UNIVERSIDADE FEEVALE

WILLIAM RIBEIRO DA SILVA

ISAI4E – INTERVENÇÃO PARA A MELHORIA DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Novo Hamburgo

2020

WILLIAM RIBEIRO DA SILVA

ISAI4E – INTERVENÇÃO PARA A MELHORIA DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do grau de Bacharel em Ciência da Computação pela Universidade Feevale

Orientador: Dra. Marta Rosecler Bez

Novo Hamburgo

2020

WILLIAM RIBEIRO DA SILVA

ISAI4E – INTERVENÇÃO PARA A MELHORIA DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do grau de Bacharel em Ciência da Computação pela Universidade Feevale

APROVADO EM: ___ / ___ / _____

DRA. MARTA ROSECLER BEZ
Orientador – Feevale

NOME DO AVALIADOR 1
Examinador interno – Feevale

NOME DO AVALIADOR 2
Examinador interno – Feevale

Novo Hamburgo
2020

AGRADECIMENTOS

Gostaria de agradecer a todos os que, de alguma maneira, contribuíram para a realização desse trabalho de conclusão, em especial: Minha namorada Michele, que me acompanhou desde a ideia inicial do projeto até sua conclusão. Ao meu professor orientador Daniel, que sempre se mostrou disponível para supervisionar e auxiliar com o desenvolvimento. À minha orientadora professora Marta Bez, que generosamente me acolheu na transição do TC1 para o TC2. Obrigado a todos.

RESUMO

Nos dias atuais, é comum o uso da tecnologia para a otimização e agilidade de processos em um ambiente corporativo. Assim, manter a segurança e integridade de tais processos e suas informações têm se tornado um desafio maior a cada dia devido ao constante aperfeiçoamento das técnicas utilizadas por atacantes. Atualmente, uma das maiores ameaças de segurança aos computadores de uma organização está na forma em que os colaboradores os usam. Comportamentos como falta de informação, negligência, indiferença e apatia podem estar presentes e contribuir para tais ameaças. O presente trabalho tem como objetivo propor uma intervenção abordando a conscientização de segurança da informação, mensurando melhorias de forma quantitativa. Tal intervenção se deu por forma de treinamento/*workshop*, possibilitando que a evolução e medição de melhorias fossem documentadas. Os *workshops* aconteceram após a aplicação de um questionário em uma amostra de voluntários, seguido de novo questionário. Os resultados foram medidos através de comparação entre as respostas dos questionários aplicados antes e depois dos *workshops*. A pesquisa, de natureza aplicada, foi executada com procedimento quase-experimental. Os resultados mostraram que houveram melhorias em todas as áreas de foco do estudo, e que existe uma alta correlação positiva entre o conhecimento em uma área de estudo e o comportamento que um indivíduo exerce. Dessa forma, concluiu-se que a intervenção é capaz de influenciar positivamente o nível de conscientização em segurança da informação de indivíduos.

Palavras-chave: Segurança da informação, conscientização, treinamento, intervenção, questionário, ISAI4E.

ABSTRACT

Nowadays, it is common to use technology to optimize and streamline processes in a corporate environment. Thus, maintaining the security and integrity of such processes and their information has become a greater challenge every day due to the constant improvement of the techniques used by attackers. Currently, one of the biggest security threats to an organization's computers is in the way employees use them. Behaviors such as lack of information, neglect, indifference and apathy can be present and contribute to such threats. This study aims to propose an intervention addressing information security awareness, measuring improvements in a quantitative way. The intervention was applied using training/workshop, allowing the evolution and measurement of improvements to be documented. The workshops took place after a questionnaire was applied to a sample of volunteers, followed by a new questionnaire. The results were measured by comparing the responses to the questionnaires, applied before and after the workshops. The research, of an applied nature, was carried out with a quasi-experimental procedure. The results showed improvements in all focus areas of the study, and that there is a high positive correlation between the knowledge in an area of study, and the individual's behavior. Thus, it was concluded that the intervention is able to positively influence the level of awareness of individuals' information security.

Keywords: Information security, awareness, training, intervention, questionnaire.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CSI	Conscientização em Segurança da Informação
KAB	*Knowledge, Attitude and Behaviour*
SI	Segurança da Informação
HAIS-Q	*Human Analysis Information Security Questionnaire*
ASTUTE	*Assess Security Training Effectiveness*

SUMÁRIO

1 INTRODUÇÃO

Antigamente, ao tratar aspectos de proteção e segurança de ativos e informações no âmbito empresarial, entendia-se que os problemas pertinentes a esses aspectos costumavam ser abordados sob um ponto de vista mais técnico e operacional. Contudo, devido às novas necessidades da segurança da informação (SI), estudos apontam uma atenção especial das lideranças para com os comportamentos de seus colaboradores, de forma a avaliar e observar como estes podem influenciar tais problemas (SOOMRO; SHAH; AHMED, 2016).

De forma complementar, devido à maior segurança contra ataques remotos dedicada aos servidores das organizações, a fim de ganhar acesso à uma rede, atacantes têm direcionados seus vetores de ataques para os colaboradores das empresas, uma vez que as estações de trabalho comumente apresentam mais vulnerabilidades do que servidores. Documentos em PDF são regularmente utilizados em investidas contra usuários, visto que ainda existe um consenso de que a plataforma é segura e uma alternativa adequada para outras aplicações, como Microsoft Word (BRANDIS; STELLER, 2012).

Assim, compreende-se que problemas relacionados a SI não podem ser resolvidos apenas com soluções técnicas, uma vez que muitos dos mesmos são provenientes de falha humana (PARSONS et al., 2014a). Como apontado por Gundu, Flowerday e Renaud (2019), negligenciar a eficiência de treinamentos pode expor a organização aos seguintes problemas:

1. Dar continuidade em campanhas de Conscientização de Segurança da Informação (CSI) defeituosas;
2. Diminuir o nível de CSI dos colaboradores;
3. Ter a falsa impressão de que os colaboradores estão cientes dos perigos que correm;
4. Ter a falsa impressão de que futuras campanhas de CSI não são necessárias.

Este estudo objetiva mensurar, a partir de um questionário, o conhecimento em SI por parte das pessoas/colaboradores, e aplicar uma intervenção em formato de *workshop* para abordar a CSI, e tem especificamente os seguintes objetivos:

- Analisar estudos que abordam a conscientização de segurança da informação;
- Identificar as principais lacunas na conscientização de segurança da informação;
- Elaborar um questionário de nivelamento de conscientização;

- Elaborar um treinamento para a conscientização de segurança da informação;
- Aplicar o questionário no grupo voluntário;
- Aplicar o treinamento no grupo voluntário;
- Aplicar o questionário novamente em uma amostra do grupo.

Ademais, posteriormente ao *workshop*, mensurar e documentar novamente o conhecimento dos participantes a fim de validar a intervenção. Portanto, este estudo é norteado pela seguinte questão de pesquisa: "Como capacitar pessoas/colaboradores de modo a desenvolver conhecimentos específicos da área de SI que possam contribuir com a cultura de segurança e privacidade no âmbito empresarial?".

O referencial teórico do estudo, presente no capítulo 2, visa apresentar os temas que tangem a CSI. Dentre estes, principalmente os conceitos gerais de CSI, quais aspectos compõem o escopo de uma campanha de CSI e como medir seu sucesso e tipos e categorias de intervenções que, comumente, são adotadas por organizações. Ao final do capítulo, são abordadas as implicações em CSI, isto é, tipos de falhas cometidas, fatores que influenciam o usuário, problemas enfrentados pelas organizações ao implementar uma campanha de CSI e motivos pelos quais tais campanhas falham.

Adiante, no capítulo 3, são apresentados descritivamente 2 trabalhos correlatos que abordaram intervenções mensurando o nível de CSI utilizando dois métodos diferentes. O primeiro utilizou o HAIS-Q, mesmo questionário que o presente estudo utilizou. O segundo, utilizou o ASTUTE, uma ferramenta capaz de testar se um determinado treinamento é eficiente na melhoria da CSI. Ainda no capítulo 3, uma tabela compara as ações tomadas em diferentes estudos com as ações do presente estudo.

O capítulo 4 apresenta a coleta de dados através de questionário *online*, a formulação de conteúdo para o *workshop*, assim como a coleta e organização das turmas de participantes, tabulação e organização dos dados, e análise estatística e conclusão dos resultados.

Finalmente, no capítulo 5, apresenta-se a conclusão e limitações do presente estudo, assim como ideias para futuros estudos.

2 METODOLOGIA DE PESQUISA

Este trabalho teve como objetivo propor uma intervenção em formato de treinamento/*workshop* para abordar a CSI e visou responder a seguinte questão de pesquisa: "Como capacitar pessoas/colaboradores de modo a desenvolver conhecimentos específicos da área de Segurança da Informação que possam contribuir com a cultura de segurança e privacidade no âmbito empresarial?". Em sua natureza, a pesquisa foi definida como aplicada, visto que, segundo Prodanov e Freitas (2013), a pesquisa aplicada objetivou gerar conhecimentos para a aplicação prática dirigida a solução de prolemas específicos.

Foi realizada uma revisão de literatura para identificar as principais lacunas na conscientização dos aspectos que afetam a Segurança da Informação em ambientes corporativos. Além disso, em seguida, foi elaborado um questionário e um treinamento a serem aplicados em um grupo formado por voluntários que ocupem cargos em ambientes corporativos e executem suas tarefas diárias em computadores. Para a coleta de dados da revisão da literatura, foram realizadas pesquisas nas bases de dados *Science Direct*, IEEE, *Springer* e ACM. Os descritores que foram utilizados nas bases eram "*information security*", "*awareness*" e "*enterprise*", sendo possível adicionar novos descritores para refinar os resultados. Além disso, os artigos científicos foram pesquisados utilizando filtros como ano de publicação, autor, idioma, relevância, etc.

A próxima etapa da pesquisa, foi a leitura dos resumos e conclusões dos artigos científicos obtidos nas bases de dados. Após o entendimento de que os mesmos tinham relevância para a pesquisa, foi feita a leitura completa dos artigos. Subsequentemente, de forma qualitativa, foram documentados os resultados e conclusões obtidas nos artigos estudados como, por exemplo, lacunas, dificuldades, limitações e etc. Tais resultados foram utilizados de modo que um plano de intervenção pode ser construído e, posteriormente, implementado.

