individuals from best practices in information security, the following are identified: limited contact with the company's information technology specialists, which tends to provide an exchange of technical knowledge related to good information security practices; reduced technical perception of threats to information security, with a lack of awareness regarding the extent of damage from unsafe behavior; a lower degree of commitment to the organization's information security objectives, represented by a lack of concern for potential losses to the company, with worries focused solely on personal losses; deficient communication from the organization's technology management; lack of involvement from the organization's managers; and low adherence to training, possibly influenced by low interest and a sense of low self-efficacy in operating digital devices. For future research, it is suggested that similar studies be conducted in private companies, evaluating possible differences in the perceptions of elderly individuals in these environments, particularly concerning behavioral and process aspects.*

**Keywords:** information security; elderly people; organizational environment; case study.

## 1 INTRODUÇÃO

A Organização Mundial da Saúde (OMS, 2024) classifica como idosos os adultos com mais de 60 anos de idade. Esse estrato social é visto pela literatura especializada em segurança da informação (SI) como particularmente vulnerável a cybercriminosos. Para o *Federal Bureau of Investigation*, ou FBI estadunidense, as perdas financeiras desse domínio populacional aumentaram 84% entre 2020 e 2022, alcançando a soma de US$ 3,1 bilhões. São os maiores valores entre as 06 faixas etárias verificadas no relatório anual de perdas com ataques cibernéticos da agência norte-americana (FBI, 2023).

Nesse interim, estimativas do Instituto Brasileiro de Geografia e Estatística (IBGE, 2019) sinalizam que idosos estarão mais ativos no mercado de trabalho nos próximos anos, sobretudo 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 à busca por suplementação de renda nos próximos anos (DIEESE, 2017; IBGE, 2019).

Adicionalmente, os próprios usuários de dispositivos digitais são descritos como causadores de cerca de 70% dos incidentes de segurança da informação (Green; Dorey, 2016). Dito isto, esse estudo recorre ao conceito da Conscientização em Segurança da Informação (CSI), que aborda o conjunto dos aspectos referentes à consciência do usuário quanto a ameaças e boas práticas em SI em um ambiente organizacional. Com efeito, a investigação do nível de CSI de empregados pode auxiliar na identificação de fatores de afastamento de usuários de uma organização às boas práticas em SI (Haeussinger, 2017).

Considerando as estimativas do mercado de trabalho, a relação dos idosos com a segurança da informação e o aumento na frequência das ameaças de segurança expostos até aqui, essa pesquisa teve como objetivo investigar a percepção de empregados idosos acerca dos aspectos da CSI num ambiente corporativo, identificando fatores de afastamento a boas práticas de proteção à informação. Para o alcance desse objetivo foram investigadas as percepções de idosos de uma organização pública sergipana acerca dos aspectos componentes da CSI, a saber: cognitivos, comportamentais e de processos. Após concluídas as investigadas das percepções dos idosos da empresa, foram elaborados mapas mentais para a visualização dos fatores de afastamento dos usuários da organização a boas práticas em SI.

A pesquisa foi empreendida em uma organização pública sergipana: a EMDAGRO (Empresa de Desenvolvimento Agropecuário de Sergipe), vinculada à Secretaria do Estado da Agricultura, Desenvolvimento Agrário e Pesca (SEAGRI). A empresa foi escolhida como ambiente de pesquisa em virtude da elevada faixa etária média de seus trabalhadores: 70%

deles são idosos. Outro fator para a escolha da organização é a participação do autor como integrante do núcleo de informática da empresa, sendo responsável pelo atendimento e administração dos recursos tecnológicos do órgão.

O objetivo da pesquisa em tela foi escolhido, inicialmente, pela ausência de estudos que possam contribuir acadêmica e profissionalmente ao tema. Observa-se também a existência de interesse social por melhores práticas de gestão de dados e informações, bem como a entrada em vigor da LGPD (lei geral de proteção de dados). Pesquisas que lancem luz sobre questões relacionadas à relação dos idosos com a SI podem fornecer conhecimentos oportunos à sua maior inclusão tecnológica, favorecendo a inserção e permanência no mercado de trabalho e a qualidade de vida dessas pessoas (Felix, 2016; FBI, 2023).

No tocante à estrutura do estudo, será exposto inicialmente seu referencial teórico, seguido de seus procedimentos metodológicos, da análise dos resultados inferidos e, por último, suas considerações finais.

## 2 REFERENCIAL TEÓRICO

### 2.1 Segurança da Informação e seus objetivos

A Segurança da Informação 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 (ISO, 2022). É descrita ainda como instrumento que auxilia na maximização do retorno sobre investimentos e de oportunidades para as organizações, por contribuir para a redução de paradas operacionais e prejuízos de reputação. Para Rao e Nayak (2014), é área multidisciplinar de estudo e atividade profissional, ocupada em desenvolver e implementar contramedidas de segurança para manter dados e sistemas de informação livres de ameaças.

Nesse ínterim, faz-se importante expor as definições de risco e ameaça, conceitos importantes à compreensão da problemática relacionada à segurança da informação (CSIRO, 2018):

- **Ameaça**: possível invasor ou malware (software nocivo) que deseja e/ou é capaz de causar danos a um alvo;
- **Risco**: potencial que uma ameaça possui de explorar uma vulnerabilidade de segurança;
- **Vulnerabilidade**: fraqueza em um dispositivo, sistema ou rede que pode ser explorada por ameaças maliciosas.

Ainda, Whitman e Mattord (2017) descrevem a SI como processo contínuo que envolve a interdependência dos componentes de sistemas de informação em organizações, a saber: pessoas, tecnologias, políticas e processos. Para Kamariza (2017), em um ambiente corporativo, a gestão desses componentes busca a mitigação de riscos e o bloqueio a ameaças às características da informação, também chamadas de objetivos da SI.

Segundo Cherdantseva e Hilton (2013), a tríade “CID” (confidencialidade, integridade e disponibilidade) compõe a base do modelo conceitual das características da informação desde a década de 1970, quando foi mencionada pela primeira vez por Saltzer e Schroeder (1975). Desde então, o modelo vem sendo debatido e incrementado, incorporando outras características da informação, a exemplo da autenticidade, responsabilidade, privacidade e do não-repúdio. O Quadro 1 expõe definições das características mencionadas.

