

JONATHAN SOARES DA SILVA

**OS USUÁRIOS POSSUEM CONHECIMENTO BÁSICO SOBRE SEGURANÇA DA
INFORMAÇÃO? UMA ANÁLISE REALIZADA NO ÂMBITO DO SETOR PÚBLICO.**

JONATHAN SOARES DA SILVA

**OS USUÁRIOS POSSUEM CONHECIMENTO BÁSICO SOBRE SEGURANÇA DA
INFORMAÇÃO? UMA ANÁLISE REALIZADA NO ÂMBITO DO SETOR PÚBLICO.**

Monografia apresentada à Banca Examinadora do Centro Universitário São Lucas, como requisito de aprovação para obtenção do Título de Bacharel em Sistema da Informação. Orientador: Prof. Romário Vitorino Ferreira

Ji-Paraná
2023

Dados Internacionais de Catalogação na Publicação - CIP

S586u Silva, Jonathan Soares da.

Os usuários possuem conhecimento básico sobre segurança da informação? Uma análise realizada no âmbito do setor público. / Jonathan Soares da Silva. – Ji-Paraná, 2023.
40 p.; il.

Monografia (Bacharel em Sistemas de Informação) – Centro Universitário São Lucas Ji-Paraná, 2023.

Orientador: Prof. Esp. Romário Vitorino Ferreira.

1. Segurança da Informação. 2. Setor público. 3. Roubo de informações. 4. Política de gestão da segurança da informação. I. Ferreira, Romário Vitorino. II. Título.

CDU 004.056.5

RESUMO

O objetivo deste projeto acadêmico destinou-se em desenvolver uma pesquisa em um determinado órgão público em um município do Estado de Rondônia. Previamente, para o alcance deste objetivo, o estudo foi instituído primeiramente, a partir da técnica de investigação bibliográfica, através de livros, artigos científicos e pesquisas publicadas relacionados com o tema do trabalho. Um estudo examinando a segurança da informação no setor público está se tornando cada vez mais necessário. O objetivo desta pesquisa é explorar como os usuários percebem a segurança da informação e como eles reagem às atividades de desenvolvimento dos usuários. A segurança da informação tem um papel significativo no setor público. Ela ajuda as organizações a prevenir o uso não autorizado, bloquear o acesso não autorizado e minimizar os danos causados por erros acidentais ou uso indevido intencional de suas redes, bancos de dados ou outros sistemas para que seus dados eletrônicos garantam seguros. Para o gerenciamento e desenvolvimento do projeto foi utilizada a pesquisa de campo, buscando obter dados sobre uma determinada realidade em um ambiente de trabalho. Usou-se da ferramenta Google Forms para a elaboração do questionário, enviado por meio de um link a todos os colaboradores da instituição. Composto de perguntas fechadas a fim de medir os níveis de riscos a que a organização está exposta. As análises foram feitas a partir dos tratamentos dos dados do questionário no Google Forms. Em seguida os gráficos com as amostras foram interpretados para conclusão da pesquisa. Este estudo identifica que a organização estudada está vulnerável se tratando de segurança da informação, as respostas apresentadas pelos participantes mostram o pouco conhecimento sobre o tema. A gestão da segurança da informação em órgão público é essencial para manter dados corporativos em segurança.

Palavras-chaves: Segurança da Informação. Setor público. Roubo de informações. Política de gestão da segurança da informação.

ABSTRACT

The objective of this academic project was to develop research in a specific public body in a municipality in the State of Rondônia. Previously, to achieve this objective, the study was first instituted, using the bibliographic research technique, through books, scientific articles and published research related to the theme of the work. A study examining information security in the public sector is becoming increasingly necessary. The aim of this research is to explore how users perceive information security and how they react to user development activities. Information security plays a significant role in the public sector. It helps organizations prevent unauthorized use, block unauthorized access, and minimize damage caused by accidental errors or intentional misuse of their networks, databases, or other systems so their electronic data is secure. For the management and development of the project, field research was used, seeking to obtain data about a certain reality in a work environment. The Google Forms tool was used to prepare the questionnaire, sent via a link to all employees of the institution. Composed of closed questions in order to measure the levels of risks to which the organization is exposed. The analyzes were carried out based on the processing of questionnaire data in Google Forms. Then the graphs with the samples were interpreted to conclude the research. This study identifies that the organization studied is vulnerable when it comes to information security, the answers presented by the participants show the little knowledge on the topic. Information security management in a public body is essential to keeping corporate data safe.

Keywords: Information security. Public sector. Information theft. Information security management policy.

LISTA DE GRÁFICOS

Gráfico 01 – Conhecimento sobre senhas pessoais seguras.....	27
Gráfico 02 – Periodicidade de renovação de senhas.....	28
Gráfico 03 – Padrão adotado para criação de senha.....	29
Gráfico 04 – Senhas curtas ou senhas longas.....	30
Gráfico 05 – Diversificação de senhas.....	30
Gráfico 06 – Guardar senhas.....	31
Gráfico 07 – Autenticação de senhas em duas etapas.....	32
Gráfico 08 – Hábitos ao checar e-mails.....	33

SUMÁRIO

1. INTRODUÇÃO	8
1.1. PROBLEMATIZAÇÃO.....	8
1.2. OBJETIVO GERAL	9
1.2.1. Objetivos específicos	9
1.3. JUSTIFICATIVA.....	9
2. REFERENCIAL TEÓRICO	12
2.1 ÓRGÃOS PÚBLICOS	12
3.3 RISCOS QUE O USUÁRIO ESTÁ EXPOSTO	14
2.3.1 Credenciais	15
2.3.2 <i>Phishing e Spamming</i>	15
2.3.3 <i>Cookies</i> espiões.....	17
2.3.4 <i>Spyware</i>	17
2.3.5 Cavalo de troia.....	18
2.3.6 Backdoor.....	18
2.3.7 <i>Home office</i>	19
2.2.8 Ransomware	20
2.4 DIREITOS E PENALIDADES SOB A NORMA JURÍDICA	22
2.5 POLÍTICA DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO	23
3. MATERIAL E MÉTODOS	25
3.1 DEFINIÇÃO DO TIPO DE PESQUISA QUANTO AOS OBJETIVOS.....	25
3.2 DEFINIÇÃO DO TIPO DE PESQUISA QUANTO À ABORDAGEM.....	25
3.3 DEFINIÇÕES DA POPULAÇÃO/AMOSTRA	26
3.4 AMOSTRAGEM NÃO PROBABILÍSTICA	26
3.5 PROCEDIMENTO DE ESCOLHA DA ORGANIZAÇÃO	26
3.6 TÉCNICAS E PROCEDIMENTOS DE COLETA.....	26
3.7 TÉCNICAS E PROCEDIMENTOS DE ANÁLISE	26
4. RESULTADOS E DISCUSSÃO.....	27
4.1 EM RELAÇÃO ÀS ORIENTAÇÕES PARA DEFINIÇÃO DE SENHAS PESSOAIS SEGURAS, ASSINALE A OPÇÃO QUE REPRESENTA O SEU CONHECIMENTO SOBRE O TEMA.	27

4.2 EM RELAÇÃO À PERIODICIDADE DE RENOVAÇÃO DE SENHAS, É DE SEU CONHECIMENTO QUE O RECOMENDADO PARA UMA MAIOR SEGURANÇA NOS AMBIENTES DIGITAIS É QUE ELAS SEJAM ATUALIZADAS FREQUENTEMENTE?	28
4.3 COM BASE NO SEU CONHECIMENTO SOBRE PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO, ASSINALE A OPÇÃO SOBRE O PADRÃO QUE ADOTOU PARA A CRIAÇÃO DE SUAS SENHAS.	28
4.4 EM RELAÇÃO A NOVAS SENHAS, ASSINALE A OPÇÃO QUE REPRESENTA O TIPO DE SENHA QUE VOCÊ ADOTA AO CRIA-LAS.....	29
4.5 RELACIONADO À DIVERSIFICAÇÃO DE SENHAS PARA USOS ESPECÍFICOS, VOCÊ MANTE SENHAS DIFERENTES PARA CADA SITE, APLICATIVO OU SOFTWARE QUE POSSUI CADASTRO?	30
4.6 COMO VOCÊ COSTUMA GUARDAR AS SENHAS DE APLICATIVOS E SITES QUE CADASTROU?	31
4.7 VOCÊ SABE O QUE É A AUTENTICAÇÃO DE SENHA EM DUAS ETAPAS, UTILIZADAS POR ALGUNS SITES E SOFTWARES?.....	32
4.8 COM BASE NOS SEUS HÁBITOS AO CHECAR OS SEUS E-MAILS, MARQUE AS OPÇÕES QUE VOCÊ REALIZA (PODE SER SELECIONADA MAIS DE UMA OPÇÃO).	32
5. CONCLUSÃO.....	34
REFERÊNCIAS BIBLIOGRÁFICAS	36
APÊNDICE A – Questionário	39

1. INTRODUÇÃO

Com o crescimento da tecnologia no modo geral principalmente na área eletrônica tem nos feitos procurar cada vez mais conhecimentos para atuar e até mesmo viver com mais facilidade e segurança, mesmo quando crianças já somos submetidos a uma vasta linha tecnológica, com diversos brinquedos, equipamentos e ou eletrônicos que usamos no dia a dia como celulares, *tablets*, televisores, computadores entre outros. Muitas das vezes antes mesmo de falarmos aprendemos a mover um item, abrir um aplicativo ou simplesmente segurar e arrastar de um lado para outro em nossos aparelhos *smartphone*, o que desperta cada vez mais nosso interesse por esses aparelhos incríveis.

