RMP Revista dos Mestrados Profissionais – RMP
HTTPS://PERIODICOS.UFPE.BR/REVISTAS/RMP
ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

# SEGURANÇA DA INFORMAÇÃO ORGANIZACIONAL E SÊNIORES: ASPECTOS PARA MITIGAÇÃO DE RISCOS

Filipe Valença e Silva – filipevalenca.ti@gmail.com[1]
Jefferson David de Araújo Sales – profsales@hotmail.com[1]
Alessandra Cabral Nogueira Lima - ale.cnogueira@gmail.com[1]

**Resumo** – A pesquisa teve o propósito de identificar fatores de risco à segurança da informação (SI) oriundos de hábitos e características de empregados de idade avançada em organizações, uma vez que os pilares da SI confidencialidade, integridade e disponibilidade necessitam ser equilibrados. O trabalho de características quantitativas foi realizado na EMDAGRO-SE, organização que possui mais de 60% de seus empregados com idades acima de 55 anos. Os dados foram coletados por meio de questionário, consultas a registros internos da organização relacionados a incidentes de segurança da informação e através da estratégia da observação participante. Em seguida, dos dados foram tratados com estatística descritiva, e verificou-se que os usuários mais velhos da organização apresentaram comportamentos mais inseguros com maior frequência que os mais jovens, a exemplo de uma menor busca por conhecimento sobre SI, desconhecimento sobre *phishing*, reduzida utilização de *backup*, dificuldades no gerenciamento de senhas e menor prática na utilização de dispositivos conectados à internet.

**Palavras-chave:** Segurança da informação; Tecnologias digitais; Mitigação de riscos

# ORGANIZATIONAL INFORMATION SECURITY AND SENIORS: ASPECTS FOR RISK MITIGATION

**Abstract** – The research aimed to identify risk factors for information security (IS) arising from habits and characteristics of elderly employees in organizations, since the IS pillars confidentiality, integrity and availability need to be balanced. The quantitative characteristics work was carried out at EMDAGRO-SE, organization that has more than 60% of its employees aged over 55 years old. The data was collected through a questionnaire, consultations to the organization's internal records related to information security incidents and through the participant observation strategy. Thus, the data was treated by descriptive statistics, and was verified that the older users of the organization presented insecure behaviors more often than younger people, such as less frequent search for knowledge about IS, ignorance about phishing, reduced use of backup, difficulties in password management and less practice in the use of devices connected to the internet.

**Keywords:** Information security; Digital technologies; Risk mitigation

**Data da Submissão: 24/01/2021**

**Data de aceitação: 11/03/2021**

1 - Universidade Federal de Sergipe

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

## 1. Introdução

A crescente valorização da informação e do conhecimento estimulou a ubiquidade dos aparelhos digitais e o aumento da velocidade das redes de informação, acentuando o interesse da sociedade em temas como computação em nuvem, cidades inteligentes, telemedicina e a internet das coisas. Em outras palavras, a internet e os dispositivos digitais têm sido utilizados com finalidades e situações inéditas e em lugares onde não estavam disponíveis (AWAD; FAIRHUST, 2018).

Paralelamente a este fenômeno, grupos especializados baseados na internet ou infiltrados em organizações corporativas empenham-se em praticar ataques cibernéticos, que consistem em coletar informações não autorizadas ou provocar danos a dispositivos e estruturas de tecnologia da informação. Órgãos governamentais e o setor privado procuram evitar de diversas maneiras serem alvos e vítimas destes ataques. Todavia, apesar dos esforços, a frequência e a severidade desses crimes têm aumentado (NISC, 2017; MCAFEE, 2018).

De acordo com a McAfee (2018), fabricante de software de segurança cibernética, as perdas no ano de 2018 no mundo com esses crimes atingiu a casa dos 600 bilhões de dólares, o que representa aproximadamente 1% do PIB mundial. Tais prejuízos são oriundos de descontinuidades operacionais, ações legais iniciadas por consumidores prejudicados e danos estimados à reputação das marcas afetadas.

Green e Dorey (2016) inferem em seus estudos que a maioria das ameaças à segurança da informação (SI) nas organizações ocorre por conta da fragilidade do elo humano nessas cadeias, ou seja, os usuários que fazem uso dos recursos computacionais ou falhas por parte dos administradores destes ambientes. No intuito de explorar possíveis vulnerabilidades de ordem humana, técnicas cada vez mais sofisticadas baseadas em Engenharia Social têm sido utilizadas pelos criminosos para conseguir acesso não autorizado aos dados e às redes privadas de tecnologia da informação (TI) (GARDNER; THOMAS, 2014).

Nesse contexto, a defesa contra ameaças à SI tem exigido novos hábitos do usuário final e das empresas que utilizam e administram recursos tecnológicos digitais. Deter conhecimento acerca de métodos e técnicas utilizados pelos *hackers* faz-se importante para minimizar vulnerabilidades, pois a falta de conhecimento técnico sobre a maneira correta de se utilizar as ferramentas digitais e a ignorância acerca de possíveis riscos à segurança que um simples clique indevido representa têm sido o foco dos ataques cibernéticos (HADNAGY, 2018; SYMANTEC, 2018).

Dito isto, buscando maior sucesso em suas tentativas de ataque, *hackers* fazem dos usuários mais velhos alvos frequentes. Sobre esse cenário, a empresa Kaspersky (2017) afirmou que pessoas sêniores (com mais de 55 anos de idade) costumam ser alvos de armadilhas virtuais na internet, uma vez que costumam ter menos cuidados com a segurança no uso de ferramentas cibernéticas, são menos atentas aos riscos existentes no mundo virtual e confiam mais em desconhecidos do que as outras gerações. Adicionalmente, Dias (2012) considera que entre os sêniores são significativos o desfasamento de conhecimento técnico-científico acerca de novas tecnologias - especialmente as digitais - e a fragilidade de recursos físicos e cognitivos desse domínio de cidadãos.

Ademais, estima-se uma presença mais ativa dos sêniores no mercado de trabalho nas

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

próximas décadas. Esse cenário é apresentado pelo IBGE (Instituto Brasileiro de Geografia e Estatística) em estudo de 2019 acerca do envelhecimento da população brasileira, motivado pelo aumento da expectativa de vida nacional em conjunção com as novas regras de previdência no país (IBGE, 2019a; MENTLIK et al., 2019).

Sem embargo, o envelhecimento da força de trabalho constitui um desafio às organizações modernas no sentido de minimizar os impactos da constante evolução tecnológica com os aspectos do envelhecimento humano, que podem favorecer riscos à SI organizacional. Diante desta temática, o presente trabalho buscou analisar o cenário da relação dos empregados sêniores com a SI na Empresa de Desenvolvimento Agropecuário de Sergipe (EMDAGRO).

A pandemia do novo coronavírus, enfrentada especialmente a partir do ano de 2020, favoreceu a aceleração de um processo que já vinha se desenvolvendo globalmente: o regime remoto de trabalho, conhecido como *home office* ou teletrabalho. No Brasil, por exemplo, o IBGE divulgou em 2019 que houve um crescimento de 44% nessa modalidade de trabalho no país entre 2012 e 2018, e atualmente 7,9 milhões de brasileiros estão nesse regime funcional. Com efeito, adaptações tecnológicas se fazem necessárias para acompanhar essa nova realidade em organizações com forças de trabalho cada vez mais envelhecidas a adequar-se de maneira eficiente e segura a sistemas utilizados para ambientes virtuais de trabalho, como conexões via VPN (*Virtual Private Network*, ou Rede Virtual Privada) e plataformas públicas de videoconferência (IBGE, 2019b).

Criada em 1962, a EMDAGRO atua no apoio técnico aos produtores agrícolas e pecuaristas do estado de Sergipe. Possui uma força de trabalho de 568 colaboradores, sendo 465 servidores e 103 terceirizados e uma média de idade de 49 anos, superior à dos servidores públicos estaduais (46 anos). Seu último concurso público foi no ano de 2004 para o provimento de 15 vagas, e não há renovação prevista em seu cronograma. A empresa não conta com política de segurança da informação definida, nem investe em treinamentos técnicos em tecnologia para seus colaboradores (TRANSPARÊNCIA SERGIPE, 2019).

