INSTITUTO FEDERAL DE CIÊNCIA E TECNOLOGIA GOIANO

CAMPUS CERES

CURSO BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ANNY KAROLINY MORAES RIBEIRO

AVALIAÇÃO DOS CONHECIMENTOS BÁSICOS EM SEGURANÇA DA INFORMAÇÃO NO IF GOIANO CAMPUS CERES

CERES – GO

2021

ANNY KAROLINY MORAES RIBEIRO

Neste artigo iremos analisar o conhecimento de pessoas da comunidade interna do Instituto Federal de Ciência e Tecnologia Campus Ceres em conceitos básicos de segurança da informação, veremos como conceitos simples são importantes para evitar golpes digitais, roubos de dados entre outras situações. Os dados foram obtidos via questionário online e serão analisados por meio de gráficos comparativos sob orientação do professor Doutor Flávio Manoel Coelho Borges Cardoso e co-orientação do professor Mestre Rangel Rigo.

CERES - GO

2021

Sistema desenvolvido pelo ICMC/USP
Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas - Instituto Federal Goiano

Moraes Ribeiro, Anny Karoliny
M484a AVALIAÇÃO DOS CONHECIMENTOS BÁSICOS EM SEGURANÇA DA INFORMAÇÃO NO IF GOIANO CAMPUS CERES / Anny Karoliny Moraes Ribeiro; orientador Flávio Manoel Coelho Borges Cardoso; co-orientador Rangel Rigo. -- Ceres, 2021.
32 p.

TCC (Graduação em Bacharelado em Sistemas de Informação) -- Instituto Federal Goiano, Campus Ceres, 2021.

1. segurança da informação. 2. vírus. 3. malwares. 4. ataques digitais. 5. vulnerabilidades. I. Coelho Borges Cardoso, Flávio Manoel , orient. II. Rigo, Rangel, co-orient. III. Título.

Responsável: Johnathan Pereira Alves Diniz - Bibliotecário-Documentalista CRB-1 n°2376

INSTITUTO FEDERAL
Goiano

Repositório Institucional do IF Goiano - RIIF Goiano
Sistema Integrado de Bibliotecas

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano, a disponibilizar gratuitamente o documento no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

Identificação da Produção Técnico-Científica

[ ] Tese
[ ] Dissertação
[ ] Monografia – Especialização
[X] TCC - Graduação
[ ] Produto Técnico e Educacional - Tipo: _____
[X] Artigo Científico
[ ] Capítulo de Livro
[ ] Livro
[ ] Trabalho Apresentado em Evento

Nome Completo do Autor: Anny Karoliny Moraes Ribeiro
Matrícula: 2016103202030125
Título do Trabalho: AVALIAÇÃO DOS CONHECIMENTOS BÁSICOS EM SEGURANÇA DA INFORMAÇÃO NO IF GOIANO CAMPUS CERES

Restrições de Acesso ao Documento

Documento confidencial: [X] Não [ ] Sim, justifique: _____

Informe a data que poderá ser disponibilizado no RIIF Goiano: __/__/__
O documento está sujeito a registro de patente? [ ] Sim [X] Não
O documento pode vir a ser publicado como livro? [ ] Sim [X] Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O/A referido/a autor/a declara que:

1. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
2. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
3. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

Ceres - GO, 22/11/2021.
Local Data

Anny Karoliny Moraes Ribeiro
Assinatura do Autor e/ou Detentor dos Direitos Autorais

Ciente e de acordo:

Assinatura do(a) orientador(a)

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

ATA DE DEFESA DE TRABALHO DE CURSO

Ao(s) 23 dia(s) do mês de agosto do ano de dois mil e vinte um, realizou-se a defesa de Trabalho de Curso do(a) acadêmico(a) ANNY KAROLINY MORAES RIBEIRO, do Curso de bacharelado em Sistemas de Informação, matrícula 2016103202030125, cujo título é "AVALIAÇÃO ESTATÍSTICA PONTUAL DO NÍVEL DE CONHECIMENTO EM SEGURANÇA DA INFORMAÇÃO". A defesa iniciou-se às 20 horas e 30 minutos, finalizando-se às 23 horas. A banca examinadora considerou o trabalho APROVADO com média 8,3 no trabalho escrito, média 9,0 no trabalho oral, apresentando assim média aritmética final de 8,7 pontos, estando a estudante APTO para fins de conclusão do Trabalho de Curso.

Após atender às considerações da banca e respeitando o prazo disposto em calendário acadêmico, a estudante deverá fazer a submissão da versão corrigida em formato digital (.pdf) no Repositório Institucional do IF Goiano – RIIF, acompanhado do Termo Ciência e Autorização Eletrônico (TCAE), devidamente assinado pelo autor e orientador.

Os integrantes da banca examinadora assinam a presente.

(Assinado Eletronicamente)
Nome do Presidente da Banca

(Assinado Eletronicamente)
Nome do Membro 1 Banca Examinadora

(Assinado Eletronicamente)
Nome do Membro 2 Banca Examinadora

Documento assinado eletronicamente por:

- **Rangel Rigo, COORDENADOR DE CURSO - FUC1 - CCEG-CE**, em 26/08/2021 20:23:30.
- **Roitier Campos Goncalves, PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 26/08/2021 12:00:05.
- **Cleyber Bezerra dos Reis, Cleyber Bezerra dos Reis - Professor Avaliador de Banca - Instituto Federal Goiano - Campus Ceres (10651417000410)**, em 23/08/2021 23:10:20.
- **Flavio Manoel Coelho Borges Cardoso, PROFESSOR ENS BASICO TECN TECNOLOGICO**, em 23/08/2021 23:07:37.