Isso realmente é agradável, nos deixa cheios de energia e curiosidades para aprender cada vez mais, nos ensina a ser mais ativos e procurar soluções em distintos locais para um problema do qual não aceitamos ter, mas a principal questão é a ideia central deste artigo é: estamos seguros? Nós enquanto pessoas comuns temos a obrigação de aprender o mínimo possível sobre segurança da informação, temos que descobrir como lidar com as possíveis formas que existem de roubo de informação digital, sequestro de dados, entre males que existem como vírus.

1.1. PROBLEMATIZAÇÃO

A maior parte do público em geral é de um modo geral desatento a questões de segurança e privacidade. Esta pesquisa busca descrever uma análise de práticas de segurança da informação utilizadas entre funcionários do setor público. Tal investigação é especialmente importante à luz dos recentes incidentes de segurança que aumentaram a conscientização sobre a necessidade de buscar conhecimento, bem como à luz das possíveis mudanças ao longo do tempo em termos de políticas e estruturas institucionais, o que se refletiu em diferentes níveis de atividade entre as instituições.

Como profissionais temos uma obrigação ainda maior com a responsabilidade, devemos sempre procurar meios de estar atualizados no quesito segurança, manter dados importantíssimos longe de “mãos” erradas. De acordo com a PWC (2020, p.01),

Os principais tipos de crimes sofridos pelas empresas nos últimos 24 meses foram: fraude em compras (34% no Brasil e 22% no mundo), suborno ou corrupção (26% no Brasil e 25% no mundo), fraude cometida pelo

consumidor (24% no Brasil e 29% no mundo), crime cibernético (22% no Brasil e 31% no mundo), fraude contábil (22% no Brasil e 20% no mundo) e má conduta empresarial (19% no Brasil e 28% no mundo).

Sabemos que esse tipo de crime está cada vez mais comum, sendo assim grande empresas do setor privado tem solicitado aos seus funcionários um certo conhecimento na área da informática, e mesmo com o conhecimento básico ou até mesmo avançado muitas das empresas capacitam seus colaboradores para que desempenham com maior segurança suas atividades do dia a dia, o que nos leva a questionar, como anda o setor público, concede treinamentos e capacitação constantemente? Atualmente grande parte dos ataques *hacker*, são as instituições públicas por concentrar uma grande quantidade de informações e baixo nível de segurança.

1.2 OBJETIVO GERAL

Este trabalho tem o objetivo de identificar se funcionários de um determinado município de Rondônia usam práticas de segurança da informação no âmbito do setor público.

1.2.1. Objetivos específicos

- Fundamentar conceitos relacionados à segurança da informação partir da técnica de investigação bibliográfica;
- Definir a organização pública como objeto de pesquisa;
- Realizar levantamentos de dados a partir da aplicação de questionários;
- Analisar, interpretar e descrever o cenário atual da organização a partir dos dados coletados;
- Apresentar os resultados junto ao gestor da empresa, a fim de tomar decisões diante das conclusões obtidas.

1.3. JUSTIFICATIVA

Este trabalho tem como foco principal a segurança da informação no setor público, pois como citado anteriormente, os ataques às instituições governamentais pelo Brasil e mundo tem crescido de forma alarmante segundo a matéria do jornal CNN só em 2021 a polícia federal apontou que os ministérios e mais 20 órgãos do

governo foram invadidos (CNN, 2021), mas o que leva a uma exposição assim? É possível evitar ou pelo menos não facilitar tanto a invasão pelos criminosos?

Que a tecnologia eletrônica é o futuro isso é indiscutível, mas como a segurança será feita isso sim é um ponto ainda muito discutido por vários especialistas, durante a trágica pandemia da *covid-19* muito se falou em trabalho *home office*, tornando-se o distanciamento social a principal forma de prevenção, de fato houve a necessidade de trabalhar de forma remota, fomos obrigados a acelerar esse processo, em um curto período de tempo, empresas, prefeituras, ministérios, policiais e governo no geral precisaram se reinventar, sentiu a necessidade do trabalho remoto. Momento em que os profissionais de T.I junto com seus superiores discutem a melhor forma de seguir com as atividades.

Sem nenhuma capacitação, funcionários começam a criar uma rotina de trabalho diferenciada, transformando sua casa em escritório particular. Profissionais da tecnologia da informação tentam ao máximo fazer o serviço avançar de forma contínua com poucas ferramentas, sabemos que muitos não têm facilidade com a tecnologia, visto que um trabalho remoto não é muito fácil de ser implantado, além dessa desarmonia há a principal questão, quando saímos da estrutura física da nossa empresa também estamos deixando de lado a estrutura lógica onde ficam para trás toda nossa segurança, precisávamos que os trabalhos continuassem, mas não estávamos preparados para uma mudança repentina.

As instituições disponibilizam equipamentos para colaboradores que não possuem, contas de acesso de usuários são criados com um nível de segurança muito franco, esses são alguns dos exemplos que colaboram para a vulnerabilidade da empresa. Por outro lado, também contribuiu para o crescimento da tecnologia nas instituições, pois serviços que ainda eram feitos em formato manual, surgiram maneiras de realizá-los de forma eletrônica, arquivos e documentos mantidos de forma física houve a necessidade de digitalizar para que fossem compartilhados e arquivados para que todos tivessem acesso sempre que preciso.

Contudo considerando o surgimento de vários entraves, podemos conceituar um grande avanço da tecnologia em meio a humanidade, mas também uma grande oportunidade para os criminosos, *logins* salvos em máquinas que não deveria, acessos descuidados a sites impróprios ou com baixa segurança, e-mails maliciosos sendo abertos de forma errônea, pouquíssima ou nenhuma proteção contra vírus, o

que infestavam documentos importantes que ao ser enviado a nuvem facilitaram o acesso a demais computadores até chegar no servidor central da instituição.

Diante disso, se faz necessário um melhor entendimento sobre o grau de conhecimento de segurança da informação que os servidores possuem, para então buscar uma melhoria, o que se propõe através deste estudo. Este é um debate necessário no meio acadêmico, setores públicos e empresarial por estarmos vivendo um momento de grandes revoluções tecnológicas.

2. REFERENCIAL TEÓRICO

Segurança da informação (SI) é um termo amplo que abrange muitas áreas da ciência da computação, como criptografia e segurança de *software*. A segurança das informações inclui como elas são coletadas, processadas, armazenadas e transmitidas.

A tecnologia tem uma grande presença em nossas vidas, gostemos ou não. Seja através do trabalho, entretenimento ou comunicação, estamos sempre encontrando novas maneiras de sermos mais eficientes. A necessidade de segurança no aspecto da informação continuará a crescer à medida que a tecnologia se tornar ainda mais difundida em nossa sociedade.

2.1 ÓRGÃOS PÚBLICOS

De acordo com FREITAS (2013) “podemos conceituar órgão público como uma unidade que une atribuições praticadas pelos agentes públicos que o formam com o objetivo de manifestar a vontade do Estado [...]”.

A atribuição de órgão público é baseada no setor público. Ele se refere ao status legal de uma organização governamental ou institucional, ou seja, uma pessoa que tem caráter público e pode exercer direito ou funções públicas, que são limitadas por territórios, nacionalidade e personalidade.

De acordo com a Constituição da República Federativa do Brasil de 1988, constituem objetivos fundamentais como:

I- construir uma sociedade livre, justa e solidária; II - garantir o desenvolvimento nacional; III - erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais; IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.

Os princípios mencionados estão presentes no Artigo 3º da Constituição Federal do Brasil. São eles:

I - Construir uma sociedade livre, justa e solidária: A ideia é construir uma sociedade onde haja igualdade de oportunidades para todos, onde as liberdades individuais sejam preservadas e onde haja cooperação e solidariedade entre os cidadãos.

II - Garantir o desenvolvimento nacional: O objetivo é promover o crescimento econômico e social do país, garantindo melhores condições de vida para a população e proporcionando o avanço do país como um todo.

III - Erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais: Busca-se eliminar a pobreza e a marginalização, assegurar a inclusão social e reduzir as desigualdades entre os diferentes grupos sociais e regiões do país.

IV - Promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação: A intenção é garantir a igualdade e a dignidade de todas as pessoas, sem qualquer forma de preconceito ou discriminação, promovendo a inclusão e o respeito pela diversidade.

Esses princípios fundamentais são a base para a construção de uma sociedade mais justa e igualitária, onde todos tenham oportunidades e direitos garantidos.

Emmanuel (2019), afirma que

Os órgãos públicos são as repartições internas do Estado, criados a partir da desconcentração administrativa, com a finalidade de desempenhar funções estatais, sendo despidos de personalidade jurídica. Ou seja, é o compartimento na estrutura estatal a que são cometidas determinadas funções, sendo integrado por agentes públicos que, quando as executam, manifestam a própria vontade do Estado.