O plano de intervenção constituiu no desenvolvimento de um *workshop* a ser apresentado a um grupo de voluntários. A escolha dos voluntários se deu por conveniência. O *workshop* elaborado foi apresentado em dois momentos. No primeiro momento com 20 alunos do curso de sistema de informação e ciência da computação da universidade Feevale com a duração de duas horas. E o segundo, composto por 8 trabalhadores, com duração de duas horas. O questionário aplicado foi dividido em duas páginas, a primeira com perfil dos respondentes, e a segunda com perguntas traduzidas e adaptadas do formulário HAIS-Q de Parsons et al. (2014b). O mesmo questionário foi aplicado antes e depois da intervenção.

De forma quantitativa, os resultados dessa pesquisa foram tabelados e analisa-

dos, de maneira que fosse possível medir se o nível de conscientização em Segurança da Informação sofreu alteração. Tal intervenção caracterizou o procedimento como Quase-Experimental, dado que o presente trabalho constituiu uma classe de estudos de natureza empírica sem um controle completo do ambiente e sem randomização de amostra participante e grupo de controle (CAMPBELL; STANLEY, 1979).

A figura 1 apresenta, destacado, o tipo de pesquisa e suas características.

Figura 1: Tipo e características do estudo

Tipo de Pesquisa			Características		
Quanto à Natureza	Quanto à Forma de Abordagem do Problema	Quanto aos Fins da Pesquisa	Quanto aos Procedimentos	Gerais	Tipos de instrumento
BÁSICA	QUANTITATIVA	EXPLORATÓRIA	Bibliográfica	- Base em material já elaborado	Fontes Bibliográficas
			Documental	- Materiais que não receberam tratamento analítico ou podem ser reelaborados - Efeitos de variável – formas de controle	Fontes Secundárias de dados
APLICADA	QUALITATIVA	DESCRITIVA	Experimental	- Verificar a relação entre variáveis	Plano da pesquisa – Manipulação de condições e observação dos efeitos produzidos
			Quase-Experimental		
			Ex-Post-Facto	- Conhecer Comportamento Interrogação Direta	Observação, questionário e entrevistas
			Levantamento	- Idem levantamento – um grupo ou uma comunidade - Estudo aprofundado de um ou poucos objetos	Questionário, entrevista e formulário
		EXPLICATIVA	Estudo de Campo		Variados - Questionário, entrevistas, formulários e observação
			Estudo de caso		Várias técnicas

Fonte: do autor

O questionário utilizou escala Likert de 5 pontos, sendo disponibilizado aos respondentes pela ferramenta *Google Forms*. Para a análise, foi utilizada a ferramenta *Microsoft Excel*. Neste, utilizou-se o coeficiente de correlação de Pearson (HINKLE; WIERSMA; JURS, 2003).

3 REFERENCIAL TEÓRICO

Este capítulo visa apresentar temas que tangem a CSI e será desenvolvido em subdivisões que detalham o conceito geral de CSI, ações tomadas em campanhas e intervenções de CSI e implicações enfrentadas por organizações ao implementar tais intervenções.

3.1 CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

O termo "conscientização de segurança da informação" é usado para referenciar o estado em que usuários em uma organização estão comprometidos com as orientações de segurança. Conscientização em SI é de crucial importância, já que técnicas de segurança ou procedimentos podem ser mal utilizadas, mal interpretadas ou não utilizadas pelos colaboradores de uma organização, e, portanto, perdendo totalmente seu propósito.

Dessa forma, um nível maior de conscientização em uma organização deve minimizar as falhas cometidas pelos usuários ou até mesmo mitigá-las, além de maximizar a eficiência das técnicas de segurança e procedimentos de um ponto de vista do usuário final. Para alcançar estes objetivos, em um nível organizacional, é importante identificar, quantificar e entender os motivos pelos quais os erros humanos acontecem. Assim, isto deve ser feito sistematicamente, ao estabelecer um programa baseado em um *framework* (SIPONEN, 2000).

Alguns dos passos a serem seguidos incluem:

- Identificar o escopo, metas e objetivos do programa;
- Selecionar a equipe que irá aplicar o treinamento;
- Selecionar o público-alvo;
- Motivar a liderança e colaboradores;
- Administrar, manter e avaliar o programa;

Também, em cada passo supracitado, deve-se criar e aplicar mecanismos de medição de avaliação e *feedback*, a fim de manter-se sempre uma cultura de evolução e melhoria contínua (SIPONEN, 2000).

O sucesso de uma campanha de CSI, conforme Wilson e Hash (2003), é constituído por:

- O desenvolvimento de uma política de segurança que reflita as necessidades do negócio da organização e quais os riscos envolvidos;

- A disseminação das responsabilidades dos usuários nos quesitos que tangem a segurança e estabelecer processos para revisar e monitorar a campanha. A campanha deve atingir todos os níveis da organização, sendo que o esforço da gerência, geralmente, irá determinar a eficiência da conscientização e treinamentos (WILSON; HASH, 2003).

A partir disso, entende-se que a existência de um programa de conscientização é crucial pois ela é o veículo utilizado para transmitir as informações que todos os usuários, funcionários e gerentes precisam. Este veículo somente será eficiente se o material e os métodos utilizados forem interessantes, atuais e simples de serem seguidos. Conteúdos impessoais e genéricos possivelmente serão tratados como apenas mais um material obrigatório (WILSON; HASH, 2003).

Como riscos e ameaças mudam frequentemente, o processo de CSI precisa também ser dinâmico, e, consequentemente, deve ser atualizado constantemente. No intuito de manter seus usuários atualizados, esses programas devem ser parte da cultura organizacional. Programas consistentes e relevantes são a chave do sucesso no que se refere a CSI. A percepção de segurança, juntamente com a percepção dos métodos utilizados por atacantes, tem uma participação importante na tarefa de reduzir os riscos de falhas de segurança digital (ALLAM; FLOWERDAY; FLOWERDAY, 2014). Conforme Furnell e Thomson (2009), a cultura de SI é um aspecto da organização que, por vezes, age no inconsciente, tem forte influência sobre o comportamento da equipe e tem efeito positivo na SI.

3.2 AÇÕES DE CONSCIENTIZAÇÃO

A fim de melhorar o nível de CSI, as campanhas de conscientização e intervenções são promovidas pelas empresas através de diversos tipos de ações. Com o intuito de reunir informações sobre essas ações, o estudo de Fertig e Schütz (2020) apresenta uma revisão de literatura sobre os assuntos relacionados nos últimos 20 anos. Nesse estudo, os autores discutem 34 pesquisas, que, ao serem analisadas, geraram 9 diferentes categorias, conforme apresentado na Tabela 1.

Tabela 1: Categorias de Intervenção

Categoria	Número de Artigos Encontrados
Questionário e Enquetes	16
Questionários baseados no modelo KAB	13
Entrevistas	3
Observação	1
Monitoramento e métricas	3
Referência	1
Teoria da razão fundamentada	1
Questionário e teste de comportamento	2
Governança de senhas	2

Fonte: do autor

Algumas publicações foram mapeadas em múltiplas categorias, caso assim se encaixassem. Adicionalmente, Fertig e Schütz (2020), observaram que 31 dos 34 trabalhos analisados utilizaram algum tipo de questionário. Contudo, alguns destes também empregavam algum outro tipo de método como teste de comportamento, ou comparação por referência. Posterior à indexação dos trabalhos em categorias, concluiu-se que cerca de 40% dos mesmos, totalizando 13 estudos, eram questionários baseados no modelo *Knowledge, Attitude and Behaviour* (KAB).

O modelo KAB foi proposto por Kruger e Kearney (2006), onde um protótipo para medir a CSI foi desenvolvido. No estudo, a CSI foi dividida em três fatores: Conhecimento (K), Atitude (A) e Comportamento (B). A ideia aponta que o conhecimento, assim como as crenças do usuário, gera influência no comportamento. As perguntas presentes no questionário são separadas entre diferentes áreas da segurança, como senhas, e-mail e engenharia social. Esse questionário é amplamente utilizado na literatura, como nos estudos de Parsons et al. (2014a), Khan et al. (2011), Gundu, Flowerday e Renaud (2019), Kusumawati (2018), entre outros. Contudo, críticas apontam que o mesmo é cientificamente fraco (FERTIG; SCHÜTZ, 2020).

Na categoria Entrevistas, Parsons et al. (2014b) conduziram um questionário baseado no modelo KAB. Além disso, os autores investigaram as vulnerabilidades em CSI causadas por humanos em três agências governamentais da Austrália. Adicionalmente, na categoria Observação, Marks e Rezgui (2009) analisaram os colaboradores e utilizaram a informação obtida para mensurar o nível de CSI. Ademais, na categoria Monitoramento e Métricas, os autores relataram que, nestas intervenções, as informações foram coletadas ao acompanhar e-mails, relatórios, redes, ou manualmente pelo time de segurança da organização. A partir disso, as métricas coletadas foram: número de chamadas ao departamento de TI; número de e-mails de *phishing*; número de acessos a páginas internas (intranet); e número de acessos a páginas não autorizadas.

De forma complementar, Gardner e Thomas (2014) também apontaram outras métricas para as ações de conscientização, como o número de documentos sensíveis deixados em áreas públicas e o número de colaboradores usando suas credenciais fora das áreas da organização.

Scholl, Leiner e Fuhrmann (2017), utilizando-se de comparação por referência, ou *benchmarking*, tentaram compreender a eficácia dos métodos usados em programas de CSI e ajudar as organizações a encontrar os melhores métodos a partir do perfil da empresa. O estudo indicou os principais métodos de medida de eficiência de programas de conscientização. Além disso, mostrou as dificuldades encontradas pelas organizações ao implementar programas de SI, tais como resistência dos colaboradores, financiamento e complexidade. Já Khan et al. (2011), na avaliação dos programas de conscientização, implementaram o modelo KAB e o estenderam utilizando as teorias de ação fundamentada e do comportamento planejado. A teoria do comportamento planejado menciona que uma mudança em um comportamento apenas ocorre caso haja a intenção de uma pessoa, enquanto que a teoria da ação planejada diz que uma intenção apenas pode ser modificada caso as normas sociais também sejam, (KHAN et al., 2011). Adiante, em questionário e teste de comportamento, os artigos propuseram que apenas testes de conhecimento não eram suficientes para determinar a CSI. Também, que testes de comportamento devem ser aplicados ao invés de questionar os participantes sobre seus comportamentos (FERTIG; SCHÜTZ, 2020).