**Quadro 1** – Características da SI e suas relações com os componentes de sistemas de informação

| **Característica/Objetivo da informação** | **Definição** |
|---|---|
| Responsabilização | Capacidade de responsabilizar usuários por suas ações |
| Autenticidade | Capacidade de verificar a identidade e estabelecer confiança em terceiros e na informação fornecida |
| Disponibilidade | Asseguração de que todos os componentes do sistema estão disponíveis e operacionais quando requeridos por usuários |
| Confidencialidade | Asseguração de que apenas usuários autorizados acessam a informação |
| Integridade | Asseguração da completude e ausência de modificações não autorizadas de todos os componentes do sistema |
| Privacidade | Capacidade de habilitar usuários a exercerem controle sobre suas informações pessoais |
| Não-repúdio | Possibilidade de um sistema de provar a ocorrência/não ocorrência de um evento ou a participação/não participação de uma parte em um evento |

Fonte: Elaborado pelos autores (2023) com base em Cherdantseva e Hilton (2013)

Dito isto, são descritas pela literatura práticas que buscam a manutenção dessas características em ambientes organizacionais. Para Whitman e Mattord (2017), são exemplos dessas práticas:A verificação da instalação, atualização e funcionamento de software antivírus nos dispositivos que utilizam no ambiente de rede da organização;

- Utilização de senhas intransferíveis, diferentes e complexas para cada serviço, a exemplo de contas de e-mail, redes sociais, bancos, e portais 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.

Autores Masuch *et al*. (2021) e FBI (2023), observam no corrente contexto de aumento na frequência de incidentes de segurança, o crescimento da atenção da sociedade à gestão de dados pelas organizações e a aprovação da LGPD (Lei Geral de Proteção de Dados) em 2020, requerem que os gestores estejam atentos a medidas de proteção aos ambientes de rede corporativos. Nesse sentido, são citados como boas práticas (Whitman; Mattord, 2017; Masuch *et al*., 2021):

- 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;

- Gestores dando exemplo pela utilização segura de dispositivos e sistemas no ambiente da organização;
- A definição de políticas de fácil compreensão para usuários de qualquer nível técnico, especialmente quando relacionadas à utilização de dispositivos. 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.

Nesse ínterim, Banerjee *et al*. (2013) consideram que medidas tomadas por gestores que visem educar usuários e proteger o ambiente corporativo de riscos e ameaças em SI contribuem ao desenvolvimento de um estado de consciência em segurança da informação. Embora não haja consenso no que se refere ao conceito e às dimensões que compõem a CSI, Haeussinger (2017) avaliou 131 artigos, e 21 definições distintivas sobre o tema foram encontradas. Observa-se que existe uma grande variedade de definições da CSI, e que diversos autores não definem claramente os limites das dimensões. Entretando, a codificação dos estudos realizada por Haeussinger (2017) resultou em três principais dimensões, ou aspectos: cognitivos, comportamentais e de processos.

Em virtude da limitação de extensão desse artigo, será feita mediante o Quadro 2 a caracterização de cinco definições explícitas da CSI, que exemplificam as dimensões/aspectos e descrevem os critérios de associação a que cada definição se refere. Busca-se, dessa maneira, auxiliar na diferenciação teórica e prática entre os conceitos das dimensões da CSI.

**Quadro 2** - Definições da conscientização em SI

| **Autor** | **Definição explícita** | **Dimensões/ aspectos da CSI** | | | **Critério de associação** |
|---|---|---|---|---|---|
| | | **Cognitivos** | **Comportamentais** | **Processos** | |
| Bulgurcu *et al*. (2010) | "Conscientização que os usuários possuem sobre riscos e ameaças em SI, e procedimentos necessidade de proteger informações pessoais sensíveis" | **x** | | | Cognitivos: possessão de conhecimentos técnicos por parte dos usuários, inclusive acerca de políticas organizacionais relacionadas à SI. |
| Banerjee *et al*. (2013) | "Conscientização em segurança pode ser definido como o conhecimento e comportamento que membros de uma organização possuem acerca da proteção dos ativos de informação na organização" | **x** | **x** | | Cognitivos: possessão de conhecimentos técnicos por parte dos usuários<br>Comportamentais: exercício de um comportamento de proteção à informação no ambiente da organização |

| | | | | | |
|---|---|---|---|---|---|
| Haeussinger (2017) | "Estado mental caracterizado pelo reconhecimento e compreensão de riscos e ameaças à segurança da informação. Possuir conhecimentos necessários para utilizar sistemas de informação de maneira responsável. Construção de CSI por parte de treinamentos por parte da organização" | **x** | | **x** | Cognitivos: possessão de conhecimento técnico por parte do usuário<br>Processos: desenvolvimento programas pela organização de conscientização de usuários |
| ISO (2022) | "Programas de conscientização em SI buscam focar atenção em transmissão de conhecimento em segurança, permitindo que usuários reconheçam ameaças em segurança da informação e respondam adequadamente, exercendo comportamento ativo na proteção à informação na organização" | **x** | **x** | **x** | Associação a todas as dimensões:<br>Cognitivos: conhecimentos técnicos por parte dos usuários<br>Comportamentais: menção ao exercício de um comportamento de proteção à informação no ambiente da organização<br>Processos: menção ao desenvolvimento programas pela organização de conscientização de usuários |
| Spurling (1995) | "Quando falamos em promover a conscientização sobre segurança de computadores e construir compromisso com a segurança de computadores, tendemos a pensar em campanhas de conscientização, publicidade, vídeos, cartazes, adesivos, folhetos etc. Todas essas coisas são importantes e têm seu lugar na promoção da conscientização, mas na realidade são apenas parte do processo como um todo" | | | **x** | Processos: menção ao desenvolvimento programas pela organização de conscientização de usuários |

Fonte: Elaborado pelos autores (2023) com base em Haeussinger (2017)

Segundo Haeussinger (2017), a CSI nesse contexto é definida como um estado mental do usuário, caracterizado pelo reconhecimento de riscos e ameaças à SI, bem pela ciência de práticas recomendadas para evitá-los. Nesse sentido, a dimensão cognitiva caracteriza-se pela possessão de conhecimentos que auxiliem o indivíduo a utilizar dispositivos e sistemas de informação de maneira segura, de acordo com as boas práticas de proteção dos dados e informações.