Em face do exposto até aqui, este estudo teve como objetivo geral identificar os fatores de risco à segurança da informação oriundos dos hábitos e características dos usuários de idade avançada na EMDAGRO. Adicionalmente, pretendeu-se com a pesquisa comparar o comportamento dos empregados mais velhos da organização com os dos mais jovens, no tocante ao grau de conformidade com a segurança da informação, buscar compreender as razões pelas quais as diferenças de percepção existem e sugerir melhorias na mitigação dos riscos de SI na organização estudada.

Os objetivos foram escolhidos devido à existência de estudos relacionados à interação com a tecnologia da informação mostrarem que os seniores apresentam características que se enquadram no escopo de vulnerabilidade, como os conduzidos pela Kaspersky (2017), pelo NISC (2017) e por Panda Security (2017). Assim, essa pesquisa visa uma contribuição no campo da ciência da administração e da SI, além de auxiliar organizações no desenvolvimento e ajuste de suas práticas e políticas de proteção à informação.

No tocante à estrutura do trabalho, será exposto inicialmente o referencial teórico que norteia a pesquisa, mencionando aspectos da segurança da informação e do envelhecimento humano. Na sequência, serão apresentadas a metodologia utilizada para a execução do estudo, a análise dos resultados inferidos e, por último, as conclusões da pesquisa.

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

## 2. Referencial teórico

Registros históricos revelam que a preocupação com segurança da informação é antiga na história da humanidade. Segundo França (2014), um dos relatos mais remotos sobre o tema revela que arquitetos egípcios na antiguidade já tomavam precauções no sentido de preservar informações sensíveis ao codificar características de suas famosas construções.

De acordo com a ABNT (2013) em sua norma ISO 27002:2005, nos tempos modernos a SI pode ser compreendida como "proteção à informação contra diversos tipos de ameaças", com o objetivo de minimizar riscos, evitar a descontinuidade do negócio e maximizar tanto o retorno sobre investimentos quanto as oportunidades para a organização. Já Hadnagy (2018) afirma ser possível definir a SI como área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou indisponibilidade.

Todavia, para que sejam alcançados os objetivos supracitados, faz-se mister a preservação de características da informação, especialmente os três pilares da SI, que são: Confiabilidade (prevenção contra o uso não autorizado da informação e à quebra de sigilo de dados), a Integridade (prevenção a alterações da informação e à modificação não autorizada de dados) e a Disponibilidade (prevenção da suspensão e lentidão no acesso à informação e serviços computacionais) (MAULAIS, 2016).

Ousley (2013), por sua vez, considera que quanto mais informação se tem sob o comando de uma organização, mais capacidade ela possui para se adaptar ao ambiente no qual está inserida. Castells (2005) menciona que além da informação ser, com frequência, um dos ativos mais valiosos que uma companhia pode ter, a informação pode diferenciar estrategicamente essa empresa das concorrentes, provendo lastro para um maior sucesso no mercado.

Para Lyra (2015) e Stewart *et al*. (2015) exemplos de ativos de informação a serem protegidos 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 (aplicativos, sistemas, ferramentas e bancos de dados), hardware (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.

Sem embargo, *hackers* e outros criminosos atuantes no mundo digital buscam apoderar-se desses ativos estratégicos, representando verdadeiras ameaças aos empregados, que podem ser responsabilizados administrativa e legalmente pela falha de segurança, e às organizações, vítimas potenciais de graves prejuízos (WHITMAN, 2017).

A nível de exemplo de materialização de ameaças a organizações, ataques cibernéticos massivos atingiram em 2011 a megacorporação Sony, líder mundial em vendas de videogames. *Hackers* invadiram seus sistemas, roubaram dados e ameaçaram vazar informações pessoais de milhões de clientes por vende-las a outros criminosos que atuam na internet. A Sony então decidiu, como medida de defesa para impedir maiores danos em face da invasão de seus sistemas, desativar por 30 dias o serviço PlayStation Network (PSN), rede de jogos do videogame mais vendido no mundo, utilizada à época por 77 milhões de usuários (BONNER, 2012).

Desdobramentos do caso levaram a companhia japonesa a ser processada em diversos

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

países, a exemplo do Reino Unido e dos Estados Unidos, pela falha de segurança e em razão da ameaça dos criminosos de tornar públicos os dados pessoais dos clientes, que se sentiram lesados com suas informações expostas na internet. Ainda segundo Bonner (2012), a Sony foi multada em milhões de dólares em consequência dos processos judiciais. Somando-se a esses gastos, houveram danos à imagem da empresa e o prejuízo estimado total com o ataque foi de 10 bilhões de dólares.

A ABNT (2013) afirma ainda que organizações e seus sistemas de informação e redes digitais estão expostas a diversos os perigos além de invasões de seus sistemas. Outros exemplos são fraudes eletrônicas, roubo de dados e informações, espionagem, chantagens, sabotagem, vandalismo, inundações, incêndios, entre outros. Alexandria (2009) cita a destruição das informações, redução de capacidade de operação, modificações não autorizadas ou corrupção dos dados e interrupção de serviços e sistemas, que usualmente culminam em prejuízos financeiros e de reputação.

Adicionalmente, o relatório *Global Information Security Survey* 2018-19 (ou Levantamento Global de Segurança da Informação 2018-19 [tradução nossa]) da firma de auditoria Ernst and Young (2018) afirma que ações humanas representam 92% das ameaças à segurança da informação das organizações. Ameaças de ordem humana podem ser involuntárias e intencionais, e ambas expõem dados e informações pessoais e corporativas e podem comprometer a SI no ambiente da organização.

Rao e Nayak (2014) exemplificam cenários vulneráveis à SI criados de maneira involuntária pelos empregados, como o envio de dados pessoais sensíveis respondendo a e-mails maliciosos ou páginas fraudulentas que simulam portais legítimos (técnica de *phishing*) e download e execução de *malware* disfarçado de programa legítimo em computadores corporativos. Há ainda empresas onde podem-se trazer dispositivos pessoais e conectá-los à rede interna da instituição, potencialmente infectando involuntariamente outros dispositivos da rede corporativa. O Quadro 1 expõe os principais motivos involuntários originários de comportamentos que podem causar falhas de SI.

Quadro 1 – Principais comportamentos involuntários potencialmente inseguros em SI.

| Origem da vulnerabilidade | Características |
|---|---|
| **Ignorância técnica** | Empregados que não sabem da importância da Segurança da Informação. Muitos empregados, incluindo gerentes, não dispõem de conhecimento técnico a respeito de *cibersegurança* e práticas de prevenção de riscos. Por vezes nem sabem que estão diante de uma situação perigosa ao se depararem com armadilhas digitais |
| **Pouca conscientização** | Gestores e empregados desconhecem ameaças, formas de contágio e consequências individuais e coletivas. Não disseminam informações sobre riscos à SI e nem sobre os potenciais problemas associados às ameaças. Ocorre também de acreditarem que a proteção à informação e eventuais falhas de segurança só cabem ao *staff* de tecnologia |

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

| | |
|---|---|
| **Excesso de autoconfiança** | Há companhias que estão cientes dos riscos à SI de suas empresas, porém consideram que estão com seus ambientes protegidos, tanto em ferramentas de defesa de seus ambientes como na conscientização de seus usuários |
| **Concepções incorretas acerca da origem dos riscos** | Empregados e organizações muitas vezes não sabem que a maioria das falhas de segurança são oriundas das próprias pessoas da empresa, nem como podem ocorrer os vazamentos, pois têm a errada concepção de que as falhas vêm apenas de ataques de grupos de *hackers* em um país distante, e que só afetam grandes corporações |

Fonte: Gardner e Thomas (2014); Green e Dorey (2016).

Em termos práticos, exemplos de comportamentos que contribuem para um ambiente corporativo com falhas de segurança da informação quando sua força de trabalho não se comunica com o staff de TI, tanto para sanar dúvidas técnicas como para reportar anomalias no funcionamento de seus equipamentos, compartilha senhas com colegas ou as anotam em lugares visíveis, por vezes utilizando a mesma credencial para vários serviços. Tais práticas colocam em risco a confidencialidade, integridade e disponibilidade dos dados, informações e serviços da rede interna da organização (HADNAGY, 2018; CERT.BR, 2020).

No tocante ao gerenciamento de senhas e credenciais de acesso, Pilar *et al.* (2012) afirma que indivíduos de maior grau de instrução formal tendem a apresentar menor dificuldade em memorizar senhas. Além disso, segundo os autores, estes usuários teriam a capacidade de possuir diferentes palavras-chave para os serviços que utilizam, o que proporciona uma maior segurança na utilização de computadores e outros dispositivos.