Ao tratar de governança de senhas, Wolf, Haworth e Pietron (2011) discutem uma intervenção nas políticas de senhas em uma organização. As senhas dos participantes dessa pesquisa foram auditadas a fim de verificar se estão de acordo com as definições estabelecidas por instituições de ensino. Os autores apresentam que esta é uma ação importante nos programas de conscientização e os resultados do seu estudo mostraram progresso em todas as intervenções, que foram basicamente realizadas por e-mail.

Segundo Bauer, Bernroider e Chudzikowski (2013), canais internos de uma organização para a coleta de informações e aplicação de medidas de segurança podem incluir abordagens convencionais, abordagens lideradas por instrutores e abordagens *online*. As abordagens convencionais incluem jornais internos, panfletos, pôsteres, copos de café personalizados, etc. Já as abordagens lideradas por instrutores são, comumente, mandatórias para os colaboradores e tocam informações de conformidade e governança. Por sua vez, abordagens *online* são implementadas via internet e intranet, e, usualmente, distribuem alertas, e-mails, e repositórios contendo informações sobre comportamento seguro. Bauer e Bernroider (2017) relatam que o uso dessas abordagens pode melhorar substancialmente a conscientização e reduzem os comportamentos que levam a riscos de segurança.

O uso de *workshops* como ação de conscientização também é de grande valia para a promoção dos conteúdos relacionados. Para Albrechtsen e Hovden (2010) o uso de

workshops pode mudar as atitudes dos colaboradores relacionadas à SI. Em seu estudo, os autores utilizaram os *workshops* em um formato de fórum aberto, onde todos os participantes poderiam expressar suas opiniões e visões sobre o tópico da CSI. Posteriormente, perguntas contendo situações de possível risco foram apresentadas ao grupo como forma de identificar as visões e maneiras de superar esses riscos fornecidas pelos participantes. Nesse sentido, entende-se que, para medir se o nível de CSI sofreu melhorias, pode ser aplicado um teste com perguntas relacionadas a SI para um grupo de participantes do *workshop* como forma de avaliar qualitativamente as respostas. Esse teste, segundo os autores, deve conter temas de conscientização e comportamento e deve permitir respostas em uma escala para que seja possível uma melhor mensuração das percepções dos participantes.

As ações presentes nos programas de conscientização estão diretamente relacionadas ao comportamento. O comportamento consciente ao lidar com informações sensíveis é uma abordagem efetiva quando se trata de reduzir riscos. Quando um usuário recebe um e-mail suspeito o solicitando que altere seu usuário e senha, a conscientização e conhecimento sobre a prática de *phishing* enviam um aviso para o seu cérebro. Dessa forma, o usuário irá começar a perceber as consequências de se alterar a senha através de um e-mail. Geralmente, políticas de segurança digital em ambientes corporativos instruem seus colaboradores a alterarem suas credenciais apenas em sites oficiais, portanto, os usuários não devem sequer responder à estes e-mails. Em uma organização onde todos os colaboradores respeitam as políticas de SI, normas subjetivas, isto é, normas que são bem aceitas pela maioria da equipe e, consequentemente, forçam os demais a aceitarem também, podem ser um fator positivo em assegurar comportamentos seguros. Adicionalmente, as experiências passadas dos usuários em aspectos de segurança, juntamente com seu engajamento nas campanhas os ajuda a serem mais cautelosos em condutas que podem levar a falhas de segurança (SAFA et al., 2015).

Por fim, as ações podem conter também, de acordo com Herath e Rao (2009), itens de punição e pressão quanto às políticas organizacionais de SI. Comportamentos intrínsecos e externos afetam as ações dos colaboradores em relação às normas e conformidades. Pressões externas, causadas por normas e a pressão de grupo, influenciam a conduta dos usuários. Além disso, penalidades tem um efeito significante nos comportamentos que tangem a SI. Segundo Stanton et al. (2005), promover as boas atitudes, ao mesmo tempo em que se restringe às más, pode ser uma política eficiente para se obter um melhor cenário de segurança nas organizações.

3.3 IMPLICAÇÕES EM CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Atualmente, empresas de todos os segmentos utilizam o advento da tecnologia para a realização de suas tarefas diárias. Seus colaboradores, consequentemente, acabam por manusear informações sensíveis ou confidenciais em diversas ocasiões. Dessa forma, as organizações podem apresentar dificuldades para manter seus processos de segurança eficientes, visto que, cada vez mais, os atacantes têm aperfeiçoado suas técnicas (MIRAGLIA; CASENOVE, 2016).

Comumente, as falhas de segurança ocorrem por dois motivos: falhas técnicas e falhas humanas. Nas falhas técnicas, atacantes procuram por vulnerabilidades em um sistema, a fim de ganhar acesso às suas informações, escalar privilégios, negar seus serviços, etc. Já nas falhas humanas, os atacantes esperam por um erro cometido pelo usuário a fim de adquirir acesso à um serviço (HAMMOUCHI et al., 2019).

Existem fatores que podem influenciar no comportamento de usuários. Segundo Bada, Sasse e Nurse (2019), esses fatores podem ser classificados como conhecimento, habilidades, experiências pessoais, crenças, e familiaridade com aspectos da SI. Entende-se que a motivação pessoal pode interferir na execução de protocolos de segurança, e por isso pode ser também considerada um fator importante de influência.

Os usuários encontram problemas ao criar hábitos favoráveis para seguir os protocolos de segurança impostos pela organização. Além disso, a forma como os processos de segurança é estabelecida pela empresa pode fazer com que os funcionários tenham dificuldade em segui-la. Quando há muitos passos, os usuários acabam por ficar desmotivados para aprender e aplicar o conhecimento, mesmo tendo consciência de sua importância (BADA; SASSE; NURSE, 2019).

Considerando que processos complicados e não intuitivos irão, eventualmente, levar os usuários a cometerem erros e acharem maneiras de burlar as práticas seguras, práticas de segurança e privacidade devem ser formuladas em uma organização desde o início (COVENTRY et al., 2014). Furnell e Thomson (2009) definem que existe um limite que, se ultrapassado, torna muito difícil ou penoso para usuários manterem-se seguros ao utilizar um sistema – isso é denominado *security fatigue*.

Para Dolan et al. (2010), existem nove fatores críticos que influenciam o comportamento humano:

- **Mensageiro**. Os usuários tendem a ser influenciados por quem transmite a informação;
- **Incentivos**. As pessoas costumam a evitar comportamentos que as façam perder algo;

- **Normalidades**. Há uma influência a partir do que os outros fazem;
- **Padrões**. Os usuários tendem a seguir opções pré-definidas;
- **Saliências**. Os usuários prestam atenção ao que destaca e parece relevante;
- **Preparação**. Ações geralmente são ditadas por dicas do subconsciente;
- **Emoção**. Associações emocionais afetam nossas ações fortemente;
- **Comprometimento**. Os usuários procuram ser consistentes com nossas promessas e retribuir atos e ego, agindo de formas que os fazem se sentir bem consigo mesmos.

Para Humaidi e Balakrishnan (2013), as políticas de segurança não são seguidas por dois motivos: colaboradores não entendem os riscos envolvidos em manusear informações sensíveis de forma incorreta e não entendem as políticas de segurança que devem seguir. Já Bada, Sasse e Nurse (2019) afirmam que mudar comportamentos requer mais do que prover informação sobre riscos e reações comportamentais. Em primeiro lugar, é preciso entender e aplicar o conselho. Segundo, é preciso estar motivado e querer aplicá-lo. Finalmente, é necessário mudar suas atitudes e intenções. Entretanto, a fim de mudar estes comportamentos e possibilitar que as diretrizes de segurança sejam seguidas, faz-se necessário um método que auxilie os colaboradores a compreender os riscos aos quais estão expostos e que os façam seguir e dar atenção às normas de SI estipuladas pela organização.

4 TRABALHOS RELACIONADOS

Cindana e Ruldeviyani (2018) aspiraram, em seu estudo, mensurar a CSI dos colaboradores de uma empresa multinacional, provedora de consultoria, a partir de seu conhecimento, comportamento e atitude em relação às políticas de gerenciamento de SI da organização. O estudo procurou entender como o *framework* HAIS-Q, utilizado para medir o nível de CSI em uma organização, funciona e é conduzido. O HAIS-Q consiste em sete áreas que formam políticas de SI que, comumente, necessitam de ações de colaboradores para que tenham sucesso. Cada área é composta por três subáreas, as quais são mensurados por conhecimento, atitude e comportamento. A coleta de dados ocorreu com 50 colaboradores selecionados aleatoriamente, que receberam as 63 questões impressas em papel. Os resultados, em pontos, foram somados e agrupados em suas respectivas áreas de foco para posteriormente dizer se as políticas de SI afetam o conhecimento, atitude e comportamento dos colaboradores em relação a CSI. Os autores decidiram utilizar o HAIS-Q pois o questionário demonstrou, no estudo de Parsons et al. (2014b), que é capaz de medir a CSI em políticas corporativas eficientemente ao ser aplicado originalmente a 500 colaboradores australianos.

Por fim, a análise das respostas da organização mostrou que as pontuações para CSI e conhecimento foram categorizadas como boas. Dentre todas as áreas de foco, apenas o uso da internet foi considerado mediano.