As definições da CSI também dizem respeito ao exercício pelo usuário de um comportamento de observância à SI. Compreende a tomada de ações de resposta ou prevenção a ameaças em segurança da informação, de acordo com boas práticas e regras definidas pela organização (ISO, 2022). Tal definição corrobora Frik *et al*. (2019), que mencionam o cumprimento de recomendações da organização como pré-requisito a uma atitude consciente em relação à SI.

Como já mencionado, percebe-se estreita relação entre os aspectos cognitivos e comportamentais da CSI, com a necessidade da obtenção de conhecimentos para que sejam percebidas ameaças em SI, e se exerça um comportamento seguro no uso dos dispositivos digitais de acordo com as boas práticas. Logo, verifica-se que não existem definições da CSI que abordam apenas aspectos comportamentais, sem contemplar aspectos cognitivos do usuário (Haeussinger, 2017).

O terceiro e último aspecto é composto por processos desenvolvidos pela organização para construir a conscientização nos empregados. Em outras palavras, referem-se a medidas

que a organização conduz para fazer com que seus empregados utilizem dispositivos e serviços digitais de maneira segura e comprometida com seus objetivos, também mencionada por Haeussinger (2017). Exemplos dessas medidas são: investimentos em treinamentos dos empregados, definição de políticas e procedimentos de segurança e campanhas de conscientização (FBI, 2023).

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

## 3 METODOLOGIA

A investigação em tela apresenta traços descritivos, pois buscou expor características de uma determinada população e proporcionar a obtenção de conhecimentos aprofundados sobre sua percepção acerca de um fenômeno ou de sua realidade. A pesquisa assumiu ainda características exploratórias, em virtude de sua intenção de investigar um tema pouco aprofundado, de reduzido conhecimento sistematizado (Haeussinger, 2017; ISO, 2022).

Os objetivos da pesquisa foram abordados de maneira qualitativa, pois buscam compreender aspectos da percepção dos participantes em relação à conscientização em segurança da informação, com o objetivo de lançar luz a fatores de afastamento a boas práticas de SI no ambiente organizacional (Liebscher, 1998). Considera-se adequado, desse modo, o uso de um método qualitativo em face do paradigma interpretativista da pesquisa em tela, pois essa é motivada pelo interesse em se buscarem informações profundas acerca da relação dos empregados idosos da organização estudada com a segurança da informação.

Em relação à estratégia de pesquisa, foi escolhido o estudo de caso único, buscando investigar características da percepção de idosos da organização pesquisada acerca da segurança da informação (Yin, 2019). No contexto do estudo executado, os critérios escolhidos para a estratégia de pesquisa foram os seguintes:

- A organização na qual a pesquisa foi empreendida possui um número elevado de idosos em relação ao total de empregados (70% da força de trabalho da empresa);
- Idosos da organização apresentam dificuldades na utilização de tecnologias digitais, gerando incidentes de segurança e constantes demandas à equipe de suporte em informática;

No cenário da organização estudada foram escolhidos participantes com base em princípios de homogeneidade fundamental, considerando-se relevantes os fatores faixa etária (ao menos 60 anos de idade) e utilizarem dispositivos digitais fornecidos pela organização. Adicionalmente, buscou-se incluir gestores no grupo de participantes, intencionando diversificação. Nesse ínterim, 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. O Quadro 3 apresenta características dos empregados escolhidos.

**Quadro 3** – 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 | 60 | 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 pelos autores (2023)

A coleta de dados se deu, inicialmente, mediante entrevistas qualitativas orientadas por roteiros semiestruturados. O roteiro foi elaborado com base nas categorias de análise criadas de acordo com as dimensões da CSI, e estão expostas no Quadro 4.

**Quadro 4** – Sistemas de categorias pré-definidas para a pesquisa

| **SISTEMA: Conscientização em SI** | | | |
|---|---|---|---|
| **Categoria** | **Descrição** | **Questão de pesquisa** | **Elementos de análise** |
| COG (Cognitivos) | Descreve capacidade técnica de reconhecer e riscos e ameaças à SI. | Qual a percepção dos idosos acerca dos aspectos cognitivos da conscientização em segurança da informação? | - Conhecimento técnico sobre ameaças e seus respectivos riscos;<br>- Conhecimentos acerca de práticas de mitigação de riscos; |
| COM (Comportamentais) | Descreve o exercício de comportamento observado e declarado de observância à segurança da informação organizacional dos participantes. | Qual a percepção dos idosos acerca dos aspectos comportamentais da conscientização em segurança da informação? | - Preocupação com possíveis danos à organização;<br>- Busca por informações quando deparados com situações de risco;<br>- Comprometimento prático 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 idosos acerca dos aspectos de processos da conscientização em segurança da informação? | - Percepção acerca de processos que fomentem a SI na organização.<br>- Sugestões de criação/melhoria de processos à organização. |

Fonte: Elaborado pelos autores (2023)

Os indivíduos foram contactados pessoalmente, de maneira individual, entre os meses de dezembro de 2022 a março de 2023 nas próprias instalações da organização. O tempo de duração das entrevistas variou entre 55 e 25 minutos. Os encontros começaram com a exposição dos objetivos da pesquisa, seguida da declaração de que a gestão da organização não estava envolvida no projeto. Assim que as conversas eram realizadas eram finalizadas, foram transcritas, salvas em formato eletrônico .docx 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 as transcrições aos entrevistados, tanto para possível complementação de informações como para a confirmação de autenticidade/rejeição de interpretações realizadas pelo pesquisador.

Uma vez angariados os dados, transcritas as entrevistas e desenvolvidos os relatórios de observação do ambiente da organização, foi empreendida uma análise desses dados com o objetivo de transformá-los de um estado bruto em formatos apropriados. Escolheu-se a combinação de técnicas de análise de dados, baseadas em análise de conteúdo e confrontados os dados angariados pelas entrevistas com o exposto pela literatura.