Um órgão público é uma entidade legal composta por vários indivíduos cujo objetivo é tomar decisões em nome do público. Os membros de um órgão público são indicados por líderes políticos ou eleitos pelos eleitores, que exercem o poder com base em sua autoridade.

De acordo com a NBR ISO/IEC 17799 (2001, p.02), a segurança da informação é caracterizada pela preservação de três princípios:

a) **confidencialidade**: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso; b) **integridade**: salvaguarda da exatidão e completeza da informação e dos métodos de processamento; c) **disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Um estudo realizado em um comércio varejista da cidade de Registro, interior de São Paulo, para o identificar possíveis falhas que envolvam os três principais pilares da Segurança da Informação, mostrou que a empresa possui ausência de política de segurança da informação; Falta de controle dos acessos aos

arquivos na rede computadorizada; Falta de regras mais definidas em relação aos acessos e usos da *internet*. O autor conclui que a informação é um fator de preciosidade para as pessoas. Dentro de uma empresa, as informações devem ser tratadas com uma maior importância e devem ser vistas como um ativo essencial para o negócio, e que precisam ser protegidas. (COUTINHO, 2017).

Uma pesquisa realizada para investigar 25 artigos que tratavam do tema, Interação Humano-Computador e Cibersegurança. Conclui que os fatores humanos têm relações diretas e indiretas sobre a segurança dos dispositivos podendo aumentar proporcionalmente os riscos de vulnerabilidade devido às ações e ao comportamentos das pessoas envolvidas, fatores humanos e sociais como: características humanas e fatores externos relacionados, como o estresse, a fadiga de trabalho, falta de atenção, a falta de comunicação entre os colegas de equipe causando divergências no trabalho ou falhas, a facilidade de utilização e avisos de um *software* de segurança, se é importante ou não utilizar um antivírus e sobre pessoas que tinham conhecimentos de vírus em anexos enviados por e-mail, foram considerados razões por favorecer ameaças à segurança da informação (TAKEUCHI, 2023).

Uma análise realizada em *datasets* após ter senhas vazadas, descobriu que apesar de boa parte das senhas apresentarem uma entropia de mais de 30 bits, a grande maioria das senhas seriam quebradas em menos de 1 dia nas simulações de 10 ataques por segundo, e em menos de 1 segundo nas simulações de 10 bilhões de ataques por segundo, esses resultados demonstram o poder dos algoritmos de *cracking* atuais, e a necessidade de trocar de senha periodicamente para caso o *hash* tenha sido vazado (ROCCIA, 2021).

Podemos perceber que os ataques cibernéticos possuem seu principal intermediário, o usuário final, este sem capacitação e preparo técnico propicia que o crime aconteça.

3.3 RISCOS QUE O USUÁRIO ESTÁ EXPOSTO

A seguir veremos alguns dos possíveis riscos que o usuário final está exposto em seu dia a dia no trabalho institucional. Condições que merecem atenção, uma vez que a falha humana pode gerar prejuízos significativos aos cofres públicos, quando transcorre em órgãos governamentais.

2.3.1 Credenciais

A segurança por senha é uma parte essencial da segurança da informação do usuário final. Quando as pessoas usam senhas fracas ou reutilizam a mesma senha para vários sites e contas, é fácil para os *hackers* obter acesso às suas contas por meio de ataques de força bruta, *keyloggers* e outros *malwares*.

Véras (2005, p. 41) relata que:

Todo o processo de autenticação pode ser visualizado como sendo baseado em confiança, ou seja, uma vez autenticado, o usuário é considerado confiável para a aplicação. Em um cenário onde os dados de autenticação não são totalmente confiáveis, não se pode confiar cegamente no usuário, portanto, deve-se encontrar uma técnica complementar para comprovar a veracidade das informações de autenticação e a própria validade dessa autenticação continuamente.

Um aplicativo da *web* é tão seguro quanto seu elo mais fraco. A segurança das informações de seus usuários depende de várias camadas de defesa, começando com a autenticação e culminando no controle de acesso. Sendo necessária uma nova abordagem de autenticação baseada em modelagem de confiança contínua.

Silva (2007) faz um questionamento:

Quais são os fatores que mais afetam o desempenho humano, em relação ao uso de senhas? Esta questão parece ainda não ter resposta. Poderia ser qualquer combinação de fatores como sobrecarga de informações, fadiga, estresse, idade, tamanho das senhas, complexidade, número de senhas diferentes, frequência de alteração, ou objetivos incompatíveis entre si. No que diz respeito a senhas, a interferência parece sem dúvida muito plausível, especialmente quando um usuário precisa de lembrar de várias senhas. Também nos parece claro que senhas são um caso muito especial de memória literal, já que detalhes, como a ordem dos caracteres, devem ser lembrados precisamente. O esquecimento de um único caractere ou a falha em lembrar a ordem exata em que estes aparecem invariavelmente implica acesso negado.

É possível notar que estudos são conduzidos em busca de soluções, porque pessoas utilizam senhas pouco seguras mesmo cientes de que essa prática pode gerar prejuízos futuros, o autor apresenta possíveis fatores responsáveis por essa situação tão frequente nos dias de hoje.

2.3.2 Phishing e Spamming

O envio de vírus, também conhecido como *phishing*, é um método de envio de e-mails com anexos ou *links* maliciosos. O objetivo é enganar um destinatário para abrir o anexo/*link* e infectar seu computador. Esta técnica é utilizada para roubar informações pessoais e financeiras (PEREIRA, 2012).

O e-mail malicioso, ou spam, é uma ameaça direta à segurança do computador. Quase todos os computadores conectados à *Internet* recebem pelo menos uma mensagem de e-mail indesejada por dia. Vírus e outros programas maliciosos enviados por e-mail podem destruir dados ou travar um servidor de rede.

Há também a prática do *spamming* e o bombardeio discriminatório por e-mail, ou "bomba de e-mail", é o ato de enviar grandes volumes de mensagens de e-mail para uma caixa de entrada, muitas vezes sem o consentimento do destinatário, numa tentativa de sobrecarregar a largura de banda do servidor de e-mail. A caixa de entrada da vítima será inundada com tantos e-mails que ela não poderá recuperar nenhuma nova mensagem recebida e não poderá mais enviar e-mails enquanto sua conta de e-mail permanecer bloqueada (ANDRADE, 2004).

2.3.2.1 Partes que integram um vírus

Os vírus de computadores são constituídos por três partes, sendo essas partes: vetor de infecção: são os artifícios pelos quais o vírus consegue se reproduzir no computador. Mecanismo de ativação: condição que determina quando o vírus será ativado. Carga útil: nome dado ao papel que o vírus irá desempenhar no computador, além de se propagar (VÍRUS, 2020).

Entende-se que o objetivo final do vírus não será alcançado sem a ajuda do usuário. Quando o seu mecanismo de ativação é executado, começa a duplicação e a infecção de arquivos e programas do computador.

2.3.2.2 Tipos de vírus

No mundo virtual, existem diversos tipos de vírus com nomes diferentes e funções diferentes. Alguns deles são: macro e polimórficos. Macro vírus: são mais conhecidos por serem vírus que podem ser transmitidos pelo computador, via *internet*. Eles podem entrar no sistema com acesso a uma rede e esconder seu endereço de origem. Polimórfico-vírus: é um vírus que pode ter dois caminhos para se fixar na rede: através de um programa físico ou através da *internet*. É um vírus que tem um caminho para entrar no computador onde ocorre uma infecção e outro caminho para infectar os outros computadores na rede (VÍRUS, 2020).

2.3.3 Cookies espiões

Os *Spy Cookies* são informações coletadas de navegadores e armazenadas em um computador, telefone ou outro dispositivo eletrônico. Embora possam ser benéficos em alguns casos, eles também podem permitir que sites maliciosos acompanhem sua atividade *online*, ou são utilizados como espiões, a fim de extrair informações para serem vendidas a outra empresa sem consentimento (COURI, 2009).

Os *Spy Cookies* são cookies baseados na *web* que permitem que os sites monitorem sua atividade de navegação e rastreiam seu histórico de pesquisas, e visualização de produtos, coletam de você informações sobre seu uso de um site e seu anúncio, incluindo como você chegou lá, o que você viu e em quais anúncios você clicou. Os *Spy Cookies* são usados para rastrear sua atividade em sites que têm publicidade. Muitos desses cookies são colocados por sites que você acessa gratuitamente ou por uma taxa (COURI, 2009).

2.3.4 Spyware

A maioria dos programas de *adware* e *spyware* são obtidos inicialmente navegando na *web* ou junto com algum *software* suportado por anúncios não relacionados. Os programas raramente são instalados a partir de um site visível, mas em vez disso, por meio de anúncios de banner de engenharia social, downloads diretos e redes ponto a ponto com nomes de arquivo enganosos. Alguns programas de *adware* e *spyware* são instalados por meio da exploração de *software* em vulnerabilidades (CHIEN, 2005).

Uma vez instalado em um computador, o *spyware* pode ser usado para roubar informações e enviá-las para outro local sem o conhecimento ou consentimento da vítima. O *spyware* profundamente executa ações maliciosas, como gravar toques de teclas e enviá-las a um terceiro.