Gundu, Flowerday e Renaud (2019), mencionaram em seu estudo que comportamentos relatados pelos próprios participantes em campanhas de CSI, embora sejam positivos, geralmente são influenciados pelos participantes e podem não refletir a realidade. Portanto, os autores formularam e testaram o ASTUTE, que significa *Assess Security Training Effectiveness*, um mecanismo eficiente e preciso na medição da CSI em uma organização e que foi implementado com 30 colaboradores de uma empresa de engenharia civil da África do Sul. Os resultados proveram um contexto assim como uma visão geral do nível de CSI dos colaboradores da organização. O estudo concluiu que os colaboradores obtiveram aumentos consideráveis nos níveis de conhecimento e conscientização. Todavia, foi observado também que colaboradores reportam certos comportamentos em pesquisas de CSI, porém, frente a situações em que enfrentam incidentes de segurança, tomam ações diferentes.

A tabela 2 apresenta intervenções executadas em outros estudos, e faz um comparativo com a intervenção executada no presente estudo.

Tabela 2: Ações tomadas por outras intervenções e comparação com o presente estudo

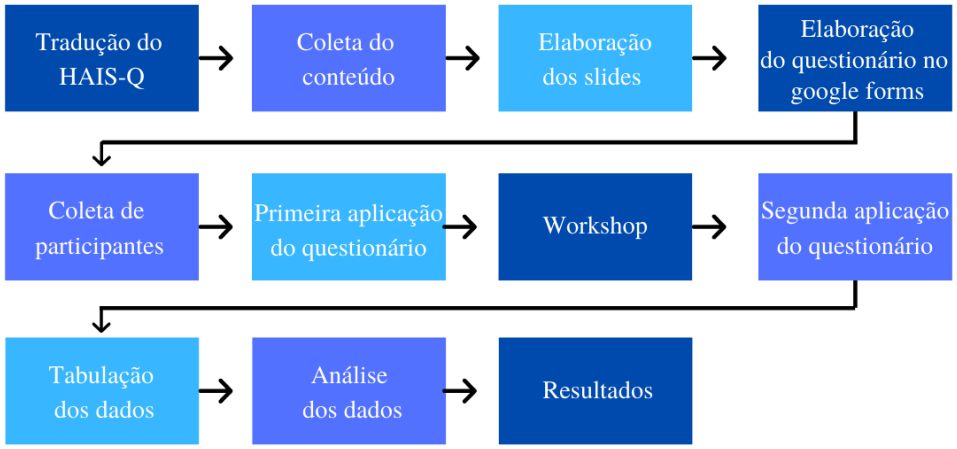
Autor & Ano	Ação de Conscientização	Comentários
Eminağaoğlu, Uçar e Eren (2009)	Melhorar a conscientização na criação e manuseio de senhas	Ação intervém apenas no aspecto de senhas. O presente trabalho agirá em diferentes aspectos que tangem a CSI
Wolf, Haworth e Pietron (2011)	Auditar a complexidade das senhas utilizadas na organização	Ação intervém apenas no aspecto de senhas. O presente trabalho agirá em diferentes aspectos que tangem a CSI
Boujettif e Wang (2010)	*Workshops* onde os próprios colaboradores geram o material de estudo	Intervenção focou as preferências dos participantes quanto à modelos de intervenções. O presente trabalho especificamente almeja mensurar resultados de uma intervenção de CSI
Scholl, Leiner e Fuhrmann (2017)	Compreender a eficiência dos métodos de CSI empregados em organizações	Estudo apenas aponta pontos fortes e fracos de métodos de CSI. O presente trabalho visa implementar um *workshop* apresentando pontos que tangem a SI e, a partir dos resultados, verificar a eficiência do mesmo
Alotaibi et al. (2016)	Pesquisa online para identificar o nível de CSI da população da Arábia Saudita	O estudo apenas mediu o nível da população, sem promover um acompanhamento posteriormente. O presente estudo medirá o nível de CSI mediante questionário antes e depois da intervenção, a fim de medir a eficiência do *workshop* implementado

Fonte: do autor

5 COLETA E ANÁLISE DE DADOS

Neste capítulo, será explicado como o processo de coleta e análise de dados, a formulação de conteúdo e a apresentação dos *Workshops*/*Webinars* aconteceram. As etapas do estudo são ilustradas na Figura 2.

Figura 2: Etapas do Estudo



Fonte: do autor

5.1 TRADUÇÃO DO HAIS-Q

A primeira etapa, ao decidir que um questionário deveria ser usado para medir o nível de CSA dos participantes, foi comparar as vantagens de se usar um questionário já existente contra as vantagens de se criar um questionário completamente novo. Posteriormente, ao revisar diferentes questionários na *web*, verificou-se que o questionário de Parsons et al. (2014a) era completo, cobrindo todas as áreas de uso de um computador em um ambiente corporativo. Ademais, o HAIS-Q já se provou capaz de medir acuradamente o nível de CSA de participantes em outros estudos, como apontado por Cindana e Ruldeviyani (2018), sejam estes participantes empresários, estudantes ou cidadãos comuns. Dessa forma, a necessidade de se criar um questionário novo para a pesquisa acabou sendo eliminada.

Após a escolha do HAIs-Q, as subáreas e perguntas do questionário foram revisadas a fim de identificar se algumas das mesmas estavam fora do contexto da pesquisa e, dessa forma, se havia a necessidade de eliminá-las. Foi decido que todas as subáreas e perguntas eram relevantes e deveriam ficar na versão final do questionário, pois tangenciavam todos

os contextos em que um colaborador de uma empresa se encontra no seu dia-a-dia de trabalho.

Contendo todas as perguntas, áreas e subáreas do questionário, iniciou-se o processo de tradução e localização das mesmas. Majoritariamente, a tradução direta das perguntas manteve o contexto, sobrando poucas perguntas onde a localização, ou seja, a utilização de diferentes termos em relação a tradução direta a fim de atender as necessidades culturais dos participantes, foi utilizada.

5.2 COLETA DE CONTEÚDO E ELABORAÇÃO DOS SLIDES

Ao iniciar a coleta de conteúdo, era sabido que o mesmo deveria abranger todas as subáreas do questionário. Além disso, decidiu-se que fontes da *web* como blogs de tecnologia, sites de soluções de SI, *wikis*, entre outros, seriam priorizadas sobre artigos científicos, visto que estes tendem a ser muito complexos e direcionados para a academia, que não se encaixa no contexto dos participantes. Ademais, o conteúdo disponível na web comumente é escrito de forma simples e de fácil consumo, contrastando com o conteúdo encontrado em artigos. Os sites, *blogs* e *wikis* utilizadas neste estudo tiveram seu conteúdo revisado pelo autor e pela orientadora a fim de verificar a qualidade e confiança dos mesmos. Em geral, o material coletado visou apontar como evitar os riscos que determinadas situações vivenciadas pelos participante em seus ambientes de trabalho podem trazer, além de boas práticas de segurança.

Feita a revisão do conteúdo, utilizou-se o site Canva para a elaboração dos 25 slides que, posteriormente, foram apresentados nos *workshops*. Os slides foram projetados de forma a conter o mínimo de descrições possíveis, a fim de serem de fácil entendimento por parte dos participantes. O conteúdo foi distribuído respeitando as áreas e subáreas do questionário. Os slides podem ser encontrados no apêndice A deste trabalho.

5.3 ELABORAÇÃO DO QUESTIONÁRIO

Para a criação do questionário, fez-se uso da plataforma *Google Forms*, aplicativo da empresa Google, que permite o compartilhamento, elaboração, e hospedagem de formulários via web. A plataforma ainda permite a opção de garantir a aleatoriedade das questões todas as vezes em que o questionário for respondido. Tal opção foi utilizada no presente estudo, aplicada nos questionários antes e depois do *workshop*. O questionário pode ser encontrado no apêndice B deste estudo. Além disso, existe a opção de gerar links de compartilhamento encurtados, facilitando, assim, o envio para os participantes antes e depois dos *workshops*.

O questionário continha 63 questões, que mediam o nível de conhecimento, atitude e comportamento dos participantes. Além disso, cada pergunta poderia ter um contexto

Positivo, ou Negativo, que ajudavam o participante a entender o propósito de cada questão. Dessa forma, utilizou-se a escala *Likert*, com cinco pontos, para a coleta de respostas. As opções de resposta foram (1)-Discordo plenamente, (2)-Discordo parcialmente, (3)-Não concordo nem discordo, (4)-Concordo Parcialmente e (5)-Concordo plenamente.

5.4 COLETA DE PARTICIPANTES

Ao planejar o presente estudo, visou-se iniciar uma campanha de CSI em empresas locais com palestras, material informativo, brindes, *workshops* presenciais, entre outros. Mediante a situação da pandemia de Covid-19, a estratégia para a campanha precisou ser modificada, tornando todas as interações com os participantes completamente *online*. Definiu-se, também, que a população de participantes dos *workshops* deveria ser, preferencialmente, composta por trabalhadores que possuem contato diário com computadores na realização de suas tarefas, porém, que não estejam inseridos no contexto de CSI diretamente.

5.5 APLICAÇÃO DO QUESTIONÁRIO E *WORKSHOP*

Inicialmente, com o propósito de teste, aplicou-se o questionário com 9 voluntários, que não passaram pelo *workshop*. Visto que o questionário foi adaptado e traduzido para a língua portuguesa, o intuito da aplicação inicial era verificar o tempo médio de resposta e coletar possíveis falhas ou dúvidas que poderiam ocorrer durante a intervenção. Concluiu-se, então, mediante retorno positivo dos participantes, que o questionário estava apto para ser utilizado nos *workshops* que estariam por vir. Nesta ocasião, não se mediu o nível de CSI dos participantes, visto que este não era o intuito do teste.

Adiante, com o questionário validado e as turmas de participantes completas, iniciou-se, então, a aplicação dos questionários e *workshops*. A primeira aplicação ocorreu em uma turma com 20 alunos de uma universidade. Foi solicitado aos participantes que escolhessem um codinome para a identificação, visto que a pesquisa era anônima. O mesmo codinome deveria ser utilizado na segunda aplicação do questionário, logo após o término do *workshop*. Depois, em outra data, o *workshop* foi aplicado em uma outra turma contendo 8 participantes, que também responderam ao questionário antes e depois da intervenção. Posteriormente, os dados coletados das respostas seriam tabelados e analisados.