Ao final do capítulo de análise, os dados dos participantes foram agrupados de acordo com sua aproximação às boas práticas em SI, procedimento adotado para dar destaque a fatores de diferenciação entre as percepções dos grupos. Os agrupamentos estão expostos no Quadro 5, sendo que os participantes com frequência de adesão a práticas recomendadas em segurança igual ou maior que 50% foram inseridos entre os mais conscientes. Foram também desenvolvidos mapas mentais de cada grupo, com o intuito de expor graficamente as diferenças nas percepções dos grupos sobre cada dimensão da CSI.

Foram delineados dois mapas por dimensão da CSI: um referente ao grupo de usuários com maior grau de conscientização, denominado Grupo 01, e outro que diz respeito aos idosos que apresentam menor grau de conscientização, chamado de Grupo 02. O procedimento foi adotado com o objetivo de auxiliar na visualização da percepção dos entrevistados e destacar possíveis distinções entre os grupos.

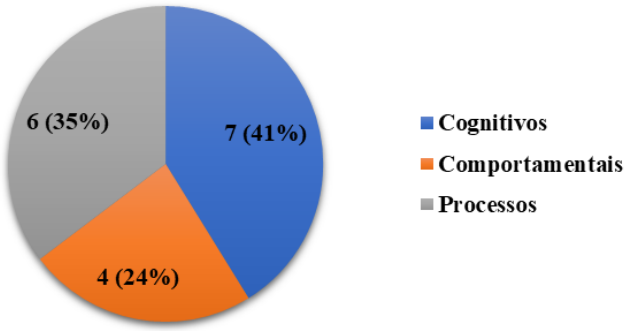
Segundo Buzan (2019), mapas mentais são ferramentas que ajudam a organizar ideias. Para o autor, mapas mentais agrupam e concatenam palavras e ideias relacionadas, ramificadas hierarquicamente a partir de uma ideia central, maior, que usualmente está centralizada. Logo, os mapas mentais foram utilizados no estudo a partir da centralização dos aspectos mencionados pelos entrevistados, inseridos como ideias concatenadas à dimensão referida. Buscou-se, assim, sintetizar graficamente a percepção dos idosos da empresa sobre as dimensões da CSI.

Finalizada a descrição dos procedimentos metodológicos, a discussão dos resultados será exposta na sequência.

## 4 RESULTADOS E DISCUSSÃO

A pesquisa buscou, por meio da investigação da percepção dos usuários idosos em relação às dimensões da conscientização em segurança da informação, conhecer fatores de afastamento dessas pessoas às boas práticas em SI. Nesse ínterim, foram mencionados pelos participantes 17 fatores relacionados à proteção à informação no ambiente organizacional, distribuídos dentre as 3 dimensões componentes da conscientização em segurança da informação: cognitivos, comportamentais e de processos. A distribuição dos aspectos em cada dimensão pode ser visualizada no Gráfico 1.

**Gráfico 1** - Distribuição de aspectos mencionados nas dimensões da CSI




Fonte: Dados da pesquisa (2023)

Dito isto, as frequências de menções de percepções tecnicamente adequadas, ou que expressem um comportamento voltado a práticas seguras podem ser observadas no Quadro 5.

**Quadro 5** – Contagem e frequência de menções a percepções tecnicamente adequadas/comportamentos seguros à organização entre os 17 aspectos citados

| Idosos com maior grau de CSI (Grupo 01) | Idosos 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 principais dados e mapas mentais desenvolvidos a partir da análise das citações feitas pelos grupos, organizados de acordo com os 17 aspectos mencionados nas entrevistas. Vale ressaltar que, durante a análise, a distribuição dos participantes nos grupos foi homogênea nas três dimensões investigadas. Ou seja, os entrevistados E1, E3 e E4 demonstraram maior aproximação em todas as dimensões da CSI estudadas. Parte-se, então, à apresentação dos dados e mapas mentais referentes aos aspectos cognitivos dos participantes.

### 4.1 Dados e mapas mentais relacionados a aspectos cognitivos

As três primeiras questões do roteiro de entrevistas foram definidas com objetivo de compreender a percepção do entrevistado acerca de sua consciência dos riscos aos quais estão sujeitos, e que práticas de proteção à informação consideram ser possíveis para mitigá-los. O Quadro 6 expõe os aspectos relacionados à dimensão cognitiva mencionados, juntamente com suas frequências de citações e proporções de menções espontâneas.

**Quadro 6** – Dimensão aspectos cognitivos, fatores mencionados e respectivas frequências de citações

| Dimensão | Nome | 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%) |
| | *Backups* | 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)

Percebe-se que os aspectos cognitivos mais citados pelos participantes foram *backups*, seguidos do gerenciamento de senhas e da ação de criminosos que atuam na internet/antivírus. A definição conceitual dos aspectos e os respectivos autores mais recorridos em cada aspecto serão apresentados no Quadro 7.

**Quadro 7** – Definições gerais dos aspectos cognitivos

| Aspecto cognitivo | Definição | Base teórica |
|---|---|---|
| Bloqueio do computador ao sair da estação de trabalho | Participante menciona a importância de se evitar deixar o computador desbloqueado, evitando acessos indevidos com suas credenciais. | Hadnagy (2018) |

| | | |
|---|---|---|
| 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. | Prabowo *et al*. (2017) |
| *Backups* | Entrevistado acredita que *backups* são importantes para evitar perda de dados. | FBI (2023) |
| 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. | ISO (2022) |
| 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 deles. | Frik *et al*. (2019) |

Fonte: Dados da pesquisa (2023)