Este documento foi emitido pelo SUAP em 21/07/2021. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 292334
Código de Autenticação: c7b8593416

INSTITUTO FEDERAL GOIANO
Campus Ceres
Rodovia GO-154, Km.03, Zona Rural, None, CERES / GO, CEP 76300-000
(62) 3307-7100

AGRADECIMENTOS

Agradeço aos meus pais e minha irmã por sempre terem me incentivado a estudar e ser uma pessoa de excelência em todas as áreas da minha vida, meus professores que me apoiaram e contribuíram com cada passo que dei ao longo do meu curso com quem aprendi tanto, não só no âmbito acadêmico mas também outras lições que levarei para vida, em especial meus orientadores Flávio Manoel Coelho Borges Cardoso e Rangel Rigo e a maravilhosa Jaqueline Ribeiro, aos meus amigos que me arrancaram sorrisos quando eu pensava que não iria conseguir, que me apoiaram nos meus momentos de cansaço com palavras de apoio e incentivo, meu namorado Fabrício que esteve ao meu lado ao longo dos dias me apoiando e principalmente cuidando de mim. Amo todos vocês unicamente, gratidão eterna por acreditarem em mim e me acompanharem nessa caminhada.

“Se der certo ou não, não importa. O que importa
é que eu tentei e fui o mais longe que pude.”
Supernatural

RESUMO

Esse trabalho consiste numa pesquisa bibliográfica sobre conceitos básicos de segurança da informação através de levantamento bibliográfico e análise dos mesmos através de aplicação de questionário dentro da comunidade interna do Instituto Federal Goiano Campus Ceres. Analisar se as pessoas conhecem o básico para se proteger de golpes, também proteger seus dados e arquivos dentro do meio digital.

Palavras-chave: Segurança da informação, vírus, *malwares*, ataques digitais, vulnerabilidades.

ABSTRACT

This work consists of a bibliographical research on basic concepts of information security through a bibliographic survey and analysis of them through a questionnaire within the internal community of the Instituto Federal Goiano Campus Ceres. Analyze if people know the basics to protect themselves from scams, also protect your data and files within the digital medium.

Keywords: Information security, viruses, malware, digital attacks, vulnerabilities

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. Introdução

O mundo tem vivenciado transformações significativas, conforme a grande velocidade com que as pessoas passaram a ter acesso a dados e informações, mudando a forma como elas se relacionam. A internet criou uma sociedade em rede, encurtou as distâncias e a forma de relacionamento interpessoal (CASTELLS, 1999).

Cada dia mais pessoas estão conectadas à internet. Segundo o IBGE(2018) “De 2016 para 2017, o percentual de utilização da Internet nos domicílios subiu de 69,3% para 74,9%, ou seja, três em cada quatro domicílios brasileiros”.

Atualmente milhões de usuários utilizam as redes para compartilhamento de fotos, dados pessoais, realizar atividades bancárias, compras online, entre tantas outras atividades, a segurança se tornou um problema (TANENBAUM; WETHERALL, 2011).

A internet que utilizamos teve início sobre uma rede chamada ARPANET (Advanced Research Projects Agency Network – Rede da Agência de Projetos de Pesquisa Avançada), que foi criada no ano de 1969 pelo Departamento de Defesa dos Estados Unidos (WAZLAWICK, 2016).

Devido à grande taxa de pessoas conectadas à internet, se faz cada dia mais necessário a aplicação da segurança da informação. A segurança da informação é um tema complexo e abrange diversas questões, um de seus objetivos é evitar que usuários não autorizados tenham acesso às informações compartilhadas ou adulteradas. Outra característica da segurança é impedir que usuários mal-intencionados tenham acesso a informações não autorizadas. Por fim, procura da melhor forma possível identificar se determinada mensagem é verdadeira ou falsa. A partir das técnicas desenvolvidas com a segurança da informação é possível analisar situações em que mensagens são capturadas e adulteradas, além de responsabilizar o usuário por ter enviado certas mensagens (TANENBAUM; WETHERALL, 2011).

O número de vulnerabilidades existentes cresce consideravelmente dia após dia, uma das maiores empresas de antivírus da atualidade, a Kaspersky, disponibilizou dados recentes a respeito:

> Ao todo, as tecnologias de detecção da Kaspersky Lab encontraram 346 mil novos *malware* por dia nos dez primeiros meses do ano. O número e o alcance de novos arquivos maliciosos detectados diariamente são uma boa

> indicação dos interesses dos cibercriminosos envolvidos na criação e distribuição de *malware* (KASPERSKY, 2019).

Geralmente as situações que envolvem problemas com segurança são causadas premeditadamente por indivíduos mal-intencionados, com objetivo de alcançar algum benefício próprio ou perturbar uma pessoa determinada (TANENBAUM; WETHERALL, 2011).

Este artigo tem como objetivo realizar um estudo a partir de um levantamento bibliográfico sobre as vulnerabilidades mais recorrentes mecanismos básicos e eficazes de defesa e levantar o nível de conhecimento das pessoas da comunidade interna do Instituto Federal Goiano Campus Ceres sobre através de questionário.

2. Levantamento Bibliográfico

Nesta seção serão abordados os aspectos teóricos relacionados com a vulnerabilidade dos sistemas, as suas ameaças mais significativas e como se proteger. Dentre outros assuntos abordados também temos a importância da informação, o que é e quais os objetivos da segurança da informação.

2.1. A importância da informação

A informação é vital para as instituições independente do ramo, as informações são utilizadas para auxiliar no processo decisório e para alcançar o sucesso, obtendo um melhor desempenho comercial. Diante disso é necessário garantir a segurança dessas informações, para evitar perdas financeiras e danos para imagem da organização (GALEGALE; FONTES; GALEGALE, 2017).