Um tipo de *software* malicioso bastante conhecido no universo da informática é o *rootkit*, que basicamente consiste em um conjunto de programas que tentam se ocultar no sistema para serem executados sem que o usuário perceba. Os *rootkits* podem se camuflar de várias maneiras, sejam em pastas ocultas ou em drivers de dispositivos, bibliotecas de sistemas ou até mesmo na BIOS do computador (YAMANAKA, 2016).

As aplicações *Spyware* podem registrar ou coletar dados como históricos do navegador, chaves e senhas usadas. Muitas aplicações de *spyware* são consideradas *malware*. O termo "*spyware*" é usado de forma intercambiável com o de "*adware*", embora o *software* classificado como *adware* não seja necessariamente malicioso.

Programas de *adware* e *spyware* são instalados em um sistema de várias maneiras, mas raramente de forma visível e maneira direta. Em um estudo do Instituto Ponemon, 47% dos entrevistados "não tinham ideia" de onde programas vieram. Além disso, 97% não se lembravam de ter visto um contrato de licença de usuário final (CHIEN, 2005).

2.3.5 Cavalo de troia

O Cavalo de Troia é um tipo de *malware* que se disfarça de *software* legítimo. Criminosos virtuais podem utilizá-lo para obter acesso aos sistemas dos usuários. Nesse tipo de ataque, os usuários são enganados por meio de engenharia social para carregar e executar o *malware*. Uma vez ativados os cavalos de troia, eles habilitam acesso de criminosos com o intuito de roubar informações (GTL, 2019).

Normalmente o usuário recebe um e-mail com um anexo, ao abrir o arquivo malicioso, este será instalado no computador, facilitando ao *hacker* o controle total de sua máquina, poderá ver e copiar todos os seus arquivos, descobrir todas as senhas que você digitar, formatar seu disco rígido, ver sua tela e até mesmo ouvir sua voz se seu computador tiver um microfone. Ele poderá gravar tudo o que está sendo digitado por usuários de aplicativos no mesmo computador. Ele também poderá controlar os movimentos do mouse além de iniciar programas que você não estava envolvido no lançamento em primeiro lugar.

2.3.6 Backdoor

O maior perigo do *backdoor* é o desconhecimento do usuário. São considerados como *backdoors* que utilizam os serviços de um Sistema Operacional. Estes são programas de computador que permitem o acesso remoto do usuário ao seu computador ou dispositivo. *Backdoors*, ou alçapões, são uma forma de os projetistas de *software* se fornecerem uma forma de acessar seu computador ou *smartphone* depois de instalar o *software* deles e ligá-lo. Às vezes, estes foram

adicionados para fins de depuração e não são destinados a serem usados de forma maliciosa, mas nas mãos de alguém com má intenção, mesmo uma porta voltada para a depuração pode ser usada como um vetor de ataque (JÚNIOR, 1999).

2.3.7 Home office

Vivemos uma era de grandes mudanças, tanto no país quanto no mundo, ao enfrentarmos a pandemia do coronavírus (*COVID-19*). Nesse contexto, os desafios foram muitos, e uma das áreas que requereu atenção foi a segurança do *home office*. Muitas empresas tiveram que adotar esse modelo de trabalho devido ao isolamento social exigido por muitas organizações. Diante deste cenário crítico houve um número crescente de ataques cibernéticos.

De acordo com a Câmara de Comércio França-Brasil de São Paulo (CCFB-SP), um levantamento realizado pela Trend Micro, líder global em soluções de segurança de dados corporativos e cibersegurança, foram detectadas, entre os meses de fevereiro e março, cerca de 22.700 URLs maliciosas com relação ao *COVID-19*. O número de ameaças superou 900 mil. Foram encontrados também dezenas de aplicativos falsos que geraram 6,7 milhões de vítimas. O uso do nome de grandes marcas como *Heineken*, *Netflix*, *Tramontina* e *Melissa* nos golpes potencializaram o volume de pessoas impactadas.

De acordo com a revista IstoÉ (2021), os ataques cibernéticos a empresas aumentaram 300% na pandemia, questões como adoção generalizada do *home office*, crescimento expressivo de operações digitais, vulnerabilidade de sistemas digitais, essas informações estão presentes no estudo “*How Covid-19 is impacting future investment in security and privacy*”, elaborado pela EY. Foram ouvidas mais de 130 companhias dos cinco continentes, em países como Estados Unidos, Brasil, África do Sul, Suíça, Índia e Dinamarca, entre outros.

Portanto existem algumas práticas que possam auxiliar na manutenção da segurança cibernética no *home office* tais como: manter o sistema operacional sempre atualizado, realizar *download* de *softwares* diretamente do site oficial, evitar abrir e-mails desconhecidos, usar filtro de spams, tomar precauções em acesso à redes públicas, manter o uso constante de backups do sistema, manter senhas dos e-mails e demais redes sociais atualizadas, certificar-se de que, as portas do firewall do computador estão devidamente fechadas, não acessar páginas que não possuem o prefixo do código “*https://*”, que além de sinalizar que o site é protegido

contra ataques de Spoofing – falsificação de identidade na rede – e *Cross-site Scripting* – ataque de injeção de código malicioso - serve de grande auxílio para manter os dados de navegação segura contra outros tipos de códigos maliciosos e ataques subsequentes com o uso de criptografia (JÚNIOR, 2021).

De acordo com Barbosa (2021),

As tecnologias digitais exercem papel crucial nesses tempos de pandemia, tendo um aumento no acesso, bem como o aceleração no uso de algumas ferramentas a Inteligência Artificial, a qual está sendo bastante aplicada na área da saúde, seja no monitoramento de pacientes infectados, na busca de desenvolver vacinas, para citar alguns. Nesse sentido, vale ressaltar que essas transformações provocadas no uso das tecnologias digitais trazem imensos desafios seja no campo ético na regulação de uso, na área de segurança e proteção dos dados, respeito aos direitos fundamentais de privacidade, na era pós-Covid-19.

Mesmo após o período de pandemia, devemos continuar os cuidados com relação ao roubo de dados, protegendo os dados organizacionais. Ainda que a população esteja recuperada e os sistemas de comunicação tenham sido restaurados, é importante que todas as organizações mantenham seus procedimentos de segurança da informação em vigor.

2.2.8 Ransomware

Nos últimos anos, o *ransomware* evoluiu para uma das maiores ameaças à segurança cibernética. Do ponto de vista do criminoso, a *Internet* é um presente enorme, não só para *ransomware*, mas também para *malware* em geral. *Ransomware* é um *malware* que utiliza o computador ou os dados da vítima e está sendo cada vez mais usado por criminosos para gerar receita por meio de extorsão (O'KANE, 2018).

O golpe evoluiu ao longo do tempo, usando várias técnicas para desativar um computador. A evolução mais recente bloqueia a tela do computador e não permite que o usuário acesse nenhum programa. O computador então exibe uma mensagem, geralmente algo como “Você pesquisou materiais ilícitos e deve pagar uma multa”. Muitas pessoas pagam, ou porque acreditam nas mensagens ou porque percebem que é uma farsa, mas ainda querem restaurar o acesso aos seus computadores. Infelizmente, mesmo que uma pessoa pague, os fraudadores geralmente não restauram a funcionalidade. A única maneira confiável de restaurar a funcionalidade é remover o *malware*. Inicialmente confinado a um ou dois países

da Europa Oriental, o malware se espalhou por toda a Europa e através do Atlântico para os Estados Unidos e Canadá (O'GORMAN, 2012).

Essa guerra criptográfica agora representa danos estimados em US\$ 1 bilhão. A *Internet* criou um ecossistema criminoso que dá suporte ao desenvolvimento, implantação e mecanismos financeiros para dar suporte a *malware*. A popularidade das moedas eletrônicas, como o *Bitcoin* cresceu significativamente e a existência desses mecanismos de pagamento anonimizados faz o jogo dos cibercriminosos e fornece um método mais direto de monetizar suas atividades nefastas. Onde o criminoso pede o pagamento do resgate em *Bitcoin*, passando por várias carteiras de criptomoedas realizando lavagem de dinheiro, para cobrir ainda mais os rastros dos criminosos. Considerando o fato de que muitos usuários da Internet parecem desconhecer o *ransomware* e fazem pouco para se proteger. Devido à natureza secreta do *ransomware*, a lucratividade dos empreendimentos criminosos não é clara, mas o que é certo é que o *ransomware* está crescendo (O'KANE, 2018).

A seguir MOHURLE, (2017) lista algumas das medidas preventivas para evitar *ransomware*:

- Os antivírus devem estar sempre atualizados.
- As mensagens de spam não devem ser abertas ou respondidas.
- Faça backup dos dados.
- Personalize as configurações anti-spam da maneira certa.
- Aplique patches e mantenha o sistema operacional, antivírus, navegadores, Adobe Flash Player, Java e outros softwares atualizado.
- Mantenha o Firewall do Windows ativado e corretamente sempre configurado.
- Aumente a segurança do seu Microsoft Office componentes (Word, Excel, PowerPoint, Access entre outros).
- Pense sobre em desativar os serviços remotos.
- Filtrar arquivos EXEs no e-mail.
- Use um pacote de segurança respeitável.
- Use a Restauração do sistema para voltar a um estado limpo conhecido.
- Certifique-se de desativar o compartilhamento de arquivos.