Outras práticas comuns por parte de usuários em organizações também podem representar riscos à SI organizacional são a utilização de dispositivos de armazenamento USB infectados com *malware* - como pen drives e discos rígidos portáteis - em computadores externos e conectando-os aos dispositivos da empresa, além da não utilização de áreas de *backup* disponibilizadas na rede corporativa (NISC, 2017).

A organização, por sua vez, deve estar atenta à sua responsabilidade de mitigar comportamentos e situações que coloquem em risco a sua SI. Côrte (2014) afirma que há três elementos-chave que o gestor deve gerenciar de maneira adequada nesse sentido, que, segundo o autor, são a tecnologia (dimensionamento, implementação e gestão da infraestrutura da organização), os processos (políticas e diretrizes claras que protejam ativos de informação) e as pessoas (investindo em sua conscientização e treinamento).

## 2.1 Envelhecimento humano, tecnologias digitais e SI

Debert (2004) afirma que mudanças ocorridas nos processos produtivos, especialmente aquelas relacionadas à informatização, afetam de maneira crítica a carreira de indivíduos técnica e tecnologicamente deficientes. Segundo a autora, o processo de adaptação dos sêniores à implementação de tecnologias digitais nos processos organizacionais é prejudicado pela interferência de conhecimentos anteriormente adquiridos em suas vidas.

No tocante à capacidade de lidar de maneira mais satisfatória com a tecnologia, Schleife

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

(2006) e Esteves (2014) inferem que um nível elevado de escolaridade afeta positivamente a relação do indivíduo com novas tecnologias, incluindo sua capacidade de memorizar senhas. Em paralelo a isto, segundo o IBGE (2019), em 2015 38,4% da população analfabeta do Brasil tinha mais que 55 anos, o que representa a maioria de brasileiros com baixa escolaridade e que 50% da população dessa faixa etária está ocupada no mercado de trabalho.

De acordo com Dias (2012), seres humanos apresentam mudanças ao longo da vida, iniciadas com uma etapa desenvolvimento físico e mental durante a infância e adolescência. Sucede-se então uma fase mais prolongada, na qual o organismo se torna menos eficiente pelo declínio considerável de algumas de suas capacidades, a exemplo do tempo de reação e da inteligência fluida. Esta última é uma referência à classificação da psicologia para os tipos de inteligência humana: a fluida e a cristalizada (CATTELL, 1998. SCHELINI, 2006).

Schelini (2006) associa a inteligência fluida à capacidade de lidar com situações pouco ou não dependentes de conhecimentos adquiridos previamente. Tarefas novas ou pouco conhecidas que não executadas de maneira automática são conduzidas por esse tipo de inteligência, sendo grandemente afetada por fatores biológicos, a exemplo de deficiências físicas, danos cerebrais e má nutrição. Em outras palavras, representa a capacidade humana de raciocinar corretamente e com velocidade em situações não usuais, tendendo a declinar após os 21 anos de idade, justamente devido à gradual degeneração das estruturas biológicas humanas (CATTELL, 1998; CARROLL, 1993).

A inteligência cristalizada, por sua vez, abarca as experiências culturais e os conhecimentos educacionais obtidos pelo indivíduo ao longo da vida. De acordo com Mackintosh (2012), este tipo de inteligência, ao contrário da fluida, tende a evoluir com o avanço etário devido ao acúmulo de conhecimento no decorrer dos anos. Com efeito, compreender os tipos de inteligência humana pode auxiliar no sentido do favorecimento da retenção de habilidades necessárias para evitar riscos à segurança da informação, especialmente nas camadas sociais mais vulneráveis nesse sentido, como os sêniores.

No que se refere a problemas físicos proporcionados pela utilização de computadores e outros dispositivos digitais por várias horas, Garcia (2001) menciona consequências nocivas à visão e aos músculos, tendões e nervos dos membros superiores, afetando sobretudo indivíduos mais velhos. A autora aponta ainda que tais efeitos por vezes acarretam o surgimento da síndrome conhecida como LER (Lesão por Esforços Repetitivos).

Tais efeitos nocivos que afetam de variadas maneiras toda a força de trabalho, mas com mais severidade os mais velhos, podem ser amenizados com a prática da Ginástica Laboral. A medida tem como benefícios potenciais reduzir efeitos físicos nocivos do uso prolongado de computadores por vezes realizado em posturas inadequadas, a exemplo de dores e lesões musculares, além de estresse físico e mental. Ademais, favorece o aumento da atenção e da qualidade de trabalho, além de estimular a integração social no ambiente corporativo (SWERTS; ROBAZZI, 2014).

Acerca de aspectos comportamentais dos sêniores em sua relação com a SI, a Panda Security (2017) sugere que pessoas de idade avançada não utilizaram computadores na escola, e a maioria deles nunca foi treinada adequadamente, além do fato de que muitos deles não tem consciência do valor que informações de cartões de crédito, senhas e outros dados pessoais têm para criminosos que atuam na internet. O'Keeffe (2014) e Lee *et al. (*2018) afirmam que os adul-

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

tos mais velhos apresentam menos confiança e se sentem menos confortáveis no uso de novas tecnologias que os jovens, inclusive pelo aumento constante na complexidade dos dispositivos digitais.

No entanto, apesar de sua inexperiência acerca dos riscos de SI, os mais velhos tendem a passar mais tempo on-line, pois cada vez mais governos, bancos e outras instituições estão digitalizando seus serviços em favor de um menor custo operacional. Uma pesquisa feita pela Kaspersky em 2017 descreve os sêniores como pessoas com mais tempo livre para explorar o mundo on-line e mais dinheiro disponível, o que os coloca em situação de potencial perigo no que se refere a riscos no mundo digital.

O estudo menciona também que apesar de que esses indivíduos utilizam com cada vez maior frequência recursos oferecidos online, como o envio de e-mails e compras pela internet, são os que menos utilizam software antivírus em seus dispositivos. Outra conclusão da pesquisa afirma que os usuários de idade avançada costumam levar mais tempo para perceberem que estão sendo alvos de fraudes cibernéticas do que pessoas de faixas etárias mais jovens (KASPERSKY, 2017).

Carlson (2007) corrobora com a Kaspersky nesse sentido, pois menciona que os mais velhos vêm de uma geração em que negócios e acordos eram conduzidos muitas vezes a partir de apenas um aperto de mão. De maneira geral, 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.

Para Friedberg (2003), a aproximação da aposentadoria também favorece que usuários de idade mais avançada evitem investir tempo e recursos financeiros em treinamentos que os habilitem a utilizar melhor computadores e outras ferramentas digitais. Trabalhadores mais velhos e empresas nas quais estas pessoas trabalham por vezes consideram que não haverá tempo hábil para o investimento em treinamento ser recuperado, uma vez que lhes resta pouco tempo de serviço em comparação a outras faixas etárias.

Por fim, Thompson e Mayhorn (2012) afirmam que as tecnologias digitais têm potencial para facilitar ou impedir o sucesso de trabalhadores mais velhos, que são cada vez mais expostos a ambientes de trabalho tecnológicos. Os autores justificam a afirmação dizendo que, embora as ferramentas e a tecnologia de modo geral estejam aprimorando a acessibilidade para capitalizar os pontos fortes desse grupo de empregados e sobrepor suas limitações - a exemplo da potencial redução na memória, força física, acuidade visual e mobilidade - a própria tecnologia tem a capacidade de causar novos problemas, estabelecendo desafios a serem enfrentados pelos mais velhos.

## 3. Metodologia

Dado o caráter do estudo, percebe-se que à medida em que se busca o aprofundamento a respeito de uma realidade da unidade de análise, este pode ser classificado como um estudo de caso único, definido por Yin (2015) como sendo um questionamento empírico que investiga um fenômeno contemporâneo com seu contexto da vida real. A presente pesquisa adotou características qualitativas e quantitativas fundamentadas logicamente na amostra.

Ao adotar uma abordagem quantitativa, esta pesquisa buscou focar sua análise em quan-

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

tidade limitada de conceitos, a exemplo da verificação da conformidade do uso de computadores e outros dispositivos digitais de acordo com as boas práticas de SI. Assumiu também, todavia, características qualitativas, pois utilizou da técnica de observação participante para observar eventos. O estudo utilizou procedimentos estatísticos para analisar os dados coletados e partindo de ideias preconcebidas, relacionadas aos conceitos expostos no referencial teórico (REMLER; VAN RYZIN, 2014).