2.2. Segurança da Informação

A segurança da informação tem o objetivo de proteger informações, identificando os fatores críticos para a proteção da informação e moderar a forma de manusear a informação para se obter sucesso na proteção da informação (GALEGALE; FONTES; GALEGALE, 2017).

Também consiste na preservação da informação, mantendo os princípios de

confidencialidade, integridade, disponibilidade, autenticidade e não repúdio, impossibilitando que as vulnerabilidades sejam aproveitadas por ameaças gerando prejuízos a organização (GALEGALE; FONTES; GALEGALE, 2017).

2.3. Vulnerabilidades e ameaças

As vulnerabilidades são fragilidades que facilitam a entrada de ameaças, uma ameaça por si só pode não causar nenhum dano, porém se há uma vulnerabilidade, é como abrir uma porta para ameaça entrar (KIM; SOLOMON, 2014).

Uma ameaça pode causar danos as informações importantes para uma organização, a mesma usa vulnerabilidades encontradas para isso. Pode acontecer de forma acidental ou como uma ação premeditada (GALEGALE; FONTES; GALEGALE, 2017).

De acordo com a Avast(2019), são detectados um milhão de novos arquivos maliciosos por dia e dois bilhões de ataques por mês. E segundo as estatísticas do catálogo de fraudes da RNP(2019) temos 13459 fraudes catalogadas. Ainda temos a segundo a Kaspersky(2018) que os brasileiros são os que mais sofrem com golpes de *phishing* no mundo, cerca de 23% dos usuários brasileiros caíram no golpe em 2018, deixando o Brasil na infeliz primeira posição do *ranking*.

2.4. Engenharia Social

É necessário considerar o fator humano quando se fala de segurança da informação, golpes de engenharia social também são brechas na segurança, e são um pouco mais difíceis de tratar já que os sistemas precisam prever e antecipar o comportamento das pessoas (BARRAS, 2014).

O atacante usa técnicas persuasivas para enganar os usuários, explorando comportamentos naturais da natureza humana como a vontade de ajudar, apoiar, ser educado, ser parte de algo e também a vontade de se mostrar capaz de realizar um trabalho. Assume papéis que ganham fácil confiança das pessoas, de forma manipuladora, mentirosa e antiética (MITNICK, 2018).

2.5. Ataques de *phishing*

Como dito pela Avast(2019) o Brasil é campeão quando o assunto é cair em golpes de *phishing*, mas o que são eles?

A palavra de origem inglesa, *phishing* surgiu em meados de 1990, remete a *fishing*, que significa pescaria, trocadilho esse porque este ataque é caracterizado por deixar iscas para que usuário possa morder (PENA; SILVA; SANTOS, 2020).

São ataques baseados em engenharia social, feitos para enganar o usuário de forma que o mesmo forneça informações pessoais, imitando uma página, afim de conseguir as credenciais de acesso de determinado *site* ou rede social ou mesmo dados privados das vítimas (REDHAT, [s.d.]).

2.6. Como se proteger digitalmente?

Entre as principais recomendações de segurança, de acordo com o CERT.BR (2019) recomenda-se:

Manter sempre atualizados o sistema operacional, os programas e todas as ferramentas usadas, além de verificar sempre se os *sites* que você acessa são confiáveis e tomar cuidado com os anexos e *links* recebidos por *e-mail* mesmo que o remetente seja conhecido.

Também deve-se evitar acessar informações importantes por computadores de terceiros, ou computadores públicos, elabore bem sua senha, para evitar que a mesma seja facilmente descoberta por ataques de força bruta. E sempre ativar a verificação de duas etapas para acessar e-mail, redes sociais, aplicativos etc.

A Kaspersky(2019) sugere que para melhorar a segurança online deve-se prestar atenção nos seguintes aspectos:

Verificar as configurações de privacidade das redes sociais. Não utilizar armazenamento público para informações pessoais. Para evitar rastreamento, utilizar a aba anônima. Manter seu *e-mail* principal e telefone privados.

Utilizar somente aplicativos autorizados (baixados diretamente da App Store, Play Store) e dar preferência aos que utilizam criptografia de ponta a ponta. Tomar cuidado com as permissões de aplicativos e extensões de navegadores. Assim como configurar senhas de acesso em seus dispositivos (computadores, celulares etc.).

2.7. Antivírus

Antivírus são *softwares* de detecção e remoção de arquivos maliciosos, como vírus e *worms*. São utilizados para proteger e prevenir contra códigos maliciosos e dar mais segurança ao usuário, possui vários métodos de identificação para impedir a

entrada de vírus, como atualizações automáticas, escaneamento, quarentena entre outros meios. Há muitas formas de infectar uma máquina com vírus, através de *pen drives*, *emails*, sites de conteúdo adulto, *downloads* de arquivos e programas infectados entre outros meios, por isso o uso de um bom antivírus no computador pessoal é tão importante (CANALTECH, 2021).

2.8. Verificação de duas etapas

A verificação de duas etapas também é conhecida pelo termo autenticação de dois fatores, se trata de uma camada extra de proteção. Originária do inglês "*two-factor authentication*" e representada pela sigla 2FA, inclui uma segunda verificação de identidade no momento da autenticação, impedindo a entrada às contas mesmo quando o invasor conhece a senha (TECHTUDO, 2021).

3. Metodologia

Esta é uma pesquisa com abordagem quantitativa e de caráter exploratório. Isto porque, se trata de um tema pouco estudado e explorado, sendo muito utilizado em levantamentos bibliográficos, documentais e estudos de caso (GIL, 2008).