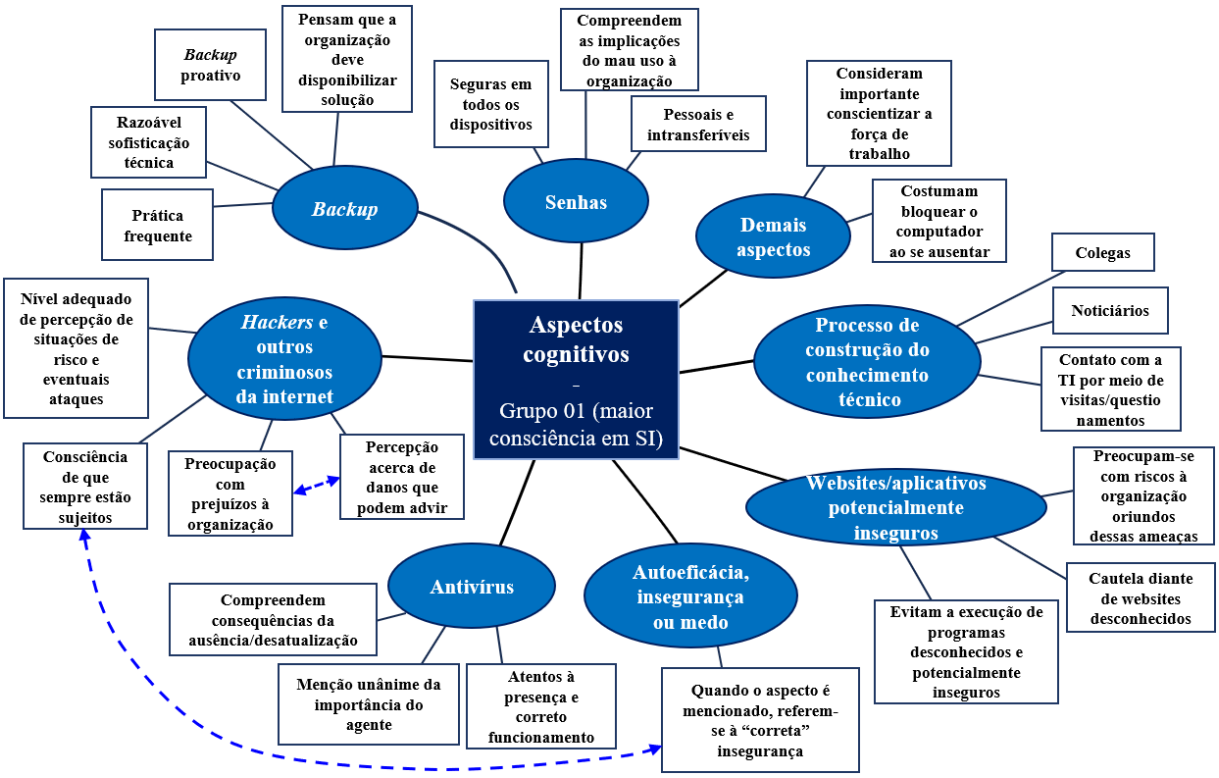
Prosseguindo a análise, observou-se que há significativa diferença entre os grupos definidos. Entrevistados do Grupo 01 apresentaram respostas às questões com maior segurança e espontaneidade, trazendo informações técnicas referentes aos aspectos citados. Embora alguns detalhes importantes da proteção 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. Dito isto, a Figura 1 apresenta o modelo mental do Grupo 01.

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.

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, podendo-se observar a ligação no modelo mental entre os dois aspectos citados. Apresentam-se assim pelo Grupo 01 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*.

**Figura 1** – Mapa mental de aspectos cognitivos do Grupo 01

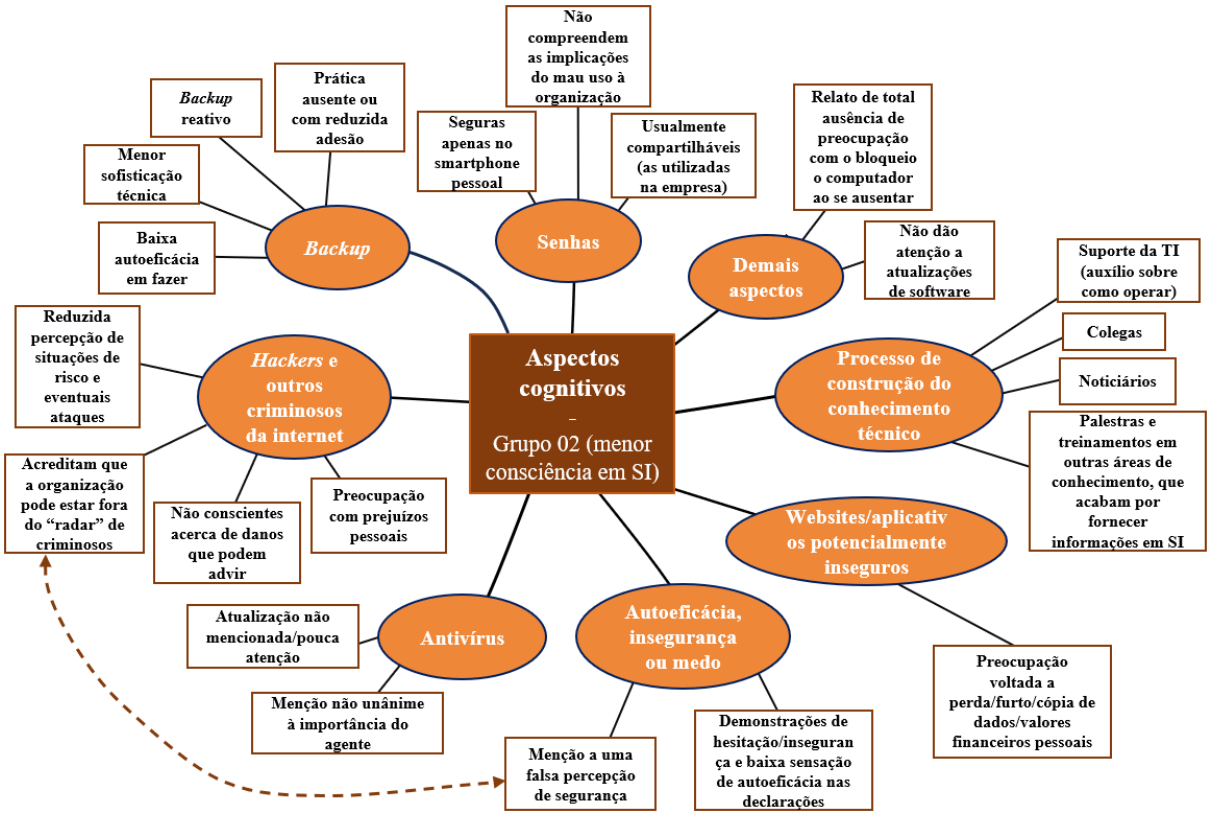



Fonte: Elaborado pelos autores (2023)

Adicionalmente, o Grupo 01 mantém contato constante com a equipe de TI da organização, seja por prévias experiências profissionais no setor (E1), como pela frequente presença no local que os técnicos exercem suas funções (E3). 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 2 apresenta o modelo mental referente aos aspectos cognitivos mencionados pelas participantes E2, E5, E6 e E7.