- Desligue as conexões sem fio não utilizadas, como Portas Bluetooth ou infravermelho.
- Tenha cuidado antes de usar a rede Wi-Fi.
- Não clique em links prejudiciais em seu e-mail.
- Não visite sites inseguros e não confiáveis.
- Em vez de clicar em qualquer link da web, digite o endereço web na barra do navegador.

No entanto, medidas como estas não são praticadas pelos usuários, uma vez que os mesmos são a chave para evitar que os criminosos consigam alcançar seus objetivos. Uma vez que este tipo de ataque visa empresas, certo de que as recompensas serão mais lucrativas. Além do crime possuir resgate por pagamento anonimizado, utilizando-se de criptomoedas, uma forma de encobrir rastros.

2.4 DIREITOS E PENALIDADES SOB A NORMA JURÍDICA

O Advogado Criminalista e Professor da Especialização em Ciências Criminais da PUC-Campinas, Leonardo Tieghi enumera algumas orientações às vítimas de crimes cibernéticos:

- Notificar as autoridades policiais e fazer um registro de ocorrência;
- Reunir todas as provas possíveis, como capturas de tela de redes sociais ou e-mails, com o URL da página;
- Utilizar a ata notarial, para comprovar os crimes e para que assim, seja possível buscar a reparação de danos morais e materiais causados perante o Sistema Judiciário, também a efetiva punição dos criminosos (NIC.BR, 2021).

No ano de 2012, foram aprovadas duas regulamentações que modificam o código penal, estabelecendo penalidades para delitos como invasão de sistemas, disseminação de *malwares* ou códigos para roubo de senhas, bem como para o uso não autorizado de informações de cartões de crédito e débito.

A Lei 12.735/12 estabelece a tipificação de condutas praticadas contra sistemas informatizados por meio de sistemas eletrônicos, digitais ou similares, além de exigir a criação de delegacias especializadas.

A legislação 12.737/2012, também conhecida como Lei Carolina Dieckmann, criada depois de um episódio que aconteceu em maio de 2011, quando um invasor acessou cerca de 36 fotos íntimas do computador pessoal da atriz e exigiu cerca de R\$ 10.000,00 (dez mil reais) para que as imagens não fossem

divulgadas. A solicitação não foi atendida pela personalidade que teve suas fotos expostas e replicadas por uma grande quantidade de indivíduos.

A atual regulamentação modifica os artigos 266 e 298 e acrescenta os artigos 154-A e 154-B ao Código Penal, tipificando condutas como a invasão de computadores, a violação de dados de usuários e a derrubada de sites, punindo desde delitos menos graves como invasão de dispositivo informático com pena de três meses a um ano de prisão e multa, até comportamentos mais prejudiciais como obtenção, invasão de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações, com penas de seis meses a dois anos de prisão e multa.

Foi sancionado outro importante documento legislativo, a Lei de Proteção de Dados (LGPD), Lei 13.709/2018, que busca garantir a proteção dos direitos fundamentais e da privacidade, garantindo o livre desenvolvimento da personalidade individual, com o objetivo de proteger as informações de cada cidadão, estabelecendo padrões para as formas de processamento e compartilhamento tanto por meios físicos quanto eletrônicos.

Em 2021, diante do ainda do presente cenário de insegurança virtual, a legislação brasileira recebe mais duas leis. CP passou a contar com o Artigo 147-A, conhecido como crime de perseguição, após a promulgação da Lei 14.132/2021, que busca proteger a liberdade individual contra delitos cometidos no ambiente virtual, com o intuito de constranger a vítima por meio da invasão da privacidade. O Código Penal (CP) e o Código de Processo Penal (CPP) sofreram alterações importantes com a aprovação da Lei 14.155/2021, que incluiu novos elementos para agravar os crimes de invasão, furto, estelionato entre outros crimes mediante fraude eletrônica.

2.5 POLÍTICA DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

A política de segurança da informação é uma ferramenta importante para garantir que uma organização não venha a ser vítima de ataques *hackers*, falhas na tecnologia e outras vulnerabilidades. É um documento fundamental, pois sem ela não saberemos onde devemos ir caso algo aconteça.

A política de segurança descreve a filosofia e as regras básicas para o uso do recurso da informação. Tudo isso independente do ambiente em que a mesma esteja: convencional ou de tecnologia, mas a política não pode, ou melhor, não deve

surgir do nada. É necessário que a política esteja alinhada aos objetivos da organização, com a existência da política fica explicitado o que cada pessoa da organização deve cumprir no que se refere à proteção da informação. A partir dos objetivos de negócio, são definidos os objetivos da segurança da informação, que tem como destaque: possibilitar a realização do negócio no que depende do uso dos recursos de informação (FONTES, 2008).

Segundo as normas da NBR ISO/IEC 27002:2005, um certo número de controles pode ser considerado essencial para uma organização, incluem: proteção de dados e privacidade de informações pessoais; proteção de registros organizacionais; direitos de propriedade intelectual.

Os controles considerados práticas para a segurança da informação incluem: documento da política de segurança da informação; atribuição de responsabilidades para a segurança da informação; conscientização, educação e treinamento em segurança da informação; processamento correto nas aplicações; gestão de vulnerabilidades técnicas; gestão da continuidade do negócio (ver seção; gestão de incidentes de segurança da informação e melhorias (NBR ISO/IEC 27002:2005).

A segurança da informação é uma parte integrada do programa de gerenciamento de risco geral de qualquer organização. Ela é controlada através da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de *software*. Estes controles precisam ser alcançados para garantir que os objetivos específicos de segurança da organização sejam alcançados.

3. MATERIAL E MÉTODOS

O presente estudo foi instituído primeiramente, a partir da técnica de investigação bibliográfica, através de livros, artigos científicos e pesquisas publicadas relacionadas com o tema do trabalho, procurando embasamento do tema e melhor entendimento do mesmo.

Na primeira fase da pesquisa, foi investigadas questões sobre a gestão da segurança de informação, características, pilares, elementos da tecnologia, e seu poder transformador sobre os indivíduos e organizações, avanço da tecnologia e seu uso cotidiano, e quais os tipos de ataques cibernéticos e como podemos evitar cada um deles.

Na segunda fase do trabalho, foi avaliado se os usuários ou funcionários usam práticas de segurança. Os inquéritos foram realizados através de um questionário criado especificamente para o efeito.

3.1 DEFINIÇÃO DO TIPO DE PESQUISA QUANTO AOS OBJETIVOS

Utilizou-se método que envolve um estudo de pesquisa de campo, descritiva. Descritiva porque buscou-se obter dados sobre uma determinada realidade. Descreveu-se os fatos pelo levantamento de dados e pela aplicação de questionários, propôs estudar, registrar, analisar, interpretar e descrever o problema levantado (WAZLAWICK, 2010). A pesquisa de campo focaliza uma comunidade, que pode ser de trabalho, de estudo ou lazer. O estudo é feito por meio de observações, questionários e entrevistas direta focada na realidade do grupo estudado (GIL, 2002).

3.2 DEFINIÇÃO DO TIPO DE PESQUISA QUANTO À ABORDAGEM

A pesquisa quali-quantitativa uniu-se da pesquisa qualitativa e a pesquisa quantitativa, ou seja, as duas não são contrárias ou opostas, mas um complemento. “[...] Esta associação pode estar relacionada ao processo de “tradução” da questão inicialmente qualitativa em estratégias de coleta de dados quantitativos e à (re) tradução dos resultados quantitativos para uma resposta qualitativa” (GÜNTHER, 2006, p.204).

3.3 DEFINIÇÕES DA POPULAÇÃO/AMOSTRA

O objeto de pesquisa, para aplicação da estratégia ocorreu em uma instituição do setor público, que se dispôs em participar do estudo.

3.4 AMOSTRAGEM NÃO PROBABILÍSTICA

Utilizou-se da amostragem não probabilística de caráter intencional, composta de indivíduos que compõem a equipe de funcionários de uma organização do setor público.

3.5 PROCEDIMENTO DE ESCOLHA DA ORGANIZAÇÃO

A primeiro momento foi realizado visitas em organizações públicas de um município do estado de Rondônia, convidando-as para participar do projeto, expondo a proposta, e seus benefícios na gestão da segurança da informação.

Após o aceite da empresa, realizou-se uma reunião com todos os colaboradores da empresa, para informar sobre a aplicação do estudo, e quais procedimentos iriam ser realizados.

3.6 TÉCNICAS E PROCEDIMENTOS DE COLETA

Os dados foram coletados a partir de um questionário online, via Google Drive, por meio de um link enviado para 50 (cinquenta) funcionários. O questionário ficou aberto durante uma semana para receber resposta. Composto de 08 (oito) perguntas fechadas que abordou questão de segurança de dados e proteção de informações em ambientes digitais. Obteve resposta de 20(vinte) pessoas. As questões foram respondidas na opção que melhor representa a opinião do colaborador. Se tratando de uma pesquisa anônima, em nenhum momento foi identificado neste estudo o nome dos participantes e da organização estudada.

3.7 TÉCNICAS E PROCEDIMENTOS DE ANÁLISE

As análises foram feitas a partir do tratamento dos dados do questionário no Google Forms. Em seguida os gráficos com as amostras foram interpretados para conclusão do projeto.