A coleta de dados foi realizada por meio de duas técnicas distintas: o levantamento bibliográfico e por questionário estruturado. Na primeira delas, foram feitas pesquisas em artigos científicos nas bases de dados Spell, Scielo, Google Scholar e também livros relevantes para o trabalho. Nesta fase, o objetivo foi aprofundar o conhecimento a respeito do tema e identificar os principais estudos ou trabalhos sobre segurança da informação na atualidade.

Inicialmente as pesquisas foram de artigos dos últimos 10 anos, com palavras chaves e resumo que contivessem os termos “Segurança da informação”, ”vírus”, ”*malware*”. Posteriormente foi levantado outros artigos de assuntos mais específicos separadamente que pudessem enriquecer o trabalho com mais detalhes e informações relevantes. Também foram utilizados dados fornecidos por empresas da área de segurança da informação, mais especificamente grandes empresas de antivírus. Que dispõe sempre dos dados mais recentes e atualizados a respeito do tema.

Foram considerados artigos que tivessem um embasamento teórico que

contivesse conceitos sobre a importância da informação e de protegê-la, de segurança da informação e/ou tratasse conceitos de vírus, vulnerabilidades, ameaças e defesas eficientes. Descartou-se artigos que levaram a teoria para a parte de políticas de segurança com enfoque em empresas e segurança física (câmeras, alarmes).

A segunda técnica empregada foi o questionário estruturado, que como um instrumento de coleta de dados, elaborado pelo pesquisador com um roteiro pré-definido, deve ser aplicado a um público específico que irá contribuir com os resultados da pesquisa. O questionário é definido como um conjunto de perguntas para saber a opinião do respondente sobre um determinado tópico (PINHEIRO; GÜNTHER, 2008). As variáveis que foram utilizadas neste trabalho são: os tipos de vulnerabilidades e ameaças (vírus, *malwares*, golpes de engenharia social, *phishing*) mais comuns tanto em quaisquer dispositivos com ou sem acesso à internet que contiver informações importantes e suscetíveis a eles, tipos de defesas mais apropriadas incluindo instruindo contra ataques de engenharia social que atingem diretamente o pessoal da organização, também o ano de ocorrência do ataque, local do ataque, quem identificou o ataque (empresa ou pessoa) e fonte de pesquisa sobre o ataque.

O questionário aplicado foi direcionado ao público interno do Instituto Federal Goiano de Ciência e Tecnologia Campus Ceres, alunos e servidores. Foram enviados para todos os alunos e colaboradores via *email* institucional da ASCOM da instituição, e deles obtivemos 111 respostas e após filtrar e apagar os registros repetidos tivemos 108 respostas para analisar. Dentre as variáveis estudadas a primeira foi quanto ao número de usuários com relação a gênero biológico e houve um equilíbrio entre os mesmos com masculino (50,9%) e feminino (49,1%) dos respondentes. Quanto a escolaridade, houve um predomínio dos cursos superior incompleto e ensino médio incompleto, que somados representavam mais de 61% dos respondentes. Como era de se esperar a área de formação/estudo dos pesquisados está muito relacionada a área de informática ou tecnologia com 47,3%.

Quanto a análise dos dados encontrados, foram tratados por meio de estatística descritiva (frequências e outras medidas de tendência) e apresentados por meio de gráficos/figuras e tabelas.

4. Resultados e Discussões

Neste capítulo são apresentados os resultados encontrados neste estudo sobre segurança da informação na internet. Por meio das respostas dos questionários aplicados podemos observar que a comunidade interna do Instituto Federal Goiano Campus Ceres é mais consciente que a maioria dos brasileiros, como foi possível perceber pelo levantamento bibliográfico realizado ainda há muito com que se preocupar no âmbito segurança digital no contexto Brasil. A literatura apontou que os brasileiros ainda são muito vulneráveis a golpes digitais porque não tomam as medidas de segurança adequadas no uso de seus equipamentos na referida rede de computadores mundiais.

Quando se perguntou aos entrevistados sobre a sua preocupação com a segurança dos seus dados quando navega pela internet, a grande maioria (88,9%) respondeu que se que sim, que preocupa com seus dados na internet. Da mesma forma, quando questionado se participa de promoções de empresas nomeadas (Boticário, Americanas entre outras) que recebe por whatsapp e outros meios onde se precisa preencher seus dados pessoais, novamente a grande maioria respondeu que ignora a mensagem e a apaga (81%), e ainda, 8% afirmaram que Clica no *link* para saber se a promoção é verdadeira e a partir daí decide se manda ou não seus dados.

Um aspecto importante sobre segurança é as permissões que os usuários têm que dar para usar aplicativos e *softwares*, a grande maioria dos respondentes (75,9%) afirmaram que olham cuidadosamente sobre o assunto, porém, existem pessoas que nem sabiam que isso existia (24,1%), o que é preocupante para segurança de dados, já que muitos aplicativos utilizam de forma maliciosa as permissões para obter acesso a dados sensíveis dos usuários. Uma variável importante para segurança em celulares é a verificação em duas etapas, um mecanismo de defesa que dificulta o acesso não autorizado a contas mesmo quando a senha é comprometida, 31,5% dos respondentes afirmaram que ativaram porque o aplicativo obrigou, mas não sabem para que serve e 68,5% disseram que conhecem esse dispositivo de segurança.