O questionário, aplicado utilizando a ferramenta *Google Forms*, consistia em duas páginas. A primeira página era responsável por coletar dados demográficos, como codinome, idade, sexo, profissão e escolaridade. A página também questionava se o participante usava um computador para a realização em suas tarefas diárias no trabalho. A segunda página continha as 63 perguntas relacionadas a CSI, divididas em 7 áreas de foco, que, por

sua vez, eram também divididas em 3 subáreas. A divisão de áreas, subáreas, tais quais as questões aplicadas, podem ser observadas nas tabelas 3, 4 e 5. As questões contendo um símbolo de @ indicam que a mesma tinha um contexto nocivo, ou seja, contemplaram pontos negativos caso o participante concordasse com a afirmação.

No total, 38 pessoas responderam ao questionário, das quais, 29 participaram do *workshop*. Dentre os participantes que estiveram presentes na intervenção, 15 produziram respostas válida, isto é, as respostas não foram descartadas por qualquer motivo. 14 respondentes tiveram as respostas descartadas por não terem adicionado o mesmo codinome antes e depois da participação do *workshop*, impossibilitando a identificação, e, consequentemente, a medição do nível de CSI antes e depois da aplicação.

Coletados na primeira página do questionário, os dados demográficos indicaram que 60% dos participantes eram compostos por homens, enquanto que 40% eram mulheres. 20% continham entre 17 e 24 anos, 33% entre 25 e 34 anos, 27% entre 35 e 44 anos e 20% entre 45 a 54 anos. 87% requerem o uso de um computador ou dispositivo móvel para a realização de suas tarefas diárias, 13% não fazem uso destas ferramentas. Nenhum participante estava desempregado no período em que a intervenção ocorreu. 47% dos participantes possui ensino superior incompleto, 13% superior completo, 33% ensino médio completo e 7% são pós graduados. Verificou-se, também, que 47% dos participantes atuam na área de tecnologia da informação, enquanto que os restantes trabalham em áreas diversificadas da indústria, comércio e educação. Os dados demográficos supracitados correspondem apenas a participantes com respostas válidas.

Tabela 3: Questões Aplicadas: Gerenciamento de Senhas, Uso de e-mail, Uso de internet

Subárea	Conhecimento	Atitude	Comportamento
Área de Foco: Gerenciamento de Senhas			
Uso de senhas repetidas	É aceitável utilizar a senha das minhas redes sociais nos acessos do trabalho. @	É seguro utilizar a mesma senha em minhas redes sociais e acessos do trabalho. @	As senhas de minhas redes sociais são diferentes das senhas de meus acessos do trabalho.
Compartilhando senhas	Tenho permissão para compartilhar minhas senhas de trabalho com colegas. @	É uma má ideia compartilhar minhas senhas de trabalho, mesmo que um colega peça.	Eu compartilho minhas senhas de trabalho com colegas.@
Usando uma senha forte	É necessária uma mistura de letras, números e símbolos para senhas de trabalho.	É seguro ter uma senha de trabalho composta apenas por letras. @	Eu uso uma combinação de letras, números e símbolos em minhas senhas.
Área de Foco: Uso de e-mail			
Clicar em links em e-mails de remetentes conhecidos	Posso clicar em qualquer link de e-mail de pessoas que conheço. @	É sempre seguro clicar em links de e-mails de pessoas que conheço. @	Eu nem sempre clico em links de e-mails só porque vêm de alguém que conheço.
Clicando em links em e-mails de remetentes desconhecidos	Não tenho permissão para clicar no link de um e-mail de um remetente desconhecido.	Nada de ruim pode acontecer se eu clicar em um link em um e-mail de um remetente desconhecido. @	Se um e-mail de um remetente desconhecido parecer interessante, eu clico em um link dentro dele. @
Abrindo anexos em e-mails de remetentes desconhecidos	Tenho permissão para abrir anexos de e-mail de remetentes desconhecidos. @	É arriscado abrir um anexo de e-mail de um remetente desconhecido	Eu não abro anexos de e-mail se o remetente for desconhecido para mim.
Área de Foco: Uso de internet			
Baixando arquivos	Tenho permissão para baixar qualquer arquivo no meu computador do trabalho, se me ajudarem a realizar minhas funções. @	Baixar arquivos no meu computador de trabalho pode ser perigoso.	Eu baixo qualquer arquivo em meu computador do trabalho que me ajude a realizar as minhas tarefas. @
Acessando sites duvidosos	Enquanto estou trabalhando, eu não devo acessar alguns sites.	Só porque posso acessar um site no trabalho, não significa que seja seguro.	Ao acessar a internet no trabalho, visito qualquer site que eu quiser. @
Inserindo informações online	Tenho permissão para inserir qualquer informação em qualquer site se isso me ajudar a fazer meu trabalho. @	Se me ajuda a fazer meu trabalho, não importa as informações que coloco em um site. @	Eu avalio a segurança dos sites antes de inserir informações.

Fonte: adaptado de Parsons et al. (2014b)

Tabela 4: Questões Aplicadas: Uso de Redes Sociais e Notebooks & Dispositivos Móveis

Subárea	Conhecimento	Atitude	Comportamento
Área de Foco: Uso de redes sociais			
Configurações de privacidade da rede social	Devo revisar periodicamente as configurações de privacidade das minhas redes sociais.	É uma boa ideia revisar periodicamente as configurações de privacidade das minhas redes sociais.	Eu não reviso periodicamente as configurações de privacidade das minhas redes sociais. @
Considerando as consequências	Não posso ser demitido por algo que posto nas redes sociais. @	Não tem problema postar coisas nas redes sociais que eu normalmente não diria em público. @	Eu não posto algo nas redes sociais antes de considerar as consequências negativas.
Postando sobre meu trabalho	Posso postar o que quero sobre o meu trabalho nas redes sociais. @	É arriscado postar certas informações sobre meu trabalho nas redes sociais.	Eu posto tudo o que quero sobre meu trabalho nas redes sociais. @
Área de Foco: Notebooks & dispositivos móveis			
Protegendo dispositivos móveis fisicamente	Quando trabalho em um local público, tenho que manter meu laptop comigo o tempo todo.	Ao trabalhar de um local público, é seguro deixar meu notebook sem supervisão por alguns minutos. @	Quando trabalho em um local público, deixo meu laptop sem supervisão. @
Envio de informações confidenciais via Wi-Fi	Eu tenho permissão para enviar arquivos confidenciais de trabalho por meio de uma rede Wi-Fi pública. @	É arriscado enviar arquivos confidenciais de trabalho usando uma rede Wi-Fi pública.	Eu envio arquivos confidenciais de trabalho utilizando redes Wi-Fi públicas. @
Cuidados com espiadas	Ao trabalhar em um documento confidencial, devo garantir que estranhos não possam ver a tela do meu notebook	É arriscado acessar arquivos confidenciais de trabalho em um laptop se estranhos puderem ver minha tela.	Eu verifico se estranhos não podem ver a tela do meu notebook se estou trabalhando em um documento confidencial.

Fonte: adaptado de Parsons et al. (2014b)

Tabela 5: Questões Aplicadas: Manuseio de Informações e Relato de Incidentes

Subárea	Conhecimento	Atitude	Comportamento
Área de Foco: Manuseio de informações			
Descarte de impressões confidenciais	As impressões confidenciais podem ser eliminadas da mesma forma que as não confidenciais. @	Descartar impressões confidenciais em uma lixeira é seguro. @	Quando impressões confidenciais precisam ser descartadas, eu me certifico de que sejam rasgadas ou destruídas.
Inserindo mídia removível	Se eu encontrar um pendrive na rua, não devo conectá-lo ao meu computador de trabalho.	Se eu encontrar um *pen drive* na rua, nada de ruim pode acontecer se eu o conectar ao meu computador de trabalho. @	Eu não conectaria um pendrive encontrado na rua em meu computador de trabalho.
Cuidado com material impresso	Eu tenho permissão para deixar impressões contendo informações confidenciais em minha mesa durante a noite. @	É arriscado deixar impressões que contêm informações confidenciais na minha mesa durante a noite.	Eu deixo impressões que contêm informações confidenciais na minha mesa enquanto estou ausente. @
Área de Foco: Relato de incidentes			
Relatando comportamento suspeito	Se eu vir alguém agindo de forma suspeita em meu local de trabalho, devo denunciá-lo.	Se eu ignorar alguém agindo de forma suspeita em meu local de trabalho, nada de ruim pode acontecer. @	Se eu visse alguém agindo de forma suspeita em meu local de trabalho, faria algo a respeito.
Ignorando maus comportamento de segurança de colegas	Não devo ignorar o mau comportamento de segurança de meus colegas.	Nada de ruim pode acontecer se eu ignorar o comportamento de segurança insatisfatório de um colega. @	Se eu percebesse que meu colega estava ignorando as regras de segurança, não faria nada. @
Relatando todos os incidentes	Relatar incidentes de segurança é opcional. @	É arriscado ignorar incidentes de segurança, mesmo que eu ache que não sejam significativos.	Se eu notasse um incidente de segurança, eu o relataria.

Fonte: adaptado de Parsons et al. (2014b)

As questões foram aplicadas utilizando uma escala Likert de cinco opções, e contemplavam pontos dependendo das escolhas dos participantes. A relação de respostas e pontuação pode ser observada na tabela 6. Após os participantes terem respondido ao questionário duas vezes, uma antes do *workshop* e uma depois, os resultados foram baixados do *Google Forms* e analisados.