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.

**Figura 2** - Mapa mental de aspectos cognitivos do Grupo 02




Fonte: Elaborado pelos autores (2023)

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 (pelo seu compartilhamento 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). 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 e*t 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. 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.

### 4.2 Dados e mapas mentais relacionados a aspectos comportamentais

Os dados relacionados a essa dimensão foram obtidos principalmente por meio das questões 04, 05 e 06 do roteiro de entrevistas, buscando conhecer a percepção dos usuários

acerca de seu comportamento de proteção à informação. A discussão é assim iniciada com a exposição dos aspectos comportamentais citados, que podem ser visualizados no Quadro 8.

**Quadro 8** – Aspectos comportamentais, seus fatores mencionados e respectivas frequências de citações

| Dimensão | Nome | 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)

Podem ser assim visualizados os aspectos relacionados ao comportamento de proteção à informação mencionados, juntamente com suas respectivas quantidades e proporções de citações espontâneas. Já o Quadro 9, exposto a seguir, apresenta as definições de cada aspecto citado e suas respectivas bases teóricas.

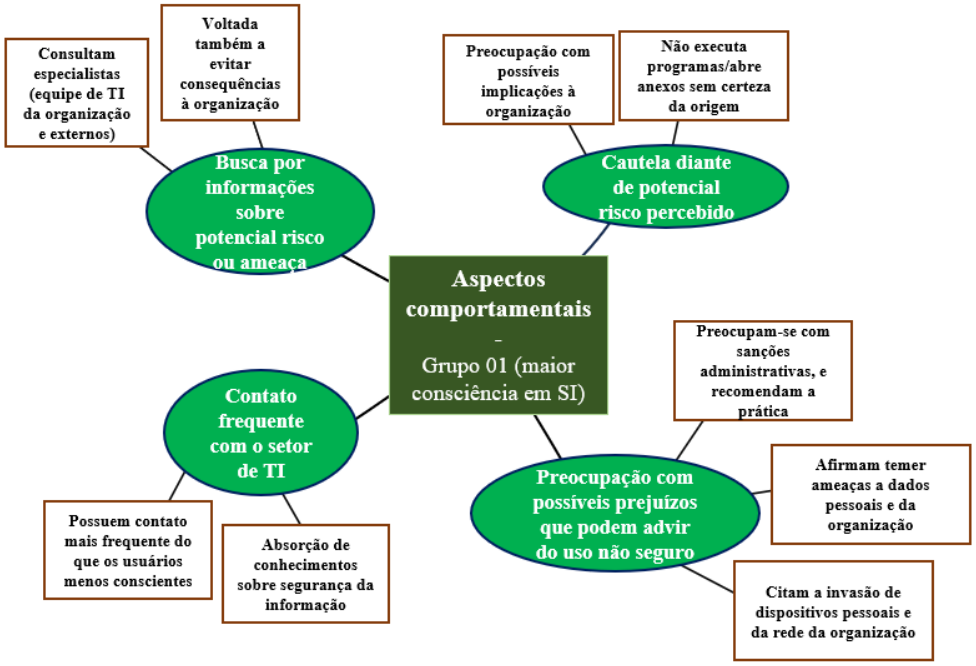
**Quadro 9** – Definições gerais dos fatores citados pelos entrevistados que se relacionam a aspectos comportamentais

| Aspecto comportamental | Definição | Base teórica |
|---|---|---|
| Cautela diante de risco percebido | Usuário(a) declara ser cauteloso(a) em face de uma situação de risco percebido | Hadnagy (2018) |
| 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 e Dorey (2016) |

Fonte: Dados da pesquisa (2023)

Uma vez apresentados os fatores e suas respectivas definições, parte-se à análise das menções dos grupos de entrevistados. Os aspectos comportamentais mencionados pelo Grupo 01 tendem a expor um maior comprometimento na contribuição aos objetivos da segurança da informação na organização. A Figura 3 expõe o mapa mental desenvolvido a partir dos relatos dos participantes desse grupo.

**Figura 3** – Mapa mental de aspectos cognitivos do Grupo 01




Fonte: Elaborado pelos autores (2023)

Assim como observado nos aspectos cognitivos, os participantes mencionam estar atentos e preocupados com 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 do Grupo 01 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.

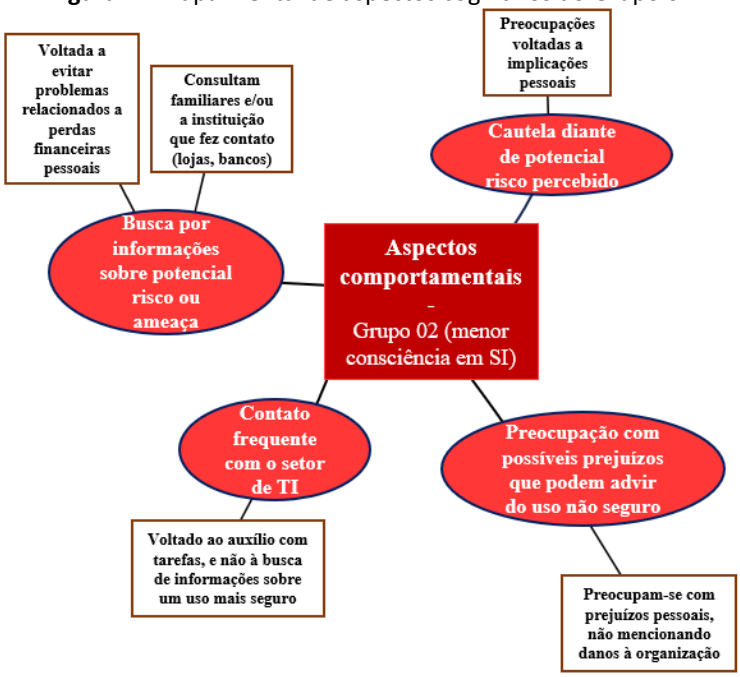
Adicionalmente, é mencionada a prática de contato constante com os especialistas em TI da empresa, o que os permite adquirir conhecimentos sobre segurança da informação, seja diante de situações de possível risco quanto para solicitar o ajuste de agentes de segurança.