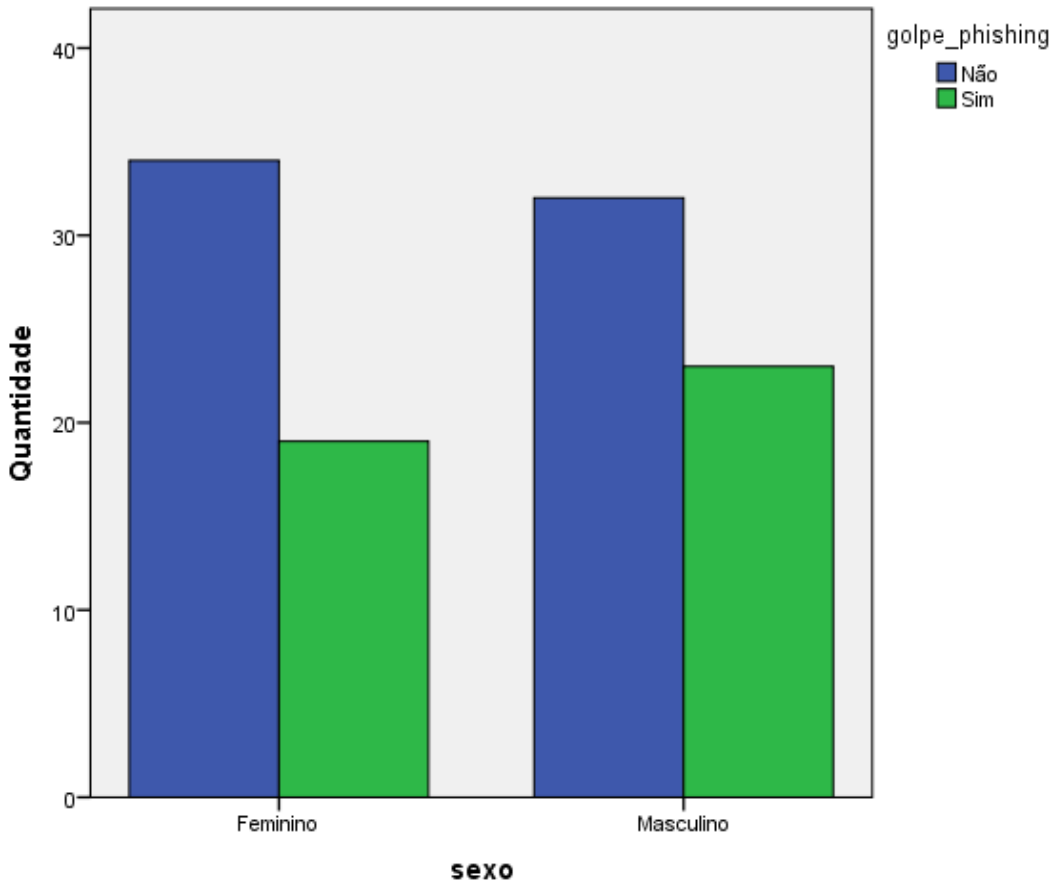
Quanto ao uso de antivírus, 63,9% disseram que sim, mas quando perguntado sobre golpes de *phishing*, 61,1% dos respondentes disseram que não conhecem. A preocupação com o uso de antivírus demonstra cuidado com segurança, contudo, o não conhecimento do golpe de phishing, pode significar uma exposição perigosa a crimes cibernéticos. Por último, quando perguntados sobre o sentimento de segurança

na internet, 71,3% responderam que não. Isto demonstra consciência sobre os riscos de segurança existentes na rede mundial de computadores e a exposição dos próprios dados.

Utilizando o ponto mais crítico no Brasil de acordo com o estudo bibliográfico que é são os golpes de *phishing*, fizemos a tabulação e comparação dos dados, para visualizar como está o conhecimento dos nossos respondentes.

Conforme observado na figura 2, onde a maior parte dos respondentes disseram não conhecer o que são os golpes de *phishing* que, quando cruzamos as respostas com a variável sexo as respostas não diferem tanto.

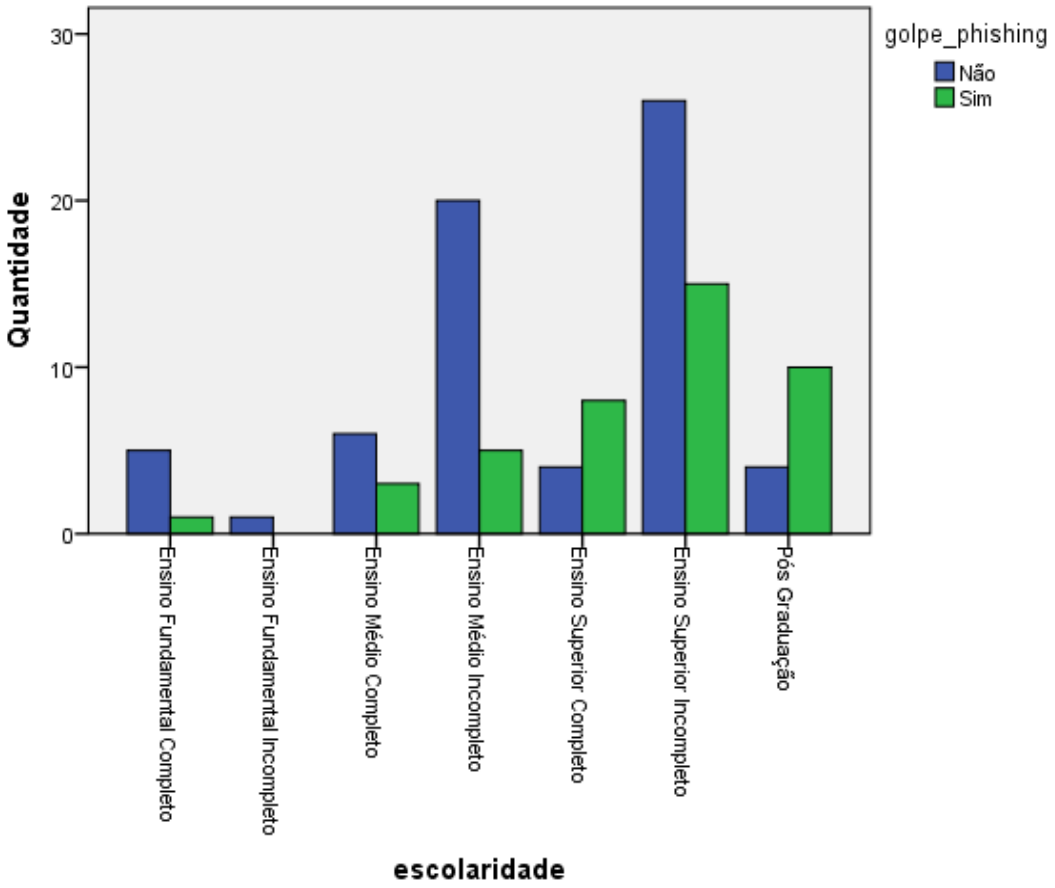
Figura 1: Tabulação cruzada sexo x conhecimento sobre golpes de *phishing*