Tabela 6: Relação Resposta x Pontuação

Contexto	Resposta	Pontuação
Positiva	Concordo Plenamente	3
Positiva	Concordo Parcialmente	2
Positiva	Discordo Plenamente	-3
Positiva	Discordo Parcialmente	-2
Negativa	Concordo Plenamente	-3
Negativa	Concordo Parcialmente	-2
Negativa	Discordo Plenamente	3
Negativa	Discordo Parcialmente	2
Positiva	Nem Concordo Nem Discordo	0
Negativa	Nem Concordo Nem Discordo	0

Fonte: do autor

Para se chegar ao valor do coeficiente de acertos, criou-se, utilizando o *software Microsoft Excel*, uma fórmula que testou o contexto da pergunta, juntamente com a resposta do participante, decidindo, dessa forma, qual pontuação deveria ser concedida. Adicionalmente, separando por área de foco, uma segunda fórmula somou a pontuação de todas as respostas enviadas pelos participantes, gerando uma média. Tal método foi escolhido seguindo o estudo de Cindana e Ruldeviyani (2018), o qual valida o mesmo. Ambas as respostas, de antes e depois do *workshop*, foram coletadas a fim de averiguar quais mudanças ocorreram na CSI do participante durante o *workshop*.

$$A = \frac{Q_1 + Q_2 + Q_3 + ... + Q_{135}}{135}$$

Na fórmula acima, A equivale ao valor da média correspondente ao coeficiente de acertos das 135 questões Q pertencentes a uma área de foco. A fórmula se repetiu para todas as 7 áreas de foco, produzindo os resultados mostrados no próximo subcapítulo.

5.6 RESULTADOS

O próximo passo da pesquisa foi tabular e analisar a pontuação coletada dos participantes e averiguar se os *workshops* tiveram efeito na CSI dos mesmos. A tabela 7 mostra os resultados dos questionários, tais quais as melhorias apresentadas. Resultados acima de 2.4 pontos foram considerados bons e tiveram as células pintadas em verde, entre 1.8 e 2.4 pontos foram considerados intermediários, pintados em amarelo. Resultados abaixo de 1.8 pontos foram considerados insatisfatórios e pintados em vermelho.

Tabela 7: Pontuação

Área de Foco	Questionário 1	Questionário 2	Diferença
Gerenciamento de Senhas	2,21	2,53	14,38%
Uso de e-mail	1,94	2,47	27,48%
Uso de Internet	1,14	2,17	89,03%
Uso de Redes Sociais	2,09	2,51	20,14%
Uso de Dispositivos Móveis	2,20	2,66	21,21%
Manuseio de Informações	1,99	2,63	32,34%
Relato de Incidentes	2,07	2,37	14,29%
TOTAL	13,66	17,37	27,10%

Fonte: do autor

A análise dos resultados mostra que todas as áreas de foco abordadas no questionário obtiveram melhorias. 6 das 7 áreas tiveram resultados intermediários na primeira aplicação do questionário, e, majoritariamente, transformaram-se em resultados considerados bons, acima de 2.4 pontos. A pontuação referente ao uso de internet era a única com um resultado considerado insatisfatório, e, após a intervenção, pôde-se observar uma melhoria de 89%, posicionando a área em um resultado considerado intermediário. Apenas duas áreas ficavam abaixo de 2.4 pontos após a intervenção: uso de internet e relato de incidentes.

Analisou-se, também, utilizando o coeficiente de correlação de Pearson, a correlação entre a soma das pontuações de questões relacionadas ao conhecimento das áreas de foco do questionário respondidas por cada participante com a soma das pontuações relacionadas ao comportamento dos usuários em situações relativas às áreas de foco do estudo. O coeficiente ρ de Pearson pode variar entre -1 e 1, e, de acordo com Hinkle, Wiersma e Jurs (2003), deve ser interpretado conforme abaixo.

- 0.9 até 1.00 (-0.90 até -1.00). Correlação positiva ou negativa muito alta
- 0.7 até 0.9 (-0.7 até -0.9). Correlação positiva ou negativa alta
- 0.5 até 0.7 (-0.5 até -0.7). Correlação positiva ou negativa média
- 0.3 até 0.5 (-0.3 até -0.5). Correlação positiva ou negativa baixa
- 0.0 até 0.3 (0.0 até -0.3). Correlação positiva ou negativa insignificante

Concluiu-se que existe uma alta correlação positiva entre as duas áreas, com um valor de $\rho = 0.822$. O valor indica que o conhecimento em uma área de foco do estudo influencia positivamente nas atitudes tomadas pelos indivíduos, adicionalmente, que os participantes comportam-se de acordo com seus conhecimentos nas áreas de foco.

Ao observar-se a nítida melhora na pontuação de CSI dos participantes após o *workshop*, conclui-se que o mesmo é capaz de influenciar positivamente o nível de CSI de indivíduos.

6 CONCLUSÃO

A CSI é a parte da SI que visa conscientizar os usuários sobre os riscos envolvendo o uso de tecnologias, ao passo que tenta engajá-los com as normas, boas práticas e orientações de políticas de SI, sejam essas de uma instituição ou com equipamentos de uso pessoal. A importância da CSI é crucial, visto que auxilia na prevenção de falhas de segurança, influencia na cultura de segurança de uma organização, dentre outros.

O presente estudo apresenta melhorias no nível de CSI de indivíduos que passaram pelos *workshops* da intervenção. O conhecimento em todas as áreas de foco abordadas pelo *workshop* obtiveram melhorias, e 5 das 7 áreas obtiveram pontuações consideradas boas. Também observou-se uma forte correlação positiva entre o comportamento dos participantes e o conhecimento sobre as áreas de foco, indicando que, de fato, os participantes tendem a praticar o que sabem.

Desta forma, o objetivo de executar uma intervenção em forma de *workshop*, medindo melhorias, foi atingido. Assim, respondendo à questão de pesquisa deste trabalho, concluiu-se que através de intervenções em forma de *workshops*, é possível capacitar colaboradores e pessoas de modo a contribuir para a cultura de segurança e privacidade e desenvolver conteúdo e conhecimentos na área de SI. Este achado corrobora o apresentado por Albrechtsen e Hovden (2010), pois, tanto os achados deste TCC quanto dos autores supracitados, encontram respostas positivas e melhorias no nível de CSI após a intervenção.

De forma complementar, o presente estudo tem como principal contribuição a regionalização de uma intervenção em forma de *workshop/webinar* utilizando-se de questionário. Tal temática não foi, até o presente momento, aplicada ou executada no contexto brasileiro ou no idioma português.

Apesar de obter resultados positivos, o estudo teve limitações causadas pela pandemia de Covid-19. Eliminou-se a possibilidade de intervenções físicas em empresas, divulgação de material didático, acompanhamentos com indivíduos participantes, entre outras atividades. Tais atividades, se postas em prática, poderiam ter influenciado no resultado final. As limitações deste estudo deixam oportunidades para possíveis trabalhos futuros, os quais se beneficiariam de encontros presenciais com mais voluntários, produzindo mais dados em parceria com lideranças de empresas.

REFERÊNCIAS

ALBRECHTSEN, E.; HOVDEN, J. Improving information security awareness and behaviour through dialogue, participation and collective reflection. an intervention study. *Computers & Security*, Elsevier, v. 29, n. 4, p. 432–445, 2010. Citado 2 vezes nas páginas 17 e 33.

ALLAM, S.; FLOWERDAY, S. V.; FLOWERDAY, E. Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, Elsevier, v. 42, p. 56–65, 2014. Citado na página 15.

ALOTAIBI, F. et al. A survey of cyber-security awareness in saudi arabia. In: IEEE. *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*. [S.l.], 2016. p. 154–158. Citado na página 22.

BADA, M.; SASSE, A. M.; NURSE, J. R. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*, 2019. Citado 2 vezes nas páginas 19 e 20.

BAUER, S.; BERNROIDER, E. W. From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, ACM New York, NY, USA, v. 48, n. 3, p. 44–68, 2017. Citado na página 17.

BAUER, S.; BERNROIDER, E. W.; CHUDZIKOWSKI, K. End user information security awareness programs for improving information security in banking organizations: preliminary results from an exploratory study. In: *AIS SIGSEC Workshop on Information Security & Privacy (WISP 2013), Milano*. [S.l.: s.n.], 2013. Citado na página 17.

BOUJETTIF, M.; WANG, Y. Constructivist approach to information security awareness in the middle east. In: IEEE. *2010 International Conference on Broadband, Wireless Computing, Communication and Applications*. [S.l.], 2010. p. 192–199. Citado na página 22.

BRANDIS, R.; STELLER, L. Threat modelling adobe pdf: Dsto-tr-2730. *DSTO Formal Reports*, Defence Science and Technology Organisation, Anzac Park West Offices Lambda . . . , n. 2730, 2012. Citado na página 10.

CAMPBELL, D. T.; STANLEY, J. C. *Delineamentos experimentais e quase-experimentais de pesquisa*. [S.l.]: EPU São Paulo, 1979. Citado na página 13.

CINDANA, A.; RULDEVIYANI, Y. Measuring information security awareness on employee using hais-q: Case study at xyz firm. In: IEEE. *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*. [S.l.], 2018. p. 289–294. Citado 3 vezes nas páginas 21, 23 e 30.

COVENTRY, L. et al. Using behavioural insights to improve the public's use of cyber security best practices. *Gov. UK report*, Government Office for Science, 2014. Citado na página 19.

DOLAN, P. et al. Mindspace: influencing behaviour for public policy. Institute of Government, 2010. Citado na página 19.

EMINAĞAOĞLU, M.; UÇAR, E.; EREN, Ş. The positive outcomes of information security awareness training in companies–a case study. *information security technical report*, Elsevier, v. 14, n. 4, p. 223–229, 2009. Citado na página 22.

FERTIG, T.; SCHÜTZ, A. About the measuring of information security awareness: A systematic literature review. In: *Proceedings of the 53rd Hawaii International Conference on System Sciences*. [S.l.: s.n.], 2020. Citado 3 vezes nas páginas 15, 16 e 17.

FURNELL, S.; THOMSON, K.-L. From culture to disobedience: Recognising the varying user acceptance of it security. *Computer fraud & security*, Elsevier, v. 2009, n. 2, p. 5–10, 2009. Citado 2 vezes nas páginas 15 e 19.

GARDNER, B.; THOMAS, V. *Building an information security awareness program: Defending against social engineering and technical threats*. [S.l.]: Elsevier, 2014. Citado na página 17.

GUNDU, T.; FLOWERDAY, S.; RENAUD, K. Deliver security awareness training, then repeat:{Deliver; Measure Efficacy}. In: IEEE. *2019 Conference on Information Communications Technology and Society (ICTAS)*. [S.l.], 2019. p. 1–6. Citado 3 vezes nas páginas 10, 16 e 21.