No que se refere aos idosos com menor grau de consciência em SI, ou Grupo 02, suas percepções acerca de aspectos comportamentais são direcionadas a consequências e prejuízos de ordem pessoal, não estando necessariamente comprometidos com os objetivos da segurança da informação da organização. Esse cenário pode ser observado na Figura 4.

Observa-se que apesar de os entrevistados do Grupo 02 demonstrarem preocupação com as ameaças que estejam sujeitos, seu comportamento de evitar prejuízos é voltado principalmente a perdas financeiras e ao acesso a fotos e senhas em dispositivos pessoais. A despeito 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).

**Figura 4** - Mapa mental de aspectos cognitivos do Grupo 02




Fonte: Elaborado pelos autores (2023)

Outra característica percebida no Grupo 02 é que o contato com a equipe de especialistas em TI da organização é voltado ao auxílio sobre na operação básica dos dispositivos. 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 num website, por exemplo. Algumas situações que ocorreram com esses participantes foram mencionadas ao longo do estudo, como e-mails de varejistas conhecidos ou bancos.

Apesar de ser tecnicamente recomendado buscar instituições oficiais para sanar dúvidas relacionadas a possíveis fraudes, a consulta à equipe de TI é considerada boa prática, 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. O desconhecimento de alguns participantes de áreas de *backup* disponibilizadas pela TI observado durante a pesquisa exemplifica essa situação.

### 4.3 Dados e mapas mentais relacionados a aspectos de processos.

Parte-se, então, à exposição de aspectos relacionados a processos percebidos e citados pelos participantes, que dizem respeito a procedimentos realizados pela organização para desenvolver a CSI em empregados. Os principais aspectos mencionados podem ser visualizados no Quadro 10.

**Quadro 10** – Dimensão aspectos de processos, fatores que foram percebidos pelos participantes e suas respectivas frequências de citação

| Dimensão | Nome | 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)

Além dos aspectos relacionados ao comportamento de proteção à informação mencionados pelos participantes, visualizam-se no Quadro 11 suas definições e respectivas bases teóricas.

**Quadro 11** - Definições gerais dos aspectos citados pelos entrevistados que se relacionam a processos

| 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. | Green, Dorey (2016) |
| 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. | Green; Dorey (2016) |
| 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 de processos citados e suas definições, expõem-se na sequência os mapas mentais dos grupos de entrevistados relacionados aos 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 5.

**Figura 5** - Mapa mental de aspectos de processos do Grupo 01


Fonte: Elaborado pelos autores (2023)

Os participantes E1, E3 e E4 mencionaram 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 ausência de investimentos em tecnologias de *backup* com uma deficiente comunicação da gestão com os empregados por eles percebida, 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; Mayak, 2014).

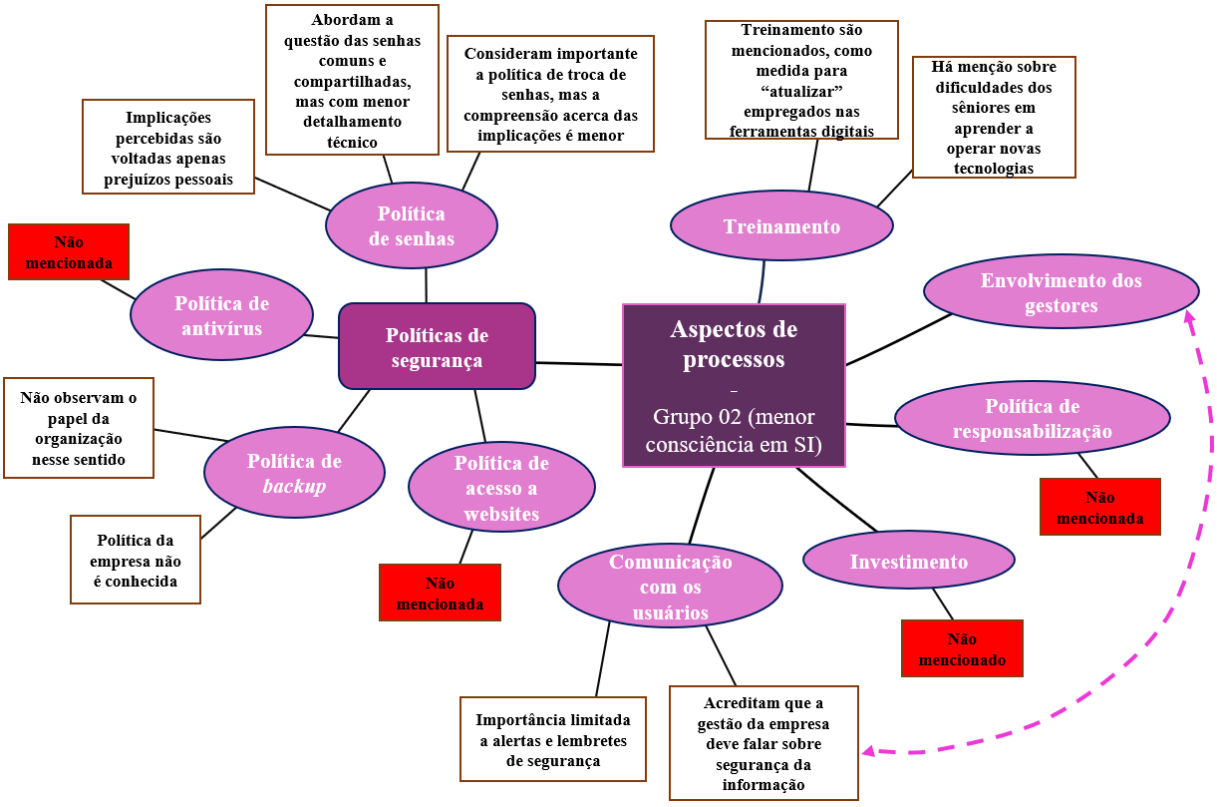
Além disso, os integrantes do Grupo 01 afirmam considerar importante que uma política de cobrança à adesão à utilização sistemas digitais pela força de trabalho idoso da empresa seja conduzida, pois observam a subutilização de sistemas disponíveis, a exemplo do protocolo eletrônico (E-DOC). Compreendem, 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 de dispositivos digitais 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 treinamento. 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). Os entrevistados do Grupo 02 mencionaram o aspecto, representado pela declaração de E2 como prática ausente na organização.