Fonte: Elaborada pelo próprio autor.

Conforme podemos observar na figura 3, mesmo os respondentes de maior escolaridade não conheciam os perigosos golpes de *phishing*.

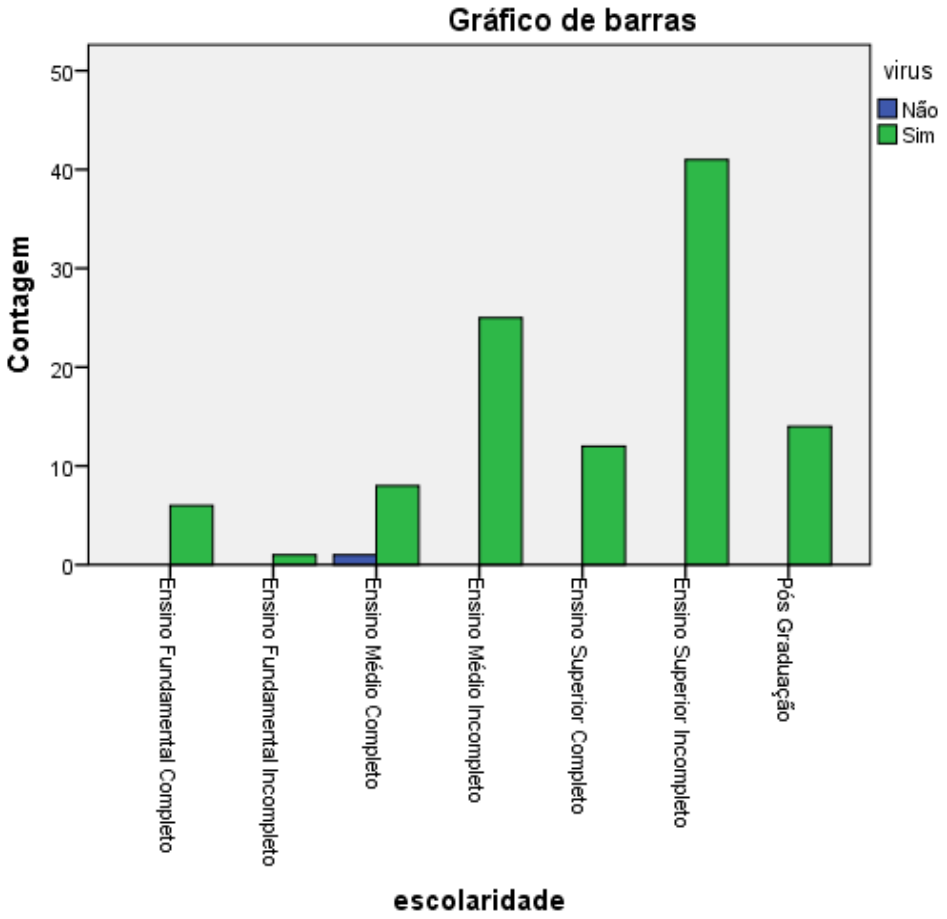
Figura 2: Tabulação cruzada escolaridade x conhecimento sobre golpes de *phishing*



Fonte: Elaborada pelo próprio autor.

Conforme podemos observar na figura 4, quando o assunto é vírus o cenário é bem diferente, sendo mais falado sobre esse tema a maioria dos respondentes sabiam o que são vírus.