Para Yin (2015), cada estudo de caso consiste em um estudo acabado no qual se procuram evidências convergentes com respeito aos fatos e às conclusões para o caso. Assim, a EMDAGRO, órgão público do estado de Sergipe, foi o único objeto de estudo. A organização foi analisada no sentido de verificar como seus usuários, especialmente o grupo dos mais velhos, se comportam em relação à proteção da informação, além de comparar esse comportamento com o exercido pelos empregados mais jovens.

No intuito de serem alcançados os objetivos da pesquisa, os dados foram coletados por meio de questionário estruturado e a estratégia da observação participante, uma vez que um dos autores possui vínculo como terceirizado na empresa. Esta última ação permite "ver" situações que os participantes não informariam voluntariamente (PATTON, 2014).

Para a aplicação do formulário, foram compostas por 19 questões fechadas dos tipos binária e de múltipla escolha, sendo estas últimas elaboradas com a utilização de escala Likert. Segundo Remler e Van Ryzin (2014), a utilização de escalas de mensuração multi-item proporciona múltiplas intensidades de concordância com o tema questionado e contribui para o alcance de resultados satisfatórios, confiáveis e que permitam conclusões apropriadas.

Inicialmente, o questionário levantou o perfil etário, educacional, da frequência de acesso à internet fora do expediente e do conhecimento sobre SI dos participantes. Na sequência, foram questionados acerca dos comportamentos em algumas situações relacionadas a boas práticas em proteção à informação, de acordo com a literatura apresentada sobre segurança da informação. Em seguida as variáveis foram classificadas em independentes e dependentes conforme o Quadro 2, e por conseguinte, cruzadas. Essa categorização das variáveis se deu pela análise da interferência que as variáveis independentes têm sobre as dependentes (REMLER; VAN RYZIN, 2014).

Quadro 2 – Variáveis da Pesquisa

| Variáveis independentes | Variáveis dependentes |
|---|---|
| Faixa etária | Busca por conhecimento sobre SI |
| Escolaridade | Desconhecimento sobre *phishing* |
| Participação em cursos de informática | Utilização de *backups* |
| Utilização de dispositivos conectados à internet fora do expediente | Frequência no reporte de anomalias ao suporte de informática |
| - | Gerenciamento de senhas |

Fonte: Elaborado pelos autores

As variáveis independentes foram traçadas para representar os aspectos de perfil apontados pela literatura que favorecem a existência de um ou mais comportamentos inseguros no tocante à proteção à informação, como faixa etária elevada, escolaridade e histórico de participação em treinamentos. Também foi avaliada a frequência de contato que o participante tem com a tecnologia digital fora do ambiente da empresa. Essa variável independente foi

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

criada para verificar o interesse do participante em utilizar dispositivos conectados à internet e se gastam mais tempo fazendo isso, segundo a literatura especializada (KASPERSKY, 2017; KI-ARIES; FAILY, 2017)

Já as variáveis classificadas como dependentes representam os diversos cenários comuns aos usuários da organização, e suas possíveis atitudes diante de tais situações. Foram avaliadas as posturas dos participantes acerca de seu conhecimento sobre phishing, frequência no reporte de anomalias de na utilização de dispositivos digitais, conhecimentos sobre *backup* e sua utilização, dificuldade na memorização de senhas e o hábito de compartilhá-las, e o interesse na busca individual por mais conhecimento sobre SI. Assim, foram escolhidas questões que avaliassem a conformidade das práticas cotidianas dos participantes da pesquisa com a SI (GARDNER; THOMAS, 2014).

Adicionalmente, houve consulta a registros históricos da organização relacionados à abertura de incidentes à equipe de atendimento ao usuário da empresa. A verificação de tais registros embasou a análise de eventos de elevada severidade ocorridos no ambiente de rede da organização, servindo como exemplo de que problemas semelhantes podem ser mitigados quando se exerce uma gestão eficiente da SI na empresa (MAULAIS, 2016).

Por ser um dos autores deste trabalho integrante da equipe de suporte em informática da organização, a pesquisa se utilizou da técnica de observação participante, haja vista esse tipo de observador vê situações em "primeira mão" e utiliza conhecimento próprio e expertise para interpretar o que está sendo observado. Além disso, há a possibilidade de "ir além" da percepção dos outros, desenvolvendo uma visão mais compreensiva. Dito isto, fez-se possível obter informações acerca da postura da organização no tratamento de seus incidentes, e no gerenciamento de seus recursos tecnológicos, no tocante à existência de políticas e diretrizes (PATTON, 2014; MERRIAM; TISDELL, 2015).

A amostra avaliada foi composta por 97 pessoas, que abrange parte da força de trabalho do escritório sede (Aracaju) e de escritórios locais e regionais da EMDAGRO em diversos municípios de Sergipe. Possui elevada faixa etária (67% dos participantes da pesquisa tem mais que 55 anos de idade, conforme pode ser verificado na Tabela 1) e foi questionada utilizando o instrumento definido nesta metodologia.

Tabela 1 - Faixa etária dos entrevistados

| Faixa etária | Frequência | Porcentagem (%) |
|---|---|---|
| **18-25** | 5 | 5,2 |
| **26-40** | 11 | 11,3 |
| **41-55** | 16 | 16,5 |
| **Acima de 55** | 65 | 67,0 |
| **Total** | **97** | **100,0** |

Fonte: Dados da pesquisa.

Verifica-se, adicionalmente, que a organização possui mão de obra qualificada em sua maioria, conforme se faz possível notar na Tabela 2.

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

Tabela 2 - Escolaridade dos participantes da pesquisa

| Grau de escolaridade | Frequência | Porcentagem (%) |
|---|---|---|
| Ensino fundamental | 5 | 3,1 |
| Ensino médio | 35 | 36,1 |
| Ensino superior incompleto | 10 | 10,3 |
| Ensino superior completo | 32 | 33,0 |
| Pós-graduação | 17 | 17,5 |
| **Total** | **97** | **100,0** |

Fonte: Dados da pesquisa

Após a aplicação do questionário, os dados foram tabulados no software SPSS versão 23 e analisados por estatística descritiva, com medidas de distribuição normal (média). A análise resultante da coleta foi feita, inicialmente, pelo cálculo de médias de frequência da presença de empregados de faixas etárias mais elevadas entre os que possuem uma postura insegura diante dos cenários avaliados, majoritariamente verificados por meio do questionário estruturado.

Acerca da análise de dados históricos da organização, foram buscados casos de falhas graves na proteção à informação da empresa estudada que poderiam colocar em risco a confidencialidade, integridade e disponibilidade das informações organizacionais, além de pôr sob ameaça o funcionamento de alguns de seus sistemas de tecnologia, e consequentemente sua produtividade. Esses dados são oriundos de reportes de usuários e de incidentes de segurança verificados pela equipe de atendimento de TI.