4. RESULTADOS E DISCUSSÃO

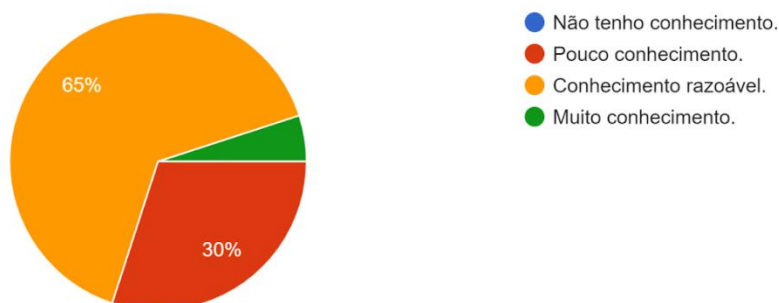
A partir das questões, o Google Forms geriu o tratamento das respostas estatisticamente gerando gráficos, com base nas representações a seguir, analisou-se o grau de conhecimento dos funcionários da instituição.

O gráfico de setores ou circular onde os valores de cada divisão é representado pela proporção dos respectivos valores contidos, com a finalidade de interpretar as porcentagens de um número total, mas também facilitar a visualização das informações.

4.1 EM RELAÇÃO ÀS ORIENTAÇÕES PARA DEFINIÇÃO DE SENHAS PESSOAIS SEGURAS, ASSINALE A OPÇÃO QUE REPRESENTA O SEU CONHECIMENTO SOBRE O TEMA.

A seguir veremos o gráfico que representa o conhecimento do usuário quando questionados sobre a definição de senhas pessoais seguras.

Gráfico 01 – Conhecimento sobre senhas pessoais seguras



Fonte: Autor, 2023

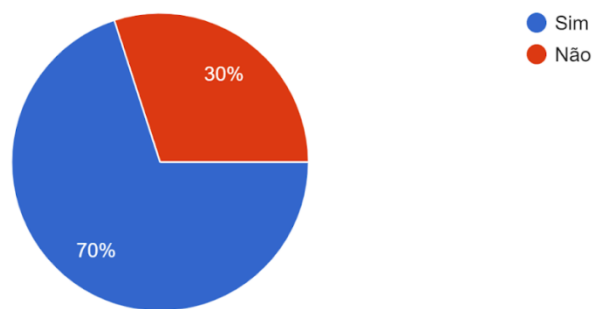
O gráfico acima mostra que 65% dos funcionários, representados pela fatia laranja, têm conhecimento razoável quando questionados sobre seu conhecimento de como definir senhas pessoais seguras e 30% dizem ter pouco conhecimento.

Para uma definição de senhas segura e recomendável que seja complexa utilizando letras maiúsculas e minúsculas, números não sequenciados e símbolos, não use nome, aniversário ou outra informação pessoal. Prefira frases longas que faça sentido só pra você. Mas tenha a ciência que precise lembrar-se dela depois.

4.2 EM RELAÇÃO À PERIODICIDADE DE RENOVAÇÃO DE SENHAS, É DE SEU CONHECIMENTO QUE O RECOMENDADO PARA UMA MAIOR SEGURANÇA NOS AMBIENTES DIGITAIS É QUE ELAS SEJAM ATUALIZADAS FREQUENTEMENTE?

A seguir observaremos o gráfico que representa a opinião dos funcionários quando questionado sobre a recomendação na periodicidade na renovação de senhas para maior segurança nos ambientes digitais.

Gráfico 02 – Periodicidade de renovação de senhas



Fonte: Autor, 2023

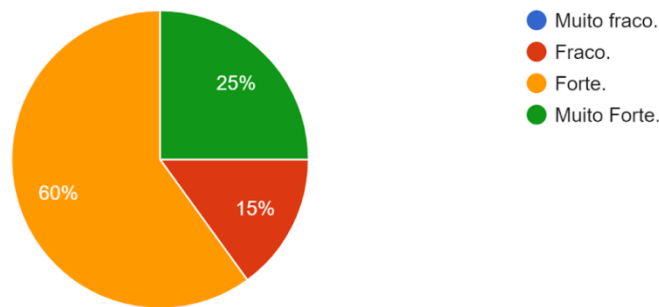
O gráfico da figura 02 mostra que 70% dos funcionários estão cientes da importância de atualizar as senhas regularmente. 30% dizem que não estão cientes da recomendação de renovar as senhas.

Mesmo que suas senhas não haja suspeita de comprometimentos, é essencial que faça a redefinição periodicamente, essa é uma prática para manter sua identidade online segura. No entanto, muitas pessoas tendem a escolher senhas mais fracas e fáceis de lembrar quando são forçadas a alterá-las com tanta frequência. Isso pode realmente aumentar o risco de segurança, já que senhas mais fracas são mais fáceis de serem descobertas por hackers. Sendo mais eficaz ter senhas fortes e exclusivas, em vez de alterá-las com tanta frequência.

4.3 COM BASE NO SEU CONHECIMENTO SOBRE PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO, ASSINALE A OPÇÃO SOBRE O PADRÃO QUE ADOTOU PARA A CRIAÇÃO DE SUAS SENHAS.

A seguir veremos o gráfico que representa o conhecimento do usuário quando questionados sobre a proteção de dados e segurança da informação em relação ao padrão adotado para criação de senhas.

Gráfico 03 – Padrão adotado para criação de senha



Fonte: Autor, 2023

O gráfico acima mostra que 60% dos entrevistados dizem que usam senhas fortes, enquanto 25% usam senhas muito fortes e apenas 15% usam senhas fracas.

Criar senhas fortes dificulta as tentativas de invasão de cibercriminosos e hackers, deve-se também evitar combinações de padrões similares. Com a ferramenta security.org é possível avaliar o quão segura sua senha é, além de ajudar no entendimento de senhas seguras.

Utilizar diversidade de caracteres: Uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais como: (!, @, #, \$, etc.). Quanto mais variados forem os tipos de caracteres utilizados, mais difícil será para um hacker adivinhar a senha.

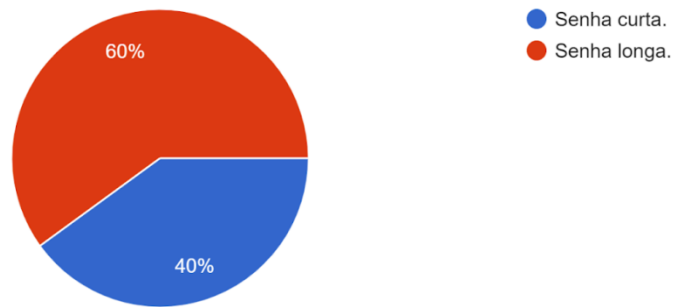
Evitar informações pessoais: Evitar usar informações pessoais óbvias, como seu nome, sobrenome, data de nascimento ou palavras relacionadas a você. Hackers podem facilmente adivinhar ou obter informações sobre você através de pesquisa na internet ou redes sociais.

Lembre-se de que criar senhas fortes é apenas parte da equação de segurança. Também é importante manter seus dispositivos e programas atualizados, ter cuidado com *phishing* e outros golpes online.

4.4 EM RELAÇÃO A NOVAS SENHAS, ASSINALE A OPÇÃO QUE REPRESENTA O TIPO DE SENHA QUE VOCÊ ADOTA AO CRIA-LAS.

A seguir observaremos o gráfico que representa a opinião dos colaboradores quando questionado qual tipo de senha que adota ao criar novas senhas.

Gráfico 04 – Senhas curtas ou senhas longas



Fonte: Autor, 2023

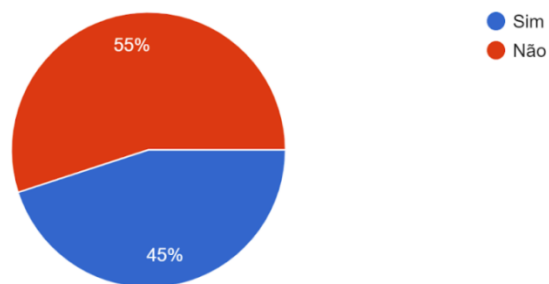
O gráfico da figura 04 mostra que 60% dos entrevistados dizem que usam senhas longas, enquanto 40% usam senhas curtas.

É recomendável a criação de senhas longas, utilize máximo de caracteres que for permitido. Prática que fará toda a diferença na segurança na prevenção de roubos de dados. Quanto mais longa a senha, mais segura ela será.

4.5 RELACIONADO À DIVERSIFICAÇÃO DE SENHAS PARA USOS ESPECÍFICOS, VOCÊ MANTE SENHAS DIFERENTES PARA CADA SITE, APLICATIVO OU SOFTWARE QUE POSSUI CADASTRO?

A seguir veremos o gráfico que representa a opinião dos colaboradores quando questionado qual tipo de senha que adota ao criar novas senhas.

Gráfico 05 – Diversificação de senhas



Fonte: Autor, 2023

O gráfico acima mostra que 55% dos funcionários dizem usar senhas diversificadas para cada site, aplicativo ou software que possui cadastro, enquanto 45% usam as mesmas senhas para varias contas de usuários.