HAMMOUCHI, H. et al. Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. *Procedia Computer Science*, Elsevier, v. 151, p. 1004–1009, 2019. Citado na página 19.

HERATH, T.; RAO, H. R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, Elsevier, v. 47, n. 2, p. 154–165, 2009. Citado na página 18.

HINKLE, D. E.; WIERSMA, W.; JURS, S. G. *Applied statistics for the behavioral sciences*. [S.l.]: Houghton Mifflin College Division, 2003. Citado 2 vezes nas páginas 13 e 31.

HUMAIDI, N.; BALAKRISHNAN, V. Exploratory factor analysis of user's compliance behaviour towards health information system's security. *Journal of Health & Medical Informatics*, v. 4, n. 2, p. 2–9, 2013. Citado na página 20.

KHAN, B. et al. Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, Academic Journals, v. 5, n. 26, p. 10862–10868, 2011. Citado 2 vezes nas páginas 16 e 17.

KRUGER, H. A.; KEARNEY, W. D. A prototype for assessing information security awareness. *Computers & security*, Elsevier, v. 25, n. 4, p. 289–296, 2006. Citado na página 16.

KUSUMAWATI, A. Information security awareness: Study on a government agency. In: IEEE. *2018 International Conference on Sustainable Information Engineering and Technology (SIET)*. [S.l.], 2018. p. 224–229. Citado na página 16.

MARKS, A.; REZGUI, Y. A comparative study of information security awareness in higher education based on the concept of design theorizing. In: IEEE. *2009 International Conference on Management and Service Science*. [S.l.], 2009. p. 1–7. Citado na página 16.

MIRAGLIA, A.; CASENOVE, M. Fight fire with fire: the ultimate active defence. *Information & Computer Security*, Emerald Group Publishing Limited, 2016. Citado na página 19.

PARSONS, K. et al. Determining employee awareness using the human aspects of information security questionnaire (hais-q). *Computers & security*, Elsevier, v. 42, p. 165–176, 2014. Citado 3 vezes nas páginas 10, 16 e 23.

PARSONS, K. et al. A study of information security awareness in australian government organisations. *Information Management & Computer Security*, Emerald Group Publishing Limited, 2014. Citado 6 vezes nas páginas 12, 16, 21, 27, 28 e 29.

PRODANOV, C. C.; FREITAS, E. C. de. *Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico-2ª Edição*. [S.l.]: Editora Feevale, 2013. Citado na página 12.

SAFA, N. S. et al. Information security conscious care behaviour formation in organizations. *Computers & Security*, Elsevier, v. 53, p. 65–78, 2015. Citado na página 18.

SCHOLL, M.; LEINER, K.; FUHRMANN, F. Blind spot: Do you know the effectiveness of your information security awareness-raising program? In: *Proceedings of the 21st World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017)*. [S.l.: s.n.], 2017. p. 361–366. Citado 2 vezes nas páginas 17 e 22.

SIPONEN, M. T. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, MCB UP Ltd, 2000. Citado na página 14.

SOOMRO, Z. A.; SHAH, M. H.; AHMED, J. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, Elsevier, v. 36, n. 2, p. 215–225, 2016. Citado na página 10.

STANTON, J. M. et al. Analysis of end user security behaviors. *Computers & security*, Elsevier, v. 24, n. 2, p. 124–133, 2005. Citado na página 18.

WILSON, M.; HASH, J. Building an information technology security awareness and training program. *NIST Special publication*, v. 800, n. 50, p. 1–39, 2003. Citado 2 vezes nas páginas 14 e 15.

WOLF, M.; HAWORTH, D.; PIETRON, L. Measuring an information security awareness program. *Review of Business Information Systems (RBIS)*, v. 15, n. 3, p. 9–22, 2011. Citado 2 vezes nas páginas 17 e 22.

.1 APÊNDICE A

Workshop: Segurança da Informação

William Ribeiro
Parte do Trabalho de Conclusão de Curso II
Ciência da Computação
Orientado por Profa. Dra. Marta Bez

Agenda:

- Uso de senhas
- Uso de e-mail
- Uso de internet
- Uso de redes sociais
- Uso de dispositivos móveis
- Manuseio de informações
- Relato de incidentes

1 Uso de senhas

EMPRESAS TENTAM SE DISTANCIAR DO USO DE SENHAS

- Impressão digital
- Imagens
- Reconhecimento facial
- Escaneamento de retina
- Senhas podem ser facilmente roubadas ou descobertas

1 Uso de senhas

FORMAS MAIS COMUNS DE LEMBRAR SENHA:

- Usar mesmas senhas
- Incorporam dados pessoais
- Anotam em post-it

RISCOS:

- Dados pessoais estão disponíveis nas redes sociais (privacidade)
- Hackers conseguem acessar diversas contas com apenas uma sem
- Post-it pode ser facilmente roubado ou fotografado

1 Compartilhar senhas no trabalho

- Falsa impressão de segurança
- Colega realizar uma tarefa

RISCOS

- Colega pode ter um computador vulnerável e vazar a sua senha
- Auditoria torna-se mais difícil
- Ex funcionários

1 Senha forte

Senhas fortes são eficientes para manter outras pessoas fora de suas contas

HACKERS TENTAM BURLAR ESTAS PROTEÇÕES UTILIZANDO:

- Ataques baseados em dicionários
- Engenharia social e informações disponíveis online (redes sociais)
- Ataque de força bruta
- Ataque de Phishing
- Vazamentos de dados

1 Senha forte

PERGUNTAS A SE FAZER:

- A minha senha é longa?
- A minha senha é difícil de adivinhar?
- Possui diferentes tipos de caracteres?
- Possui substituições óbvias? (S3NH4 ao invés de SENHA)
- Eu consigo lembrar da minha senha?
- Eu já usei essa senha antes?

2 Uso de e-mail

E-mails maliciosos tentam se disfarçar como tentativas normais de comunicação.

Servem para persuadir a vítima a baixar e instalar programas no computador.

COMO IDENTIFICAR UM E-MAIL MALICIOSO?

- Eu reconheço quem está mandando este e-mail?
- Estou familiarizado com o conteúdo da mensagem?
- Esta mensagem está pedindo algo?
- Esta mensagem está me oferecendo algo?

2 Uso de e-mail

COMO LIDAR COM UM E-MAIL MALICIOSO:

- Não abra
- Não clique nos anexos
- Se estiver esperando um e-mail, verifique:
  - Se o link está correto
  - Se o link contém "https" no início
- Não encaminhe
- Não clique em links
- Marque como spam
- Bloqueie o remetente

2 Uso de e-mail

SOBRE PHISHING:

- Tipo de ataque que força/persuade o usuário a fornecer informações ou acesso à um sistema.

- Uso de engenharia social para camuflar o ataque como legítimo, causando pânico, medo e forçando a vítima a tomar alguma ação precipitada.

2 Uso de e-mail

TIPOS

- Tradicional
- Direcionado
- Whaling
- Fraude de CEO
- Pharming
- Ataque do "Homem no meio"

3 Uso de internet

Criminosos espalham programas maliciosos na internet.

Alguns sites falsos, imitando um site que você confia, fornecem programas que podem abrir brechas para que atacantes entrem no seu computador.

Antigamente, era uma forma de pregar uma peça em alguém.

Hoje, tentam entrar sem serem percebidos.

3 Uso de internet

BOAS PRÁTICAS:
- Apenas executar programas baixados do site oficial
- Uso de antivírus de qualidade
- Limitar a instalação de programas ao departamento de TI
- Bloquear certos sites
- Reportar sites suspeitos ao departamento de TI

PERIGOS:
- Softwares que mostram soluções milagrosas
- Apontam falsas vulnerabilidades
- Spyware - Monitora e coleta dados dos usuários

3 Uso de internet

Ao atualizar sistema operacional, antivírus, leitor de PDF, sempre manter olho crítico e bom-senso.

Se um site, oferecendo uma solução incrível de graça, parece bom demais para ser verdade, provavelmente é.

3 Uso de internet

Vários sites nos ajudam diariamente

CUIDADOS
- Mesmo sendo confiáveis e gratuitos, não podemos fornecer algumas informações a certos sites.
- Google grava todos os dados que passam por seus serviços
- Grammarly oferece plug-ins instaláveis no navegador e Word
- Sempre ler os termos de uso dos sites e programas

4 Uso de redes sociais

Redes sociais fornecem opções de configuração de privacidade, permitindo bloquear que alguns dados pessoais sejam compartilhados com estranhos ou até mesmo amigos.

Mesmo com essas opções, dados ainda são coletados pela rede social e vendidos ou compartilhados com terceiros.

4 Uso de redes sociais

CONSEQUÊNCIAS

- Propagandas personalizadas
- Rede social fornecer dados dos usuários para o governo
- Aversão a um candidato antes de uma entrevista de emprego
- Análise de crédito por empresas financeiras
- Ajudar candidatos políticos em eleições (Cambridge analítica)
- Permitir que um vigarista cometa fraude de identidade

4 Uso de redes sociais

COMO NOSSOS DADOS PARAM NAS MÃOS DE TERCEIROS:

- Fotos
- Localização
- Comentários
- Curtidas
- Aceitação dos termos de uso (empresas podem ser exageradamente intrusivas)
- Apps de terceiros no FB (como meus filhos se parecerão?)
- Criação de conta do Facebook (e-mail, aniversário, telefone, visão política, orientação sexual, com quem somos casados, quais nossos parentes no site)
- Criação de contas em outros serviços (conectar conta do FB)
- API do Facebook (botão de curtir fora do site)

5 Uso de dispositivos móveis

Coisas que julgamos convenientes podem nos trazer problemas, mesmo quando solucionam alguns de nossos problemas.

RISCOS DO USO DE WIFI SEM SENHA (SPOOFING)

- Enviar ou receber informações confidenciais
- Não utilizar senhas
- Utilizar uma VPN (Virtual Private Network)

5 Uso de dispositivos móveis

O de espaços públicos (coworking) tem se popularizado devido às dinâmicas de trabalho estarem evoluindo nas indústrias.

As empresas estão começando a entender que conseguem ter 100% de aproveitamento de seus colaboradores mesmo estes não estando fisicamente nos escritórios, ou até mesmo no mesmo país.