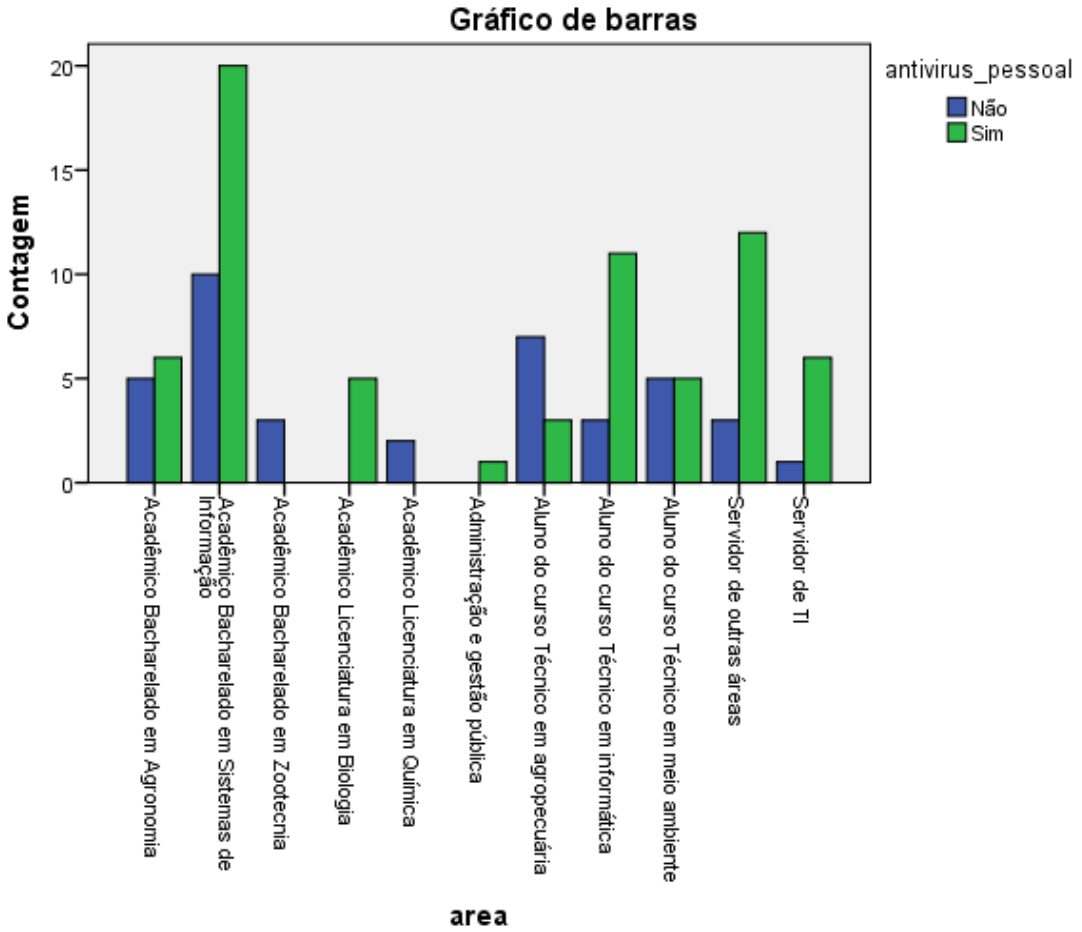
Figura 3: Tabulação cruzada escolaridade x conhecimento sobre vírus



Fonte: Elaborada pelo próprio autor.

Como podemos observar na figura 5, os respondentes da área de tecnologia apresentam ter mais consciência em relação a segurança, como podemos ver nesse gráfico que cruza o uso de antivírus e a área de estudo/atuação.

Figura 4: Tabulação cruzada área x uso de antívirus



Fonte: Elaborada pelo próprio autor.

Analisando os dados obtidos podemos observar que dentro da comunidade interna do Instituto Federal de Ciência e Tecnologia Campus Ceres há uma significativa consciência quando refere-se a segurança da informação.

5. Conclusão e Considerações Finais

Observamos que no Brasil ainda há uma carência de conhecimento sobre segurança da informação levando em consideração quantas pessoas ainda caem em golpes cada dia com mais frequência, vemos nos jornais como os números aumentaram agora na pandemia e como vimos no estudo bibliográfico o Brasil é recordista em golpes de *phishing*. Durante a análise das respostas que dentro da comunidade interna do Instituto Federal de Ciência e Tecnologia Campus Ceres há um conhecimento bastante relevante sobre os conceitos básicos de segurança da informação. Como sugestão para futuras pesquisas indicamos estudar as seguintes problemáticas:

Esse comportamento se deve pelo grau de instrução dos estudantes e

docentes do Instituto Federal Goiano Campus Ceres? Ou pelo fato de ter políticas informacionais sobre o assunto? Ou seria pelo fato de ter cursos de tecnologia na instituição e este contato acaba repassando essa cultura de ser mais cuidadoso com o digital? Esse comportamento se repete em outras instituições? E na comunidade no geral? Talvez no estado? Dentre diversos outros tendo como ponto de partida esta pesquisa.

6. Referências

AVAST. **Avast destaca cenário de ameaças para 2019**. Disponível em: <Avast destaca cenário de ameaças para 2019>.

BARRAS, C. **A ciência por trás da mentira: por que caímos em golpes?** Disponível em: <https://www.bbc.com/portuguese/noticias/2014/10/141015_vert_fut_golpes_ciencia_dg>. Acesso em: 6 jul. 2021.

CANALTECH. **O que é antivírus?** Disponível em: <https://canaltech.com.br/antivirus/o-que-e-antivirus/>. Acesso em: 7 set. 2021.

CERT.BR. **Uso seguro da internet**. Disponível em: <https://cartilha.cert.br/uso-seguro/>. Acesso em: 5 jun. 2019.

GALEGALE, N. V.; FONTES, E. L. G.; GALEGALE, B. P. Uma contribuição para a segurança da informação: Um estudo de casos múltiplos com organizações brasileiras1. **Perspectivas em Ciência da Informação**, v. 22, n. 3, p. 75–97, 2017.

GIL, A. C. **Métodos e Técnicas de Pesquisa Social**. 6. ed. São Paulo: Atlas, 2008.

IBGE. **PNAD Contínua TIC 2017: Internet chega a três em cada quatro domicílios do país**. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro-domicilios-do-pais>. Acesso em: 5 jun. 2019.

KASPERSKY. **Kaspersky detecta 350 mil novos vírus por dia em 2018**. Disponível em: <https://www.kaspersky.com.br/blog/kaspersky-detecta-novos-virus-dia-2018/11143/>. Acesso em: 5 jun. 2019.

KASPERSKY. **10 dicas para melhorar sua privacidade online**. Disponível em: <https://www.kaspersky.com.br/blog/privacy-ten-tips-2018/10616/>. Acesso em: 5 jun. 2019.

KIM, D.; SOLOMON, M. G. **Fundamentos de segurança de sistemas de informação**. 1. ed. Rio de Janeiro: LTC, 2014.

MITNICK, K. Engenheiros sociais — como eles trabalham e como detê-los. In: **A arte de invadir**. [s.l.] Pearson, 2018. p. 236.

