SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO SERVIÇO PÚBLICO MUNICIPAL

Robson Moreira da Silva Rocha[1]
Orientador: Prof. MSc, José Ivo Fernandes de Oliveira[2]

RESUMO:

Este artigo tem como propósito verificar o nível de conhecimento sobre segurança da informação em uma instituição pública municipal, a intenção não foi de estruturar um modelo de proteção com base na participação de todos os envolvidos no processo de gestão da máquina pública municipal. Este trabalho provoca o gestor público a ampliar suas habilidades, de maneira a transformar toda a rotina conhecida. Ao escrever este artigo não houve a pretensão de que os indivíduos envolvidos dominassem especificidades da Política de Segurança da Informação ou mesmo do Sistema de Gestão de Segurança da Informação. Contudo, para uma eficaz efetivação, tanto da Política, quanto da sistemática são imperativos o discernimento e o compromisso de toda sua estrutura. Determinou-se que, com abordagem menos técnica, pudesse ter uma melhor implementação e atuação do gestor e servidores em todo seu processo. É claro que a cultura organizacional precisa ser alcançada e atualizada para a realidade onde a base é a tecnologia de forma que se compreendam os aspectos da gestão de risco, integre-se a visão técnica com o viés do gestor público e se alcance as melhores definições e abrangências dos servidores que estão envolvidos nesse processo, uma vez que, 40% dos entrevistados julgam não conhecer a política de segurança da informação na instituição. O artigo está baseado na família da norma NBR ISO/IEC 27000. A pesquisa, bibliográfica, deu enfoque à literatura do estado da arte, e foi implementada um questionário online com perguntas fechadas para verificar o conhecimento dos colaboradores da instituição.

Palavras-Chave: Segurança; Informação; NBR ISO/IEC 27000.

Summary:

This article aims to verify the level of knowledge about information security in a municipal public institution, the intention was not to structure a protection model based on the participation of all those involved in the management process of the municipal public machine. This work provokes the public manager to expand his skills in order to transform the entire known routine. When writing

[1] Aluno do Curso Superior em Tecnologia em Gestão Pública do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso (IFMT) – Campus Barra do Garças.
[2] Professor Mestre, do Curso Superior em Tecnologia em Gestão Pública do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso (IFMT) – Campus Barra do Garças.

this article, there was no claim that the individuals involved would master the specificities of the Information Security Policy or even the Information Security Management system.However, for an effective implementation of both the Politics and the systematics, the discernment and commitment of its entire structure are imperative. It was determined that, with a less technical approach, it could have a better implementation and performance of the manager and servers throughout his process. It is clear that the organizational culture needs to be achieved and updated to the reality where the basis is technology so that the aspects of risk management are understood, the technical vision is integrated with the bias of the public manager and the best definitions and scope of the servers who are involved in this process is achieved, since 40% of respondents believe they do not to know the information security policy in the institution. The article is based on the NBR ISO/IEC 27000 family. The bibliographical research focused on state-of-the-art literature, and an online questionnaire with closed questions was implemented to verify the knowledge of the institution's employees.

Keywords: Security; Information; NBR ISO/IEC 27000

1. Introdução

Com o passar dos anos a tecnologia de segurança da informação foi exigindo novos procedimentos e se adequando às necessidades de cada emissor/receptor de informação. A primeira norma mundial a ser criada foi, a Britânica BS 7799 em 1.999 que deu origem aos requisitos de um Sistema de Gestão da Segurança da Informação (SGSI), gestão de riscos, métricas e medidas, e diretrizes para implementação. Esta família de normas adota um esquema de numeração usando a série de números 27000, que abrange um conjunto de padrões, que é a base da segurança aos recursos (ISO,2020).

Desde o surgimento da ISO - *International Organization for Standardization,* responsável pelo desenvolvimento de centenas de normas internacionais, várias normas de padronizações foram publicadas, por exemplo, a norma ISO/IEC 27000, que fornece uma visão geral do SGSI - Sistema de Gerenciamento de Segurança da Informação. Juntamente com a organização ISO, existe também o IEC - *International Electrotechnical Commission* que também é uma organização mundial que cujo objetivo é de organizar e

divulgar normas internacionais para várias áreas como: elétrica, eletrônica e tecnologias relacionadas (ABNT/IEC, 2020).