BOAS PRÁTICAS

- SEMPRE ESTAR JUNTO DE SEU NOTEBOOK E CELULAR
- Escolha um espaço que esteja coberto por câmeras de segurança
- Escolha um espaço que ofereça armários com chave
- Escolha um espaço que proteja a tela de curiosos

6 Manuseio de informações

Lidamos com informações confidenciais, mesmo que não saibamos

- Contratos
- Demonstrativos de pagamento
- E-mails de clientes

"Marcar" documentos com sua classificação correta ao produzi-los

- Nunca deixar documentos importantes "soltos" na mesa ao se afastar
- Guardar em armário com chave
- Levar junto
- Destruir o documento caso não seja mais útil

6 Manuseio de informações

Pen drives são pequenos, fáceis de usar, baratos e portáteis

- Podem ser modificados para infectar automaticamente qualquer computador que se conectarem.
- Outros dispositivos USB como porta-retratos USB e HDs externos também oferecem risco
- Pen drives infectados podem roubar informações diretamente, mesmo se o computador estiver desligado.
- Em segundos, senhas, chaves de criptografia e outros dados podem ser roubados sem que o dono saiba

6 Manuseio de informações

Como proteger?

- Se encontrar um USB na rua, entregue ao departamento de TI da instituição. Se for na rua, jogue no lixo
- Não conecte qualquer pen drive ou dispositivo USB desconhecido no computador para saber quem é o dono
- Faça backup das informações dos seus pen drives
- Criptografe as informações de seus pen drives
- Não use pen drives corporativos em seu computador pessoal e vice-versa
- Desative a execução automática
- Mantenha seu firewall ativado e antivírus atualizado

7 Relato de incidentes

O QUE É UM INCIDENTE?

Violação ou ameaça à segurança de informações, políticas de privacidade ou boas práticas de segurança em uma empresa.

SISTEMA DE COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA PROPORCIONA:

- A circulação de informação importante para a equipe (trends)
- Uma resposta rápida e eficiente aos problemas
- Acesso a uma fonte vasta de conhecimento sobre os problemas
- Facilidade em auditorias
- Análise rápida de possíveis ameaças
- Surgimento de novas boas práticas

7 Relato de incidentes

COMPORTAMENTOS SUSPEITOS:

- Por colegas
- Seu computador
- Link suspeito enviado
- Mensagem oferecendo oferta imperdível

POLÍTICAS DA EMPRESA

- Uso de computadores
- Manuseio de documentos
- Identificação no escritório
- Compartilhamento de informações

Não ter medo de reportar, mesmo que não tenha certeza.

.2 APÊNDICE B

Questionário de conscientização de Segurança da Informação

Lhe será pedido que responda questões que tratam do seu conhecimento, atitude e comportamento ao usar um computador. As opções de resposta são: (1)-Discordo plenamente, (2)-Discordo parcialmente, (3)-Não concordo nem discordo, (4)-Concordo Parcialmente e (5)-Concordo plenamente. A pesquisa é anônima.
*Obrigatório

1. Informe um codinome *

_____

2. Idade *

Marcar apenas uma oval.

- ◯ 17 a 24 anos
- ◯ 25 a 34 anos
- ◯ 35 a 44 anos
- ◯ 45 a 54 anos
- ◯ 55 a 64 anos
- ◯ acima de 64 anos

3. Sexo *

Marcar apenas uma oval.

- ◯ Feminino
- ◯ Masculino
- ◯ Prefiro não declarar

4. Profissão *

_____

5. Seu trabalho requer o uso de computador ou dispositivo móvel? *

Marcar apenas uma oval.

- Sim
- Não
- Não estou trabalhando no momento

6. Escolaridade *

Marcar apenas uma oval.

- Fundamental Incompleto
- Fundamental Completo
- Ensino Médio Incompleto
- Ensino Médico Completo
- Superior Incompleto
- Superior Completo
- Pós Graduado

Questionário de conscientização de Segurança da Informação

Lhe será pedido que responda questões que tratam do seu conhecimento, atitude e comportamento ao usar um computador. As opções de resposta são: (1)-Discordo plenamente, (2)-Discordo parcialmente, (3)-Não concordo nem discordo, (4)-Concordo Parcialmente e (5)-Concordo plenamente. A pesquisa é anônima.

7. É aceitável utilizar a senha das minhas redes sociais nos acessos do trabalho. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

8. É seguro utilizar a mesma senha em minhas redes sociais e acessos do trabalho. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

9. As senhas de minhas redes sociais são diferentes das senhas de meus acessos do trabalho. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

10. Tenho permissão para compartilhar minhas senhas de trabalho com colegas. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

11. É uma má ideia compartilhar minhas senhas de trabalho, mesmo que um colega peça. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

12. Eu compartilho minhas senhas de trabalho com colegas. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

13. É necessária uma mistura de letras, números e símbolos para senhas de trabalho. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

14. É seguro ter uma senha de trabalho composta apenas por letras. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

15. Eu uso uma combinação de letras, números e símbolos em minhas senhas. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

16. Posso clicar em qualquer link em e-mail de pessoas que conheço. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

17. É sempre seguro clicar em links de e-mails de pessoas que conheço. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

18. Eu nem sempre clico em links de e-mails só porque vêm de alguém que conheço. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

19. Não tenho permissão para clicar no link de um e-mail de um remetente desconhecido. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

20. Nada de ruim pode acontecer se eu clicar em um link em um e-mail de um remetente desconhecido. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

21. Se um e-mail de um remetente desconhecido parecer interessante, eu clico em um link dentro dele. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

22. Tenho permissão para abrir anexos de e-mail de remetentes desconhecidos. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

23. É arriscado abrir um anexo de e-mail de um remetente desconhecido. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

24. Eu não abro anexos de e-mail se o remetente for desconhecido para mim. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

25. Tenho permissão para baixar qualquer arquivo no meu computador do trabalho, se me ajudarem a realizar minhas funções. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

26. Baixar arquivos no meu computador de trabalho pode ser perigoso. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

27. Eu baixo qualquer arquivo em meu computador do trabalho que me ajude a realizar as minhas tarefas. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

28. Enquanto estou trabalhando, eu não devo acessar alguns sites. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

29. Só porque posso acessar um site no trabalho, não significa que seja seguro. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

30. Ao acessar a internet no trabalho, visito qualquer site que eu quiser. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

31. Tenho permissão para inserir qualquer informação, em qualquer site, se isso me ajudar a fazer meu trabalho. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

32. Se me ajuda a fazer meu trabalho, não importa as informações que coloco em um site. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

33. Eu avalio a segurança dos sites antes de inserir informações. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

34. Devo revisar periodicamente as configurações de privacidade das minhas redes sociais. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

35. É uma boa ideia revisar periodicamente as configurações de privacidade das minhas redes sociais. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

36. Eu não reviso periodicamente as configurações de privacidade das minhas redes sociais. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

37. Não posso ser demitido por algo que posto nas redes sociais. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

38. Não tem problema postar coisas nas redes sociais que eu normalmente não diria em público. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

39. Eu não posto algo nas redes sociais antes de considerar as consequências negativas. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

40. Posso postar o que quero sobre o meu trabalho nas redes sociais. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

41. É arriscado postar certas informações sobre meu trabalho nas redes sociais. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

42. Eu posto tudo o que quero sobre meu trabalho nas redes sociais. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

43. Quando trabalho em um local público, tenho que manter meu notebook comigo o tempo todo. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

44. Ao trabalhar de um local publico, é seguro deixar meu notebook sem supervisão por alguns minutos. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

45. Quando trabalho em um local público, deixo meu laptop sem supervisão. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

46. Eu tenho permissão para enviar arquivos confidenciais de trabalho por meio de uma rede Wi-Fi pública. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

47. É arriscado enviar arquivos confidenciais de trabalho usando uma rede Wi-Fi pública. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

48. Eu envio arquivos confidenciais de trabalho utilizando redes Wi-Fi públicas. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

49. Ao trabalhar em um documento confidencial, devo garantir que estranhos não possam ver a tela do meu notebook. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

50. É arriscado acessar arquivos confidenciais de trabalho em um laptop se estranhos puderem ver minha tela. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

51. Eu verifico se estranhos não podem ver a tela do meu notebook se estou trabalhando em um documento confidencial. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

52. As impressões confidenciais podem ser eliminadas da mesma forma que as não confidenciais. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

53. Descartar impressões confidenciais em uma lixeira é seguro. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

54. Quando impressões confidenciais precisam ser descartadas, eu me certifico de que sejam rasgadas ou destruídas. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

55. Se eu encontrar um pendrive na rua, não devo conectá-lo ao meu computador de trabalho. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

56. Se eu encontrar um pendrive na rua, nada de ruim pode acontecer se eu o conectar ao meu computador de trabalho. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

57. Eu não conectaria um pendrive encontrado na rua em meu computador de trabalho. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

58. Eu tenho permissão para deixar impressões contendo informações confidenciais em minha mesa durante a noite. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

59. É arriscado deixar impressões que contêm informações confidenciais na minha mesa durante a noite. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

60. Eu deixo impressões que contêm informações confidenciais na minha mesa enquanto estou ausente. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

61. Se eu vir alguém agindo de forma suspeita em meu local de trabalho, devo denunciá-lo. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

62. Se eu ignorar alguém agindo de forma suspeita em meu local de trabalho, nada de ruim pode acontecer. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

63. Se eu visse alguém agindo de forma suspeita em meu local de trabalho, faria algo a respeito. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

64. Não devo ignorar o mau comportamento de segurança de meus colegas. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

65. Nada de ruim pode acontecer se eu ignorar o comportamento de segurança insatisfatório de um colega. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

66. Se eu percebesse que meu colega estava ignorando as regras de segurança, não faria nada. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

67. Reportar incidentes de segurança é opcional. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

68. É arriscado ignorar incidentes de segurança, mesmo que eu ache que não sejam significativos. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

69. Se eu notasse um incidente de segurança, eu o relataria. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo plenamente	◯	◯	◯	◯	◯	Concordo plenamente

Este conteúdo não foi criado nem aprovado pelo Google.

Google Formulários