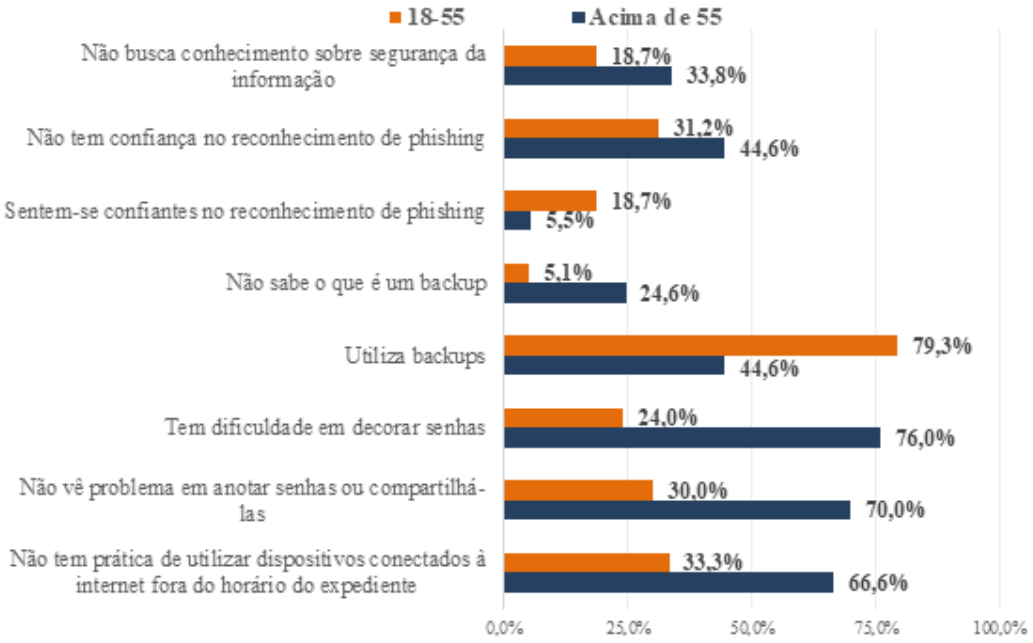
## 4. Resultados

A coleta de dados revelou alguns padrões de hábitos dos usuários da EMDAGRO de faixas etárias mais avançadas - especialmente os acima de 55 anos – que podem ser citados como favorecedores de riscos à confidencialidade, integridade e disponibilidade dos dados e informações da empresa. Percebeu-se, porém, uma conformidade às boas práticas de proteção à informação semelhante ou superior às dos pares mais jovens em alguns cenários, que serão explorados mais adiante.

Inicialmente, expondo características de inconformidade com os preceitos da segurança da informação, o gráfico 1 exibe dados dos principais resultados obtidos pela pesquisa, listando cenários nos quais os usuários sêniores apresentaram comportamentos mais inseguros em SI quando comparados aos empregados mais jovens da organização.

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

Gráfico 1 – C comportamentos em situações relacionadas à proteção da informação por faixa etária




Fonte: Dados da pesquisa.

No que se refere à procura pelo conhecimento sobre os riscos de SI aos quais estão expostos e sobre maneiras de se proteger dessas ameaças, os usuários da EMDAGRO afirmaram ter uma postura de curiosidade, pois 71,1% dos empregados afirmaram fazê-lo. Todavia, a proporção de pessoas que não tem essa preocupação entre os usuários mais velhos da organização é quase 50% maior do que entre os outros grupos etários, perfazendo 33,8% contra 18,7% dos que possuem de 18 a 55 anos de idade.

A ausência de interesse na busca de conhecimento sobre SI por parte dos empregados revela aspectos relacionados à ignorância técnica, pouca conscientização e concepções errôneas acerca dos riscos aos quais essa postura pode conduzir, tanto individuais como coletivos. Dentre os mais velhos, a reduzida postura pode indicar o que Friedberg (2003) menciona, no sentido de que a proximidade da aposentadoria e o reduzido tempo de serviço restante contribuem para um menor interesse nesse tópico.

A confiança dos empregados da EMDAGRO em sua capacidade de evitar o *phishing* também foi avaliada. Dentre os sêniores participantes da pesquisa, 44,6% nunca se sentem seguros na identificação de um e-mail fraudulento ou página web maliciosa, contra uma média de 31,2% de outras faixas etárias. Já entre os que se sentem totalmente seguros para identificar uma tentativa de *phishing*, a proporção é de apenas 5,5% entre os empregados sêniores, contra 18,7% entre os mais jovens.

Este fato corrobora com as análises de Gardner e Thomas (2014) e Green e Dorey (2016), que mencionam a ignorância técnica e concepções incorretas acerca da origem dos riscos como origens de vulnerabilidades involuntárias. Não saber reconhecer um e-mail ou página web fraudulenta, disfarçados em técnicas de *phishing*, pode conduzir o usuário a expor a SI organizacional a graves riscos, como a infecção de diversos computadores pela execução de anexos infectados e o favorecimento à invasão dos sistemas da empresa.

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

Não obstante, a capacidade de raciocínio e de tomada de decisão ao se deparar com esse tipo de ameaça, que apresenta novas características constantemente para se disfarçar em páginas e e-mails legítimos depende da inteligência fluida do usuário. Segundo Schelini (2006), essa capacidade é reduzida à medida que o indivíduo envelhece, o que pode lançar luz na tentativa de compreender a pouca confiança dos sêniores neste quesito.

Os usuários também foram questionados sobre como encaram a prática de realizar *backups*. Considerados fundamentais no conjunto de boas práticas de manutenção dos pilares da SI, uma vez que são decisivos na disponibilidade, integridade e confidencialidade dos dados e informações, foi verificado na organização estudada que à medida que a faixa etária vai avançando, menor é a frequência de criação cópias de segurança por parte dos empregados.

A pesquisa mostra que apenas 44,6% dos avaliados acima de 55 anos afirmaram possuir *backups* de seus dados. Entre entrevistados mais jovens, 71,9% responderam que salvam cópias seguras de dados que julgam importantes. Outra particularidade percebida nesta questão é a quantidade de usuários entre os sêniores que afirmaram não saber o que é um *backup.* 24,6% de pessoas desse grupo manifestaram desconhecer o assunto, em contraste de 6,2% entre os de 18 a 55 anos de idade.

Sem embargo, a falta de conhecimento dos usuários mais velhos sobre o conceito e a importância dos *backups*, além de sua reduzida prática entre esses empregados, expõe a organização a vulnerabilidades de SI, podendo ameaçar gravemente os pilares da segurança da informação. Os *backups* exercem um papel primordial na salvaguarda de dados e informações, uma vez que ataques cibernéticos e acidentes causados pelos próprios empregados - como a exclusão acidental e a execução involuntária de malware - potencialmente indisponibilizam esses recursos, afetando diretamente a disponibilidade e integridade da informação (WHITMAN, 2017).

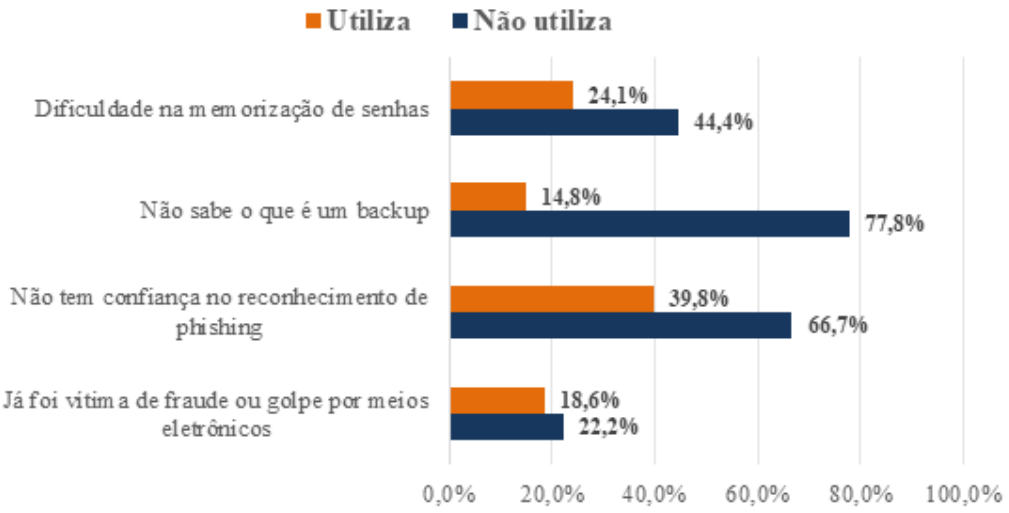
No tocante ao gerenciamento de senhas, outra faceta crítica na proteção à SI pessoal e organizacional, verificou-se na pesquisa que dos 97 entrevistados, 25 afirmaram ter dificuldade para memorizar senhas, sendo que 76% deles possuem mais de 55 anos. Entre as faixas etárias mais jovens, apenas 6 indivíduos afirmaram ter problemas para lembrar suas credenciais de acesso à rede e outros serviços (24%).

Referindo-se ao compartilhamento com colegas e a anotação de senhas em lugares visíveis, 70% dos que afirmaram não ver problemas em fazê-lo têm mais que 55 anos de idade, contra 30% dos empregados de outras faixas etárias. Esses dados confirmam as afirmações de Thompson e Mayhorn (2012), que mencionam efeitos da reduzida capacidade de memória dos mais velhos em sua relação com a tecnologia, e corroboram com as conclusões de Hadnagy (2018) no tocante aos riscos que um gerenciamento deficiente de senhas pode representar à SI.