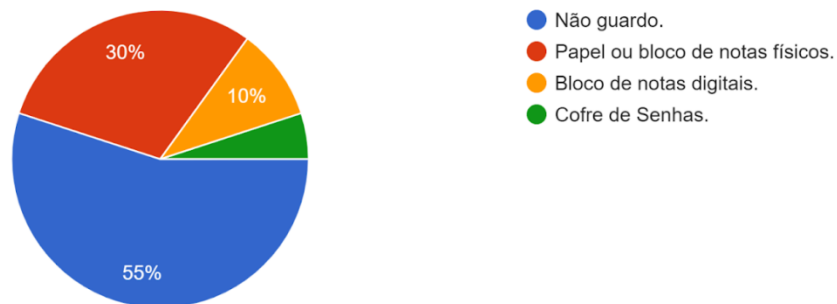
Não utilizar a mesma senha para várias contas. Se um atacante descobrir uma senha, ele terá acesso a todas as outras contas que utilizam a mesma senha,

todas as outras contas de diferentes serviços também ponderar ser acessada pelo invasor. Utilizar um gerador de senhas aleatórias fará com que tenha quantas senhas precisar, sem se preocupar em ficar criando senhas exclusivas constantemente.

4.6 COMO VOCÊ COSTUMA GUARDAR AS SENHAS DE APLICATIVOS E SITES QUE CADASTROU?

A seguir observaremos o gráfico que representa a opinião dos funcionários quando questionado como costuma guardar as senhas de aplicativos e sites que cadastrou.

Gráfico 06 – Guardar senhas



Fonte: Autor, 2023

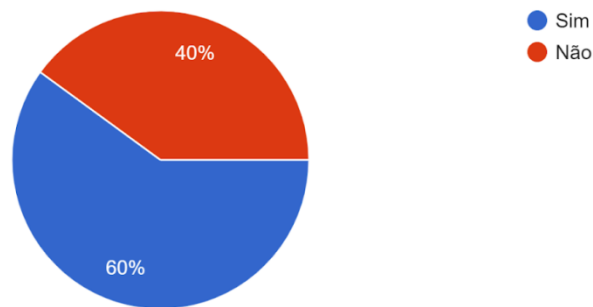
O gráfico da figura 06 mostra que 55% dos entrevistados dizem que não guardar senhas, enquanto 30% anotam em papel ou blocos de notas físicos e 10% utiliza bloco de notas digitais, contra uma pequena fatia representada na cor verde utiliza cofre de senhas.

Utilizar blocos de notas físicos ou digital ou até mesmo papel não é considerado seguro. A melhor forma de guardar senhas é utilizando o cofre de senhas, hoje existem vários aplicativos que possui a função exclusiva para este tipo de serviço. Utilizar um gerenciador de senhas confiável pode ajudá-lo a criar senhas seguras e lembrá-las quando precisar. Isso permite que use senhas longas e complexas para cada conta sem precisar se preocupar em lembrar delas.

4.7 VOCÊ SABE O QUE É A AUTENTICAÇÃO DE SENHA EM DUAS ETAPAS, UTILIZADAS POR ALGUNS SITES E SOFTWARES?

A seguir veremos o gráfico que representa o conhecimento dos funcionários quando questionado sobre a autenticação de senha em duas etapas.

Gráfico 07 – Autenticação de senhas em duas etapas



Fonte: Autor, 2023

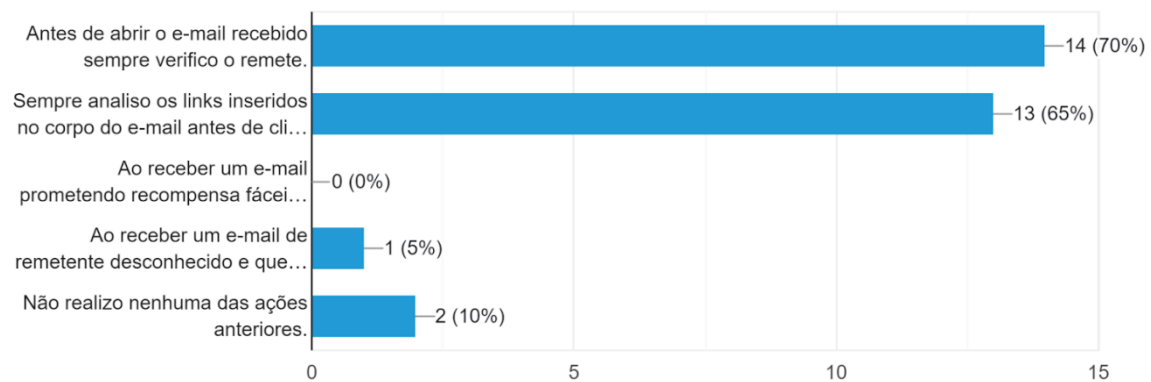
O gráfico acima mostra que 60% dos colaboradores afirma saber o que é autenticação de senhas em duas etapas, enquanto 40% não possui conhecimento sobre o tema.

A autenticação de senhas em duas etapas é uma prática adotada por principais aplicativos e sites atuais, é uma forma de dificultar mais o acesso a conta do usuário, mesmo que a senha esteja comprometida ou seja hackeada, o recurso solicita uma segunda confirmação podendo ser SMS, dispositivo de *token*, biometria entre outros, funciona como uma camada extra na segurança de contas online.

4.8 COM BASE NOS SEUS HÁBITOS AO CHECAR OS SEUS E-MAILS, MARQUE AS OPÇÕES QUE VOCÊ REALIZA (PODE SER SELECIONADA MAIS DE UMA OPÇÃO).

A seguir observaremos o gráfico que representa a opinião dos colaboradores quando questionado sobre os hábitos que adota ao checar os e-mails.

Gráfico 08 – Hábitos ao checar e-mails



Fonte: Autor, 2023

O gráfico da figura 08 mostra que 70% dos funcionários verificam o remetente do e-mail recebido antes de abri-lo, 65% afirma analisar os links inseridos no corpo do e-mail antes de clicá-lo, 5% faz download dos anexos ao receber um e-mail de remetente desconhecido sem analisar as características do e-mail. No questionamento “Ao receber um e-mail prometendo recompensa fácil abro imediatamente e acesso o link disponibilizado” não houve afirmação e 10% dos entrevistados afirmar não realizar nenhuma das ações questionadas.

O e-mail é um ambiente propício para crimes cibernéticos, é importante estar sempre atento, além dos já mencionados acima, listamos outras medidas que auxiliam na prevenção de roubos de informações: Sempre suspeitar de e-mails que solicitam dados pessoais sem estar ciente de quem os solicitou. Duvide de pedidos de ajuda enviados por e-mail, usando temas como: doença, abandono, fome, conflitos armados ou senso de urgência. Faça análise se o e-mail possui erros ortográficos e coerência textual. Sempre fique atento com e-mails que possuem em anexo faturas e boletos.

5. CONCLUSÃO

Investir na implantação de gestão da segurança da informação em uma organização pública traz vários benefícios, tornando um montante de dados e agrupamentos de informações de maneira segura. Sendo indispensável para um bom desempenho administrativo, quando se fala de órgãos públicos, são as organizações, que mais tendem a sofrer as consequências no que diz respeito à carência de conhecimento na área da tecnologia, uma vez que produz dados em volumes excessivos.

No entanto, diante dos constantes ataques de hackers em todo mundo, e a necessidade de manter informações sigilosas em seguranças, buscou-se analisar um determinado órgão público a fim de medir o nível de conhecimento dos funcionários.

Esta pesquisa baseou-se na investigação bibliográfica como metodologia de pesquisa, procurou explicar o problema e suas características para melhor entendimento do mesmo, além de elementos da segurança da informação e seu poder de transformação no desempenho das atividades governamentais.

Este estudo caracterizado como qualitativo busca-se interpretar os resultados obtidos, gerando conhecimento para solucionar questões específicas, com dados consistentes de uma determinada realidade.

Para a coleta de dados foi realizada aplicação de questionários, os dados foram levantados e interpretados. Ao analisar os resultados obtidos no desenvolvimento do estudo, podemos afirmar que a organização está vulnerável perante a segurança da informação, visto que é uma consideração significativa em transações online. A autenticação é vital para proteção contra roubo de identidade e fraude. As senhas são empregadas para autenticar usuários que acessam serviços on-line, mas são vulneráveis a esforços extensivos de hackers por parte de hackers. Propomos o uso de biometria para o processo de identificação que pode ser facilmente integrado aos sistemas existentes. Em particular, estudamos o reconhecimento de impressões digitais como uma nova maneira de autenticar as identidades dos usuários em seus desktops sem a necessidade de hardware adicional, como cartões inteligentes ou outros *tokens* exclusivos.

As senhas são uma parte importante da segurança online, mas também são suscetíveis a roubo e ataques de força bruta. A biometria oferece uma abordagem

alternativa, mas enquanto os computadores não estiverem equipados com a capacidade de ler sua mente ou DNA, você precisará de uma ou duas outras informações para fazer *login* com segurança.

A educação do usuário é a parte mais importante da segurança da informação do usuário final. Bons usuários são a melhor defesa contra vírus, hackers e outras ameaças aos seus dados.

O cenário atual da tecnologia da informação nas instituições públicas municipais realmente necessita de atenção, melhorias, investimentos e capacitação contínua dos servidores dos departamentos de tecnologia da informação. O avanço rápido da tecnologia e a massificação da internet trouxeram inúmeros benefícios para a população, mas também trouxeram desafios significativos para as instituições públicas lidarem.