PENA, B. H.; SILVA, A. SANTOS DA; SANTOS, M. DOS. Phishing. **Seminário de Tecnologia, Gestão e Educação**, p. 3, 2020.

REDHAT. **Malware: tudo o que você precisa saber para se proteger e melhorar a segurança da TI**. Disponível em: <https://www.redhat.com/pt-br/topics/security/what-is-malware>. Acesso em: 11 set. 2021.

RNP. **Catálogo de Fraudes: estatísticas**. Disponível em: <http://catalogodefraudes.rnp.br/stats>. Acesso em: 5 jun. 2019.

TANENBAUM, A. S.; WETHERALL, D. J. Segurança da informação. In: **Redes de computadores**. 5. ed. São Paulo: Pearson, 2011.

TECHTUDO. **Autenticação de dois fatores: o que é e para que serve o recurso**. Disponível em: <https://www.techtudo.com.br/noticias/2021/08/autenticacao-de-dois-fatores-o-que-e-e-para-que-serve-o-recurso.ghtml>. Acesso em: 7 set. 2021.

WAZLAWICK, R. S. Arpanet - 1969. In: **História da Computação**. 1. ed. Rio de Janeiro: Elsevier, 2016. p. 252–255.

Análise do grau de compreensão de conceitos básicos de Segurança da Informação no IF Goiano Campus Ceres

Olá, meu nome é Anny Karoliny Moraes Ribeiro e sou aluna do curso de Bacharelado em Sistemas de Informação do IF Goiano Campus Ceres. Estou realizando uma pesquisa que servirá de base para a elaboração do meu Trabalho de Conclusão de Curso. Esta pesquisa é relacionada à Segurança da Informação e, por esse motivo, estou enviando esse formulário para que você possa me contar um pouquinho sobre seu conhecimento sobre esse assunto. É importante frisar que a participação é totalmente voluntária e anônima. Sua colaboração em responder é muito importante para que eu possa obter bons resultados na minha pesquisa e o preenchimento do formulário é bem rápido, gastará apenas alguns minutos.

Por favor, só responda somente se for aluno/servidor no IF Goiano Campus Ceres! Minha pesquisa está restrita a comunidade interna do IF Goiano Campus Ceres.

Muito obrigada :)

*Obrigatório

1. E-mail *

2. Sexo: *

Marcar apenas uma oval.

- ◯ Masculino
- ◯ Feminino

3. Sua faixa etária (idade): *

Marcar apenas uma oval.

- ◯ Até 14 anos
- ◯ Entre 15 e 24 anos
- ◯ Entre 25 e 35 anos
- ◯ Entre 36 e 45 anos
- ◯ Entre 46 e 60
- ◯ Acima de 60

4. 3. Sua escolaridade: *

Marcar apenas uma oval.

- ◯ Ensino Fundamental Completo
- ◯ Ensino Fundamental Incompleto
- ◯ Ensino Médio Completo
- ◯ Ensino Médio Incompleto
- ◯ Ensino Superior Completo
- ◯ Ensino Superior Incompleto
- ◯ Outro: _____

5. Qual a sua área? *

Marcar apenas uma oval.

- ◯ Acadêmico Bacharelado em Sistemas de Informação
- ◯ Acadêmico Licenciatura em Biologia
- ◯ Acadêmico Licenciatura em Química
- ◯ Acadêmico Bacharelado em Agronomia
- ◯ Acadêmico Bacharelado em Zootecnia
- ◯ Aluno do curso Técnico em informática
- ◯ Aluno do curso Técnico em agropecuária
- ◯ Aluno do curso Técnico em meio ambiente
- ◯ Servidor de TI
- ◯ Servidor de outras áreas
- ◯ Outro: _____

6. Você se preocupa com seus dados enquanto navega na internet? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

7. Você participa de promoções de empresas nomeadas (Boticário, Americanas e outras de comércio eletrônico) que recebe por WhatsApp e outros meios onde você precisa preencher seus dados pessoais? Ao receber uma mensagem, por exemplo: "Parabéns!!! Seu número foi sorteado e você ganhou um barril de Heineken para animar a sua quarentena em casa! Clique aqui para fornecer seus dados para que possamos enviar o prêmio!". Qual a sua reação? *

   Marcar apenas uma oval.

   - ◯ Clico e preencho imediatamente pois não se pode perder uma oportunidade dessas!
   - ◯ Clico no link para saber se a promoção é verdadeira e a partir daí decido se mando ou não meus dados.
   - ◯ Faço uma busca na Internet sobre a existência de promoção da Heineken deste tipo.
   - ◯ Ignoro a mensagem e a apago.

8. Você tem ideia das permissões (a que dados do seu celular o aplicativo tem autorização para acessar) que os aplicativos precisam para serem instalados no seu celular? *

   Marcar apenas uma oval.

   - ◯ Nem sabia que isso existia
   - ◯ Sempre olho cuidadosamente

9. Você sabe o que é verificação de duas etapas? *

   Marcar apenas uma oval.

   - ◯ Ativei porque o aplicativo obrigou, mas não sei para que serve.
   - ◯ Sei sim.

10. Você utiliza algum antivírus no seu celular e/ou computador pessoal? *

Marcar apenas uma oval.

- Sim
- Não

11. Você sabe o que é golpe de Phishing? *

Marcar apenas uma oval.

- Sim
- Não

12. Você sabe o que é um Malware? *

Marcar apenas uma oval.

- Sim
- Não

13. Você sabe o que é um Vírus? *

Marcar apenas uma oval.

- Sim
- Não

14. Você se sente seguro usando a internet? *

Marcar apenas uma oval.

- Sim
- Não

15. Você deseja receber os resultados dessa pesquisa? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