A aplicação do instrumento de pesquisa trouxe à luz o fato de que sêniores são os empregados que menos acessam dispositivos conectados à internet quando estão fora do expediente. 66% dos que estão nessa condição tem mais que 55 anos de idade. Adicionalmente, dos empregados que afirmaram acessar a internet por menos de 1 hora ao dia quando estão fora da empresa, 81% são sêniores, e perceberam-se padrões potencialmente inseguros específicos a essas pessoas. Ou seja, os que menos utilizam dispositivos digitais para realizar tarefas diversas, como buscar entretenimento e informação, comunicar-se com amigos e familiares e outras atividades. Tais padrões serão exibidos no Gráfico 2.

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

Gráfico 2 – Comparação de médias características potencialmente inseguras entre usuários que não utilizam dispositivos digitais fora do expediente e os que afirmaram fazê-lo.




Fonte: Dados da pesquisa.

Com efeito, verificou-se que os usuários que não afirmaram só ter contato com dispositivos digitais durante o expediente na empresa apresentam maior dificuldade na memorização de senhas, menor conhecimento sobre *backups* e maior insegurança na identificação de *phishing*. Apresentam também maior suscetibilidade a fraudes perpetradas por meios eletrônicos: 22,2% já foi vítima desse tipo de golpe, contra 18,2% dos outros usuários.

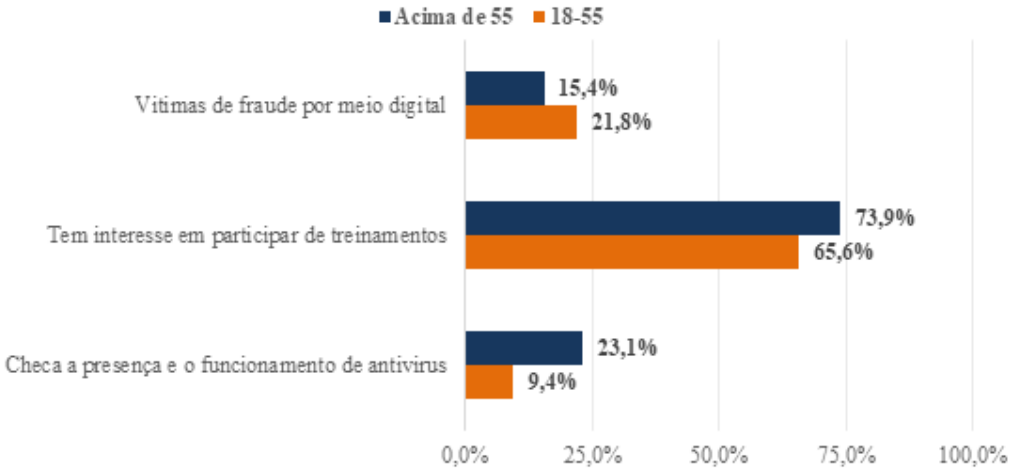
Os outros grupos, que utilizam por mais tempo computadores, *smartphones* e outros dispositivos digitais conectados à internet fora do horário de trabalho, apresentaram proporções menores de presença de vítimas de fraudes, 11,1% entre os que acessam por 1 a 2 horas e 15,6% dos que fazem uso por mais de 2 horas.

Estes resultados foram de acordo com o que afirmam autores como Lee (2018) e O'Keeffe (2014), que mencionam em seus estudos uma maior confiança e capacidade técnica na lida com dispositivos digitais oriundas não só de treinamentos formais em tecnologia e informática, mas também na utilização mais frequente desses dispositivos.

A pesquisa apresentou também resultados discrepantes ao que se verifica na literatura especializada. Esses dados serão exibidos no Gráfico 3.

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

Gráfico 3 – Porcentagens de presença das faixas etárias avaliadas em situações discrepantes às postulações da literatura especializada.




Fonte: Dados da pesquisa.

Durante a pesquisa percebeu-se que os participantes que têm mais que 55 anos afirmaram terem sido vítimas com menos frequência de golpes perpetrados por meios digitais (computador, *smartphone*) do que indivíduos mais jovens, apesar do que afirma o estado da arte da literatura, como estudos da Kaspersky e Panda Security, ambos de 2017.

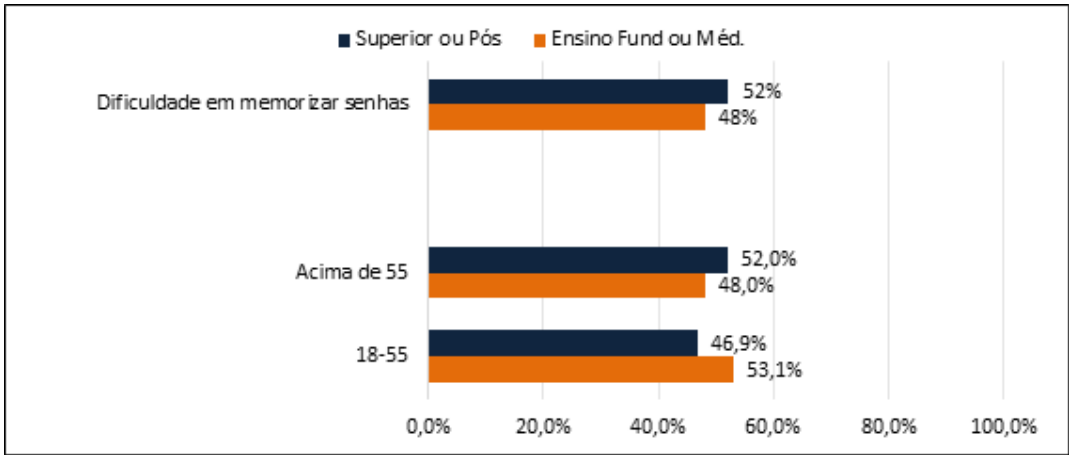
Além disso, os sêniores responderam ter mais interesse em participar de treinamentos fornecidos pela organização, apesar de buscarem menos conhecimento por conta própria, conforme verificado anteriormente nos resultados expostos no Gráfico 1. Esse cenário contraria o que é defendido por Friedberg (2003), que menciona menor interesse desse grupo de pessoas em qualificar-se em novas tecnologias, em virtude da proximidade da aposentadoria.

Ademais, os usuários mais velhos da organização afirmaram realizar com mais frequência a verificação da presença e da atualização de software antivírus nos computadores que utilizam. Mais estudos são necessários para avaliar as razões pelas quais os usuários apresentaram essa postura, já que a literatura especializada menciona a reduzida consciência dos usuários sêniores acerca dos riscos de SI e maneiras sobre como prevenir-se de tais ameaças (GARDNER; THOMAS, 2014; GREEN; DOREY, 2016).

Outro resultado do estudo que vai de encontro às postulações do estado da arte da literatura é a influência da escolaridade do indivíduo e sua capacidade de memorizar senhas, como mencionam Pilar et. al (2012) e Esteves (2014). O Gráfico 4 exibe os detalhes acerca dessa questão.

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

Gráfico 4 – Dificuldade na memorização de senhas por grau de escolaridade e Graus de escolaridade por faixas etárias.




Fonte: Dados da pesquisa.

Os dados encontrados mostram que a dificuldade na memorização de senhas esteve menos relacionada ao grau de escolaridade do participante do que à sua idade. Outra percepção que se teve na pesquisa foi a possível relação entre a memorização de senhas e a falta de prática no uso de dispositivos digitais, como verificado no Gráfico 2. Esse último fator mostrou-se mais determinante a essa deficiência por parte dos usuários do que seu grau de escolaridade ou sua idade, embora 66% dos que afirmaram não utilizar *smartphones* ou computadores fora do horário de expediente tenham mais que 55 anos de idade.

## 5. Conclusão

Procurou-se verificar aspectos de SI oriundos de hábitos e características dos sêniores que poderiam expor o ambiente de rede da organização a brechas de segurança da informação, como a infecção de dispositivos eletrônicos por vírus, invasões do sistema por *hackers* e a perda ou roubo de dados e informações sensíveis à organização.

Nesse sentido, a organização estudada mostrou-se exposta a diversas falhas de segurança. Muitos usuários, especialmente os mais velhos, apresentam comportamentos inseguros no tocante à consciência sobre a necessidade de proteção dos seus dados e do ambiente de rede da EMDAGRO, quando comparados aos funcionários mais jovens. Como exemplos deste cenário podem ser citados a menor frequência com que buscam individualmente conhecimentos sobre segurança da informação, a falta de conhecimento sobre *phishing*, a pouca utilização de *backups*, a dificuldade no gerenciamento de suas senhas e o hábito de compartilhá-las com colegas.