Identificar as falhas existentes no cenário atual e buscar soluções, juntamente com os investimentos e constante capacitação dos servidores, serão fundamentais para melhorar a infraestrutura tecnológica e a capacidade de fornecer serviços online eficientes e seguros às instituições públicas municipais. Isso fortalecerá a relação entre o governo e a população, facilitando o acesso e fornecendo uma melhor experiência do usuário.

Ao concluir compreendo que este projeto foi fundamental para adquirir novos conhecimentos, pois possibilitou encontrar problemas a serem resolvidos que o cotidiano profissional nos impõe. Proporcionando uma experiência de aprendizado mútuo, pois situações práticas da área de atuação foram estudadas e analisadas. Período dedicado no aprimoramento da carreira.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 17799: Tecnologia da informação - Código de prática para a gestão da segurança da informação**. Rio de Janeiro, p. 02. 2001.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 17799: Tecnologia da informação - Código de prática para a gestão da segurança da informação**. Rio de Janeiro, p. 02. 2001.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação**. Rio de Janeiro, p. 12. 2005.

Barbosa, J. S., Borges, D., de Oliveira, D. C., de Jesus, D. C., & de Miranda, W. F. (2021). A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. *Research, Society and Development*, 10(2), e40510212557-e40510212557.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidente da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 Nov. 2023.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em 26 maio de 2023.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 26 maio de 2023

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 26 maio de 2023.

BRASIL. Lei Nº 14.132, de 31 de março de 2021. Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm. Acesso em 26 maio de 2023.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília, DF, Diário Oficial da União, ed.100, p.1. 28 maio de 2021. Seção 1.

CHIEN, Eric. Techniques of adware and spyware. In: the Proceedings of the Fifteenth Virus Bulletin Conference, Dublin Ireland. 2005.

CNN.São Paulo:Thais Arbex, 2021-.

COURI, Gustavo Fuscaldo. Crimes pela internet. Rio de Janeiro, 2009.

COUTINHO, MATEUS MICAEL et al. ESTUDO DE CASO: PRINCIPAIS PILARES DA SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES. Revista Gestão em Foco - Edição nº 9 – Ano: 2017.

EMMANUEL, V. L. Órgão público. Jusbrasil. 2019. Disponível em: <<https://www.jusbrasil.com.br/artigos/orgao-publico/762827182>>. Acesso em 23 Nov. de 2023

FONTES, E. (2008). Praticando a segurança da informação. Brasport.

FREITAS, A. M. S. de. Órgãos públicos: conceito, natureza e classificação. 2013.

GIL, Antônio Carlos. Como Elaborar Projetos de Pesquisa. Edição SÃO PAULO EDITORA ATLAS S.A. 2002.

GTL, GRUPO et al. XXV SNTPEE SEMINÁRIO NACIONAL DE PRODUÇÃO E TRANSMISSÃO DE ENERGIA ELÉTRICA, 2019.

GÜNTHER, Hartmut. Pesquisa qualitativa versus pesquisa quantitativa: esta é a questão. **Psicologia: teoria e pesquisa**, v. 22, n. 2, p. 201-210, 2006.

JORNAL NIC.br.

JÚNIOR, E. W. R., Nogueira, E. R. L., Mendes, G. F., & da Silva Campos, L. A. (2021). Home office e a segurança da informação em tempos de pandemia. *Revista Eletrônica da Faculdade Invest de Ciências e Tecnologia*, 3(1).

JÚNIOR, José Paulo Narciso Rocha. VIRUS DE INTERNET: PREVENÇÃO E SEGURANÇA NA REDE. *Revista Tecnologia*, v. 20, n. 1, 1999.

MOHURLE, Savita; PATIL, Manisha. A brief study of wannacry threat: Ransomware attack 2017. **International Journal of Advanced Research in Computer Science**, v. 8, n. 5, p. 1938-1940, 2017.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.BR). [olhar cidade] TIC Domicílios – 2021 – Especialista analisa aumento de crimes cibernéticos durante pandemia. Nic.br, 2021. Disponível em: <<https://www.nic.br/noticia/na-midia/especialista-analisa-aumento-de-crimes-ciberneticos-durante-pandemia/>>. Acesso em: 25 maio 2023.

O'GORMAN, Gavin; MCDONALD, Geoff. **Ransomware: A growing menace**. Arizona, AZ, USA: Symantec Corporation, 2012.

O'KANE, Philip; SEZER, Sakir; CARLIN, Domhnall. Evolution of ransomware. **let Networks**, v. 7, n. 5, p. 321-327, 2018.

PEREIRA, Cleber Guedes. Phishing: Conceitos e ações preventivas aplicadas à empresa. 2012.

PRICEWATERHOUSECOOPERS BRASIL LTDA(PWC). Metade das empresas brasileiras foi vítima de crimes econômicos nos últimos dois anos. pwc.com.br, 2020. Disponível em: <[https://www.pwc.com.br/pt/sala-de-imprensa/noticias/metade-das-empresas-brasileiras-foi-vitima-de-crimes-economicos-nos-ultimos-dois-anos.html#:~:text=Os%20principais%20tipos%20de%20crimes,\)%2C%20fraude%20cont%C3%A1bil%20\(22%25/](https://www.pwc.com.br/pt/sala-de-imprensa/noticias/metade-das-empresas-brasileiras-foi-vitima-de-crimes-economicos-nos-ultimos-dois-anos.html#:~:text=Os%20principais%20tipos%20de%20crimes,)%2C%20fraude%20cont%C3%A1bil%20(22%25/)> Acesso em: 25 maio 2023.

REVISTA ISTO É. São Paulo, 30 de Out. 2021.

ROCCIA, Rubens Douglas. Usuários respeitam as normas de criação de senhas seguras? Uma análise de datasets de senhas vazadas. 2021.

SILVA, Denise Ranghetti Pilar da; STEIN, Lilian Milnitsky. Segurança da Informação: uma reflexão sobre o componente humano. **Ciências & Cognição**, v. 10, 2007.

TAKEUCHI, Eduardo Costa. Fatores humanos em cibersegurança uma revisão sistemática da literatura. 2023.

VÉRAS, Alisson LM; RUGGIERO, Wilson V. Autenticação Contínua de Usuários em Aplicações Seguras na Web. In: **Anais do V Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. SBC, 2005. p. 40-51.

VÍRUS de computadores. Direção: Dicionário de Informática. Gravação de Dicionário de Informática. Produção: Dicionário de Informática. Gravação de Dicionário de Informática. YouTube: YouTube, 2020. Disponível em: <https://www.youtube.com/watch?v=LSUwfF9lvgw>. Acesso em: 11 maio 2023.

WAZLAWICK, Raul Sidnei. Uma reflexão sobre a pesquisa em ciência da computação à luz da classificação das ciências e do método científico. **Revista de Sistemas de Informação da FSMA**, v. 6, p. 3-10, 2010.

YAMANAKA, Keiji. Proteção e Segurança em Sistemas Operacionais, 2016.

APÊNDICE A – Questionário

Você está sendo convidado a participar de uma pesquisa para Trabalho de Conclusão de Curso (TCC), onde abordará questão de segurança de dados e proteção de informações em ambientes digitais de órgãos públicos de um município do estado de Rondônia, esta pesquisa é totalmente anônima e de livre participação, devido a isto, busque responder ao questionário da maneira mais sincera possível.

1. Em relação às orientações para definição de senhas pessoais seguras, assinale a opção que representa o seu conhecimento sobre o tema.

- ☐ Não tenho conhecimento
- ☐ Pouco conhecimento
- ☐ Conhecimento razoável
- ☐ Muito conhecimento

2. Em relação a periodicidade de renovação de senhas, é de seu conhecimento que o recomendado para uma maior segurança nos ambientes digitais é que elas sejam atualizadas frequentemente?

- ☐ Sim
- ☐ Não

3. Com base no seu conhecimento sobre proteção de dados e segurança da informação, assinale a opção sobre o padrão que adotou para a criação de suas senhas.

- ☐ Muito fraco
- ☐ Fraco
- ☐ Forte
- ☐ Muito forte

4. Em relação a novas senhas, assinale a opção que representa o tipo de senha que você adota ao cria-las:

- ☐ Senha curta
- ☐ Senha longa

5. Relacionado a diversificação de senhas para usos específicos, você mante senhas diferentes para cada site, aplicativo ou software que possui cadastro?

- ☐ Sim

☐ Não

6. Como você costuma guardar as senhas de aplicativos e sites que cadastrou?

☐ Não guardo

☐ Papel ou bloco de nota física

☐ Bloco de notas digitais

☐ Cofre de Senhas

7. Você sabe o que é a autenticação de senha em duas etapas, utilizadas por alguns sites e softwares?

☐ Sim

☐ Não

8. Com base nos seus hábitos ao checar os seus e-mails, marque as opções que você realiza (pode ser selecionada mais de uma opção).

☐ Antes de abrir o e-mail recebido sempre verifico o remete.

☐ Sempre analiso os links inseridos no corpo do e-mail antes de clicá-los.

☐ Ao receber um e-mail prometendo recompensa fáceis abro imediatamente e acesso o link disponibilizado.

☐ Ao receber um e-mail de remetente desconhecido e que possui anexo, faço o download do anexo sem analisar as características do e-mail.

☐ Não realizo nenhuma das ações anteriores.