Adicionalmente, os integrantes do Grupo 01 declaram ter uma percepção voltada à adoção de recursos tecnológicos, e 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 é reduzida. Esse cenário pode ser observado na Figura 6, exposta na sequência.

**Figura 6** - Mapa mental de aspectos de processos do Grupo 02




Fonte: Elaborado pelos autores (2023)

Todavia, cabe trazer à discussão que os participantes dos grupos dos menos conscientes, apesar de demonstrarem possuir menor compreensão acerca da existência ou das implicações de não se seguirem políticas de segurança estabelecidas, consideram importantes as diretrizes definidas no que se refere, pelo menos, à política de senhas. Abordam, inclusive a questão da utilização de uma senha comuns em diversos computadores da empresa, mesmo que com menor detalhamento técnico do que o demonstrado pelos integrantes do Grupo 01.

Em relação às demais políticas, como a 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 o mencionado pelo Grupo 01, que também acredita que a gestão da empresa deve ser mais ativa no exemplo de utilizar dispositivos seguindo as 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 também à discussão a percepção desses participantes ao aspecto do treinamento, por eles considerado importante para atualizar os empregados idosos às novas tecnologias, conforme mencionado por E7, 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 idosos em treinamentos. O relato da entrevistada corrobora o cenário de desinteresse causado pela sensação de baixa autoeficácia observada em idosos da organização, que por vezes expressam desinteresse em tecnologias digitais.

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 Llorente-Barroso *et al*. (2018), que afirmam que o interesse do usuário idoso 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 a 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, como políticas de antivírus e controle de acesso a websites, investimentos e responsabilização em caso de mau uso.

Assim, a busca pela resposta ao objetivo da pesquisa iniciou-se pela investigação acerca das dimensões componentes da conscientização em segurança da informação. O atendimento a tal objetivo foi permeado pelo entendimento de que o recorte social dos idosos, inseridos no ambiente organizacional estudado, apresentou dois grupos de percepções distintas: o primeiro, constituído por 03 dos 07 participantes, mostrou-se mais consciente quanto a riscos e ameaças que permeiam o uso de dispositivos digitais, além de possuir mais conhecimentos técnicos necessários para evitá-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, uma 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 idosos (Grupo 02), que demonstrou menor consciência em relação às dimensões da CSI. Sinaliza-se assim que mais da metade dos participantes da pesquisa apresentam conhecimentos, comportamentos e percepções acerca de processos conduzidos pela empresa apartados às boas práticas de proteção à informação, com reduzido comprometimento com os objetivos de SI da organização.

Em face do exposto, os seguintes fatores de afastamento dos participantes às melhores práticas em SI foram observados:

- O limitado contato com os especialistas de TI da empresa, que tende a proporcionar um maior intercâmbio de conhecimentos técnicos aderentes às melhores práticas em segurança da informação;
- 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.

## 5 CONSIDERAÇÕES FINAIS

No que se refere a limitações observadas durante o estudo, pode-se mencionar a limitação temporal, que não tornou possível a criação de mapas mentais individuais dos participantes, o que proporcionaria uma análise mais detalhada de como percebem os idosos da organização as dimensões e aspectos da CSI. As restrições também tangem à condução de um estudo que se baseia em declarações de participantes de um grupo de pessoas de uma única organização. 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. Tal limitação é aspecto observado por diversos autores que conduzem estudos que utilizam técnicas semelhantes de coletas de dados.

Por fim, sugere-se que a nível de pesquisas futuras, seriam oportunos à área acadêmica da Administração e gestão de empresas estudos voltados à compreensão de fatores de estímulo a empregados idosos, voltados à qualificação e comprometimento a políticas de segurança à informação em organizações. Adicionalmente, 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 privadas, avaliando possíveis diferenças nas percepções dos idosos nesses ambientes, sobretudo em aspectos comportamentais e de processos.

## REFERÊNCIAS

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.

BANERJEE, C; BANERJEE, A; MURARKA, P. An Improvised Software Security Awareness Model. **International Journal of Information, Communication and Computing Technology**, [*s. l.*], v. 1, ed. 2, p. 43-48, 2013.

BULGURCU, B *et al*. INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. **MIS Quarterly**, [*s. l.*], v. 34, ed. 3, p. 523-548, setembro 2010. Disponível em: http://130.18.86.27/faculty/warkentin/BIS9613papers/MISQ_SpecialIssue/BulgurcuCavusogluBenbasat2010_MISQ34_RationalityAwareness.pdf. Acesso em: 6 nov. 2024.

BUZAN, T. **Mapas mentais.** Rio de Janeiro, RJ: Sextante, 2009.

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.

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.

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, A; CAMARANO, A; GIACOMIN, K. **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.

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

GREEN, J.; DOREY, P. **The Weakest Link**, 1. 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. 2017. 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.

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.

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.

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.

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.

OMS. Organização Mundial da Saúde. **Ageing**. [S. l.], 2024. Disponível em: https://www.who.int/health-topics/ageing#tab=tab_1. Acesso em: 27 nov. 2024.

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

SALTZER, J.; SCHROEDER, M. **The protection of information in computer systems**. Proceedings of the IEEE 63(9), pp. 1278-1308, 1975.

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.

SPURLING, P. Promoting Security Awareness and Commitment. **Information Management and Computer Security**, Vol. 3, No. 2, pp. 20–26. 1995)

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.

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

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

Recebido em/Received: 20/03/2024 | Aprovado em/Approved: 30/11/2024

## APÊNDICE A - Roteiro de entrevistas

**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?