Logo, os riscos à SI na EMDAGRO são potencializados pela menor presença de informação e conhecimento técnicos em usuários de faixas etárias mais avançadas, além do menor interesse em buscar individualmente conhecimentos acerca sobre como utilizar melhor recursos tecnológicos e como proteger seus dados e o ambiente virtual da organização. Nesse ínterim, faz-se mister estimular o treinamento individual e organizar programas de qualificação técnica coletivos, gerando confiança e familiarização no uso de aparelhos digitais, além de conscientizar acerca dos riscos e prejuízos pessoais e coletivos oriundos de falhas de SI. Outro fator que pode favorecer o ambiente da organização estudada nesse sentido é o fato de que os usuários se mostraram interessados em participar em treinamentos se porventura fossem oferecidos pela

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

empresa.

A menor frequência com que utilizam computadores e outros dispositivos digitais fora do expediente foi verificado como um fator que pode contribuir para um comportamento mais inseguro, uma vez que culmina num maior afastamento dos sêniores às tecnologias digitais e suas melhores práticas. Lee *et al. (*2018), por exemplo, afirma que a confiança e a sensação de se sentirem confortáveis e à vontade no uso dos dispositivos digitais exercem uma influência direta na habilidade dos usuários em relação à tecnologia.

Limitações cognitivas também podem fazer com que esses empregados exerçam comportamentos de maior risco à SI da organização. A menor capacidade de memorização de senhas, independentemente da escolaridade dos usuários e mais relacionada à idade e frequência de utilização de dispositivos digitais, além da reduzida inteligência fluida dos mais velhos tendem a práticas inseguras, como o compartilhamento e armazenamento escrito de credenciais de acesso e percepção menos eficiente de tentativas de fraude pela captura de dados por páginas web falsas e e-mails maliciosos.

Com efeito, no caso da EMDAGRO, e de outras organizações porventura na mesma configuração etária, criar políticas que condicionem usuários mais velhos a se habituarem a procedimentos mais próximos às boas práticas de SI e treiná-los frequentemente nesse sentido, favorecendo a retenção de conhecimentos em sua inteligência cristalizada e estimulando um relacionamento positivo com a tecnologia. O incentivo à utilização de áreas de *backup* e à retenção de senhas na mente, orientações sobre como evitar tentativas de *phishing* e execução de *malware*, além de um maior contato com o staff de TI são exemplos de práticas a serem estimuladas.

A organização, por sua vez, deve manter-se à disposição por canais eficientes de atendimento para sanar dúvidas sobre tecnologia e o reporte de anomalias no uso de dispositivos digitais podem incutir nos usuários hábitos mais seguros no tocante à proteção dos dados que utilizam diariamente, bem como do ambiente de rede da organização.

É possível também buscar maneiras de se admoestarem empregados que não buscam conhecimento sobre boas práticas em SI e cometem erros no uso de recursos tecnológicos, como conversas individuais, treinamentos de reciclagem técnica, fixação de lembretes e orientações sobre SI em quadros de anúncios. Além de evitar problemas se segurança no futuro, uma melhor relação da força de trabalho com a tecnologia digital contribui com vias a uma maior produtividade organizacional.

Todos os usuários que participaram da pesquisa utilizam o computador por várias horas durante o expediente. Com a tendência atual de uso de digitalização de processos organizacionais, empregados de faixas etárias mais avançadas são especialmente afetados pelos efeitos do uso desses aparelhos por longas horas, afetando sua visão, músculos e tendões. Dito isto, sugere-se a prática da ginástica laboral à força de trabalho da EMDAGRO. Bons resultados foram obtidos por outros órgãos da administração estadual de Sergipe, que recebem a visita de especialistas nesse tipo de ginástica de uma a duas vezes por semana, e auxiliam os usuários a minimizarem os efeitos causados por horas utilizando dispositivos digitais.

A medida tem como benefícios potenciais reduzir efeitos físicos nocivos do uso prolongado de computadores por vezes realizado em posturas inadequadas, a exemplo de dores, lesões

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

musculares e estresse físico e mental. Ademais, favorece o aumento da atenção e da qualidade de trabalho, além de estimular a integração social no ambiente corporativo.

## Referências

ALEXANDRIA, J. **Gestão da segurança da informação: uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica.** 2009. Tese de Doutorado (Pós-Graduação em Ciências em Tecnologia Nuclear – IPEN) - Pontifícia Universidade de São Paulo. São Paulo. 2009.

ARFI, N.; AGARWAL, S. Knowledge of cybercrime among elderly. **International Journal of Scientific & Engineering Research**, Volume 4, Issue 7, p. 1463-1468, July. 2013. Disponível em: https://www.ijser.org/onlineResearchPaperViewer.aspx?Knowledge-of-Cybercrime-among-Elderly.pdf . Acesso em 05 jul 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **NBR ISO/IEC 27002:Tecnologia da informação: técnicas de segurança**. Rio de Janeiro, ABNT. 2013.

AWAD, A.; FAIRHURST, M; Introduction to information security foundations and applications. In: **Information Security:** Foundations, Technologies and Applications. Londres: The Institution of Engineering and Technology, 2018. p. 3-11.

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: 02 jul 2020.

CARLSON, E. Phishing for Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting Them Follow. **The Elder Law Journal, Illinois University**, v.14, p. 423-452, 2007. Disponível em: https://theelderlawjournal.com/wp-content/uploads/2019/01/carlson.pdf . Acesso em 04 jul 2020.

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

CASTELLS, M. **A sociedade em rede: a era da informação: economia, sociedade e cultura**. 8ª. Ed. São Paulo: Paz e Terra, 2007. V. 1.

CATTELL, R. Where is intelligence? Some answers from the triadic theory. MCARDLE, J. J.; WOODCOCK, R. W. (Eds.). **Human cognitive abilities in theory and practice**. New Jersey: Erlbaum. 1998, p. 29-38.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.BR. **Cartilha de Segurança para Internet**. 2020. Disponível em: https://cartilha.cert.br/. Acesso em 01 jul 2020.

CÔRTE, K. **Segurança da informação baseada no valor da informação e nos pilares**

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

**tecnologia, pessoas e processos**. Brasília, 2014. Tese de Doutorado (Pós-Graduação em Ciência da Informação) – Universidade de Brasília. Brasília. 2014.

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

DIAS, I. O uso das tecnologias digitais entre os seniores: motivações e interesses. **Sociologia, Problemas e Práticas**, Lisboa, v. 68, p. 51-77, 2012. Disponível em: http://www.scielo.mec.pt/pdf/spp/n68/n68a03.pdf. Acesso em: 11 fev. 2019.

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

FRANÇA, W. **A utilização da criptografia para uma aprendizagem contextualizada e significativa**. Brasília, 2014. Dissertação (Mestrado em Matemática) — UNB. Brasília.

FRIEDBERG, L. The impact of technological change on older workers: evidence form data on computers. **No 8297, NBER Working Papers.** 2003. Disponível em: https://www.nber.org/system/files/working_papers/w8297/w8297.pdf. Acesso em: 25 fev 2020.

GARCIA, H. **A Terceira Idade e a Internet: uma questão para o novo milênio**. 2001. 171f. Dissertação (Mestrado) – Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília. 2001.

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

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.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA – IBGE (2019a). **Projeção da população. Projeções da População do Brasil e Unidades da Federação por sexo e idade: 2010-2060**. Rio de Janeiro: IBGE, 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.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA – IBGE (2019b). **Pesquisa Nacional por Amostra de Domicílios - PNAD COVID19**. Rio de Janeiro: IBGE, 2019. Disponível em: https://ftp.ibge.gov.br/Trabalho_e_Rendimento/Pesquisa_Nacional_por_Amostra_de_Domicilios_PNAD_COVID19/Mensal/Tabelas/pnad_covid19_202011_trabalho_BR_GR_UF.xlsx. Acesso em 20 jan 2021.

KASPERSKY. **Older and wiser? A look at the threats faced by over-55s online**. 2017. 10p. Disponível em: https://media.kasperskycontenthub.com/wp-content/uploads/

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

sites/100/2017/05/10084116/Report_Over-55s_Online_ENG_UPD.pdf Acesso em 03 jul 2020.

KI-ARIES, D.; FAILY, S.; Persona-centered Information security awareness. **Computers & security**, [S.L], n. 70, p. 663-674, jan. 2017. Disponível em: https://reader.elsevier.com/i/67404817301566?to8655FA551DAD3F8E9F0525940A4945329255D8F0D948867332288FF02E5B2095E4584C7A20E38B. Acesso em: 03 jul 2020.

LEE, C., CZAJA, S., MOXLEY, J., SHARIT, J., BOOT, W., CHARNESS, N., ROGERS, W. (2018). Attitudes toward computers across adulthood from 1994–2013. **The Gerontologist**, July 5. doi: 10.1093/geront/gny081.

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

MACKINTOSH, N. History of Theories and Measurement of Intelligence. In: R. Sternberg & S. Kaufman (Eds.), **The Cambridge Handbook of Intelligence**. Cambridge: Cambridge University Press. 2012. pp. 3-19.

MAULAIS, C. **Engenharia Social: Técnicas e Estratégias de Defesa em Ambientes Virtuais Vulneráveis**. 2016. Dissertação (Mestrado) – Mestrado em Sistemas de Informação e Gestão do Conhecimento. Universidade FUMEC. Belo Horizonte, 2016

MCAFEE. **Economic Impact of Cybercrime – No Slowing Down**. 2018. Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf . Acesso em 02 jul 2020.

MENTLIK, G.; MENEZES-FILHO, N.; KOMATSU, B. **Aposentadoria e mercado de trabalho: uma análise usando regressão descontínua**. IPEA. 2019. Disponível em: http://repositorio.ipea.gov.br/handle/11058/9768. Acesso em 03 jul 2020

MERRIAM, S.; TISDELL, E. **Qualitative research: a guide to design and implementation**. 4. ed. São Francisco: Jossey-Bass Publishers, 2015.

NATIONAL CENTER OF INCIDENT READINESS AND STRATEGY FOR CYBERSECURITY (NISC). **Information Security Handbook for Network Beginners**. The Government of JAPAN. 2017. 36p. Disponível em: https://www.nisc.go.jp/security-site/campaign/files/aj-sec/handbook-all_eng.pdf. Acesso em 02 jul 2020.

O'KEEFFE, R. **Baby boomers and digital literacy: their access to, and uses of, digital devices and digital media** (2014). Tese de Doutorado. Pepperdine University. Theses and Dissertations. 501. Disponível em: https://digitalcommons.pepperdine.edu/etd/501. Acesso em 20 jan 2021

OUSLEY, M. **Information Security: The Complete Reference**. 2. ed. atual. New York: The McGraw-Hill Company, 2013. 897 p.

PANDA SECURITY. **How to protect the elderly online**. [S. l.], 30 maio 2017. Disponível em: https://www.pandasecurity.com/mediacenter/tips/protect-elderly-online/.

PATTON, M. Q. **Qualitative research and evaluation methods.** 4th ed. Thousand Oaks,

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

Califórnia: Sage Publications, 2014. 832 p.

PILAR, D.; JAEGER, A.; GOMES, C.; STEIN, L. **Passwords Usage and Human Memory Limitations**: A Survey across Age and Educational Background. PLoS ONE 7(12): e51067. 2012. Disponível em: https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0051067&type=printable. Acesso em 21 de fev. 2019.

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

REMLER, D.; VAN RYZIN, G. **Research methods in practice**: Strategies for description and causation. Sage Publications, 2014.

SCHLEIFE, K. **Computer Use and the Employment Status of Older Workers**. LABOUR: Review of Labour Economics and Industrial Relations, 2006. 20(2).

SCHELINI, W. Teoria das inteligências fluida e cristalizada: início e evolução. **Estudos. Psicológicos**. 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.

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

SYMANTEC. **Symantec Internet Security Threat,** 2018. Disponível em: http://images.mktgassets.symantec.com/Web/Symantec/%7B4367e625-7050-4087-b199-9640c778699f%7D_ISTR23-FINAL_PT.pdf. Acesso em: 03 de nov. 2018.

SWERTS, F.; ROBAZZI, M. Efeitos da ginástica laboral compensatória na redução do estresse ocupacional e dor osteomuscular. **Revista Latino Americana de Enfermagem**, Ribeirão Preto, ano 2014, v. 22, n. 4, ed. 22, t. 4, p. 629-636, 2014. DOI 10.1590/0104-1169.3222.2461. Disponível em: http://www.scielo.br/scielo.php?script=sci_pdf&pid=S0104-11692014000400629&lng=pt&nrm=iso&tlng=pt . Acesso em: 23 mai 2019.

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

TRANSPARÊNCIA SERGIPE. **Servidores por Órgão.** 2019. Disponível em: http://www.transparenciasergipe.se.gov.br/TRS/Pessoal/PorOrgao.xhtml. 04 jul 2020.

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

YIN, R. K. **Estudo de caso**: planejamento e método. 5. ed. Porto Alegre: Bookman, 2015.

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

INSTRUMENTO DE PESQUISA (QUESTIONÁRIO ELABORADO)

UNIVERSIDADE FEDERAL DE SERGIPE

CENTRO DE CIÊNCIAS SOCIAIS E APLICADAS

DEPARTAMENTO DE ADMINISTRAÇÃO

PESQUISA – SEGURANÇA DA INFORMAÇÃO ORGANIZACIONAL

_____

1. Qual é a sua faixa etária?

( ) 18-55 ( ) Acima de 55

2. Qual o seu grau de escolaridade?

( ) Ensino Fundamental;

( ) Ensino Médio;

( ) Ensino Superior incompleto;

( ) Ensino Superior completo;

( ) Pós-graduação.

3. Já fez cursos de informática?

( ) SIM ( ) NÃO

4. Costuma utilizar computadores ou dispositivos conectados à internet em casa ou fora do ambiente de trabalho? (Se sua reposta for NÃO, favor pular a questão 5)

( ) SIM ( ) NÃO

5. Utiliza, fora do horário de trabalho, dispositivos conectados à internet por quantas horas ao dia?

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

( ) 0

( ) Mais que 1

6. Verifica a presença e correto funcionamento de programa antivírus no computador de casa, trabalho ou seu celular/smartphone?

( ) SIM

( ) NÃO

7. Busca conhecimento sobre como utilizar melhor e de maneira mais segura o computador e outros dispositivos conectados à internet?

( ) SIM ( ) NÃO

8. Já foi vítima de fraude ou golpe por telefone ou internet?

( ) SIM ( ) NÃO

9. Saberia identificar um e-mail falso, enviado por alguém aparentemente desconhecido com o objetivo de instalar vírus ou roubar dados?

( ) SIM

( ) NÃO

10. Costuma conectar a computadores da empresa ou ao seu próprio (caso tenha) dispositivos como pendrives ou HD's externos?

( ) SIM ( ) NÃO

11. Sabe o que é um backup, ou cópia de segurança de dados importantes? (Se sua reposta for NÃO, favor pular a questão 12)

( ) SIM ( ) NÃO

ISSN – 2317 - 0115
v. 9 , n. 2. (2020)
Recife – PE – UFPE / CCSA - MGP

12. Costuma ter um backup de seus arquivos importantes?

( ) SIM ( ) NÃO

13. Reporta ao setor de informática da empresa se algo aparentemente estranho ou perigoso aparece no computador que utiliza?

( ) SIM

( ) NÃO

14. Vê algum problema em compartilhar com colegas ou anotar em locais visíveis suas senhas?

( ) SIM ( ) NÃO

15. Tem dificuldade em lembrar e decorar senhas?

( ) SIM ( ) NÃO

16. Faz uso de notebook corporativo que utiliza em casa ou em outros ambientes? (Se sua reposta for NÃO, favor pular a questão 17)

( ) SIM ( ) NÃO

17. Outras pessoas utilizam o notebook corporativo além de você?

( ) SIM ( ) NÃO

18. Já teve o computador ou celular smartphone infectado por vírus, que o fez perder dados ou ficou impossibilitado de utilizar o aparelho temporariamente?

( ) SIM ( ) NÃO

19. Teria interesse em participar de treinamentos sobre como utilizar melhor o computador e celular/smartphone, protegendo de maneira mais eficiente dados pessoais e da empresa em que trabalha?

( ) SIM ( ) NÃO