Inspirados por essas ações globais de segurança da informação, vários países começaram a adotar sistemas de padronização e normas técnicas. No Brasil o órgão responsável pela padronização é a ABNT - Associação Brasileira de Normas e Técnicas, fundada em 1940, sendo membro fundador da ISO e do IEC. Esta instituição é responsável pelas elaborações e adequações das Normas Brasileiras (NBR), a ABNT, atua em várias áreas, desde certificados de produtos, sistemas e rotulagem ambiental, como também, na implementação de políticas públicas, garantindo a defesa do cidadão (ABNT/IEC, 2020).

Atualmente a norma ABNT NBR ISO/IEC 27000 proporciona uma percepção de como os padrões se encaixam, ou seja, ela fornece uma visão geral a família ISO/IEC 27000, podendo ser proposta às organizações. No decorrer deste trabalho, será abordada as normas ISO/IEC 27001, que é padrão e referência internacional para Gestão da Segurança da Informação, e a ISO/IEC 27002, que possui um conjunto de práticas para auxiliar na aplicação do SGSI.

Por consequência, a escrita deste trabalho está justificada sob a hipótese de que é possível uma nova visão a respeito do Sistema de Segurança da Informação, que deve ser sempre avaliado e modificado, devido às constantes mudanças em virtude da evolução dos ataques, nas estruturas das tecnologias que fazem parte deste sistema indispensável. Dessa maneira, este trabalho buscará responder qual é o nível de conhecimento dos colaboradores de uma determinada Prefeitura Municipal do Estado de Goiás em relação à segurança dos seus ativos informacionais? Para isso, será aplicado um questionário online com perguntas fechadas, cujo objetivo é avaliar o nível de conhecimento dos colaboradores dessa instituição.

O desenvolvimento desse artigo está dividido da seguinte forma. A primeira que é a introdução, onde é feito um breve levantamento do caráter evolutivo com uma abordagem histórica e conceitual da Informação e Segurança da Informação, o segundo capítulo, busca esclarecer as características conceituais sobre informação e Sistema da Informação. No terceiro capítulo é traçado pesquisas sobre a segurança da informação no setor público municipal e por último, verificar os resultados de como é estabelecido uma política de segurança da informação no âmbito municipal.

2. Caráter Evolutivo da Informação e Segurança da Informação

Pensar na segurança institucional da informação, na vulnerabilidade e na exposição aos riscos é uma novidade dentro da Administração Pública, porém, devido ao número crescente de notícias sobre violações, invasões e ameaças ocorridas dentro das instituições, discussões acerca de normas e condutas tornaram-se indispensáveis na atualidade, na tentativa de resguardar o patrimônio e a integridade física de seus integrantes (HORTA, 2016, p. 281).

Neste sentido, há de se observar que as informações de uma administração pública, seja na Educação, Saúde, Ação Social, Fiscal ou Tributária, são conteúdos que sempre estão sendo compartilhados com outros órgãos e ministérios. Para tanto a segurança das informações tem que ser objeto de preocupação para o gestor pública municipal. Investimento no setor de Tecnologia da Informação (TI) é garantir a preservação e proteção das informações.

Neste cenário, diariamente tem-se notícias de ataque de vírus *ransomware* causando enorme prejuízo não só intelectual, monetário e fiscal.

> O *ransomware* é um tipo de malware que sequestra o computador da vítima e cobra um valor em dinheiro pelo resgate, geralmente usando a moeda virtual Bitcoin que torna quase impossível rastrear o criminoso que pode vir a receber o valor. Este tipo de "vírus sequestrador" age codificando os dados do sistema operacional de forma com que o usuário não tenha mais acesso (CARDOSO, 2017, s/p).

A políticas de Segurança da Informação iniciou-se com o BSI (*British Standard Institute*), executor da norma BS 7799 Parte 1, em dezembro de 1995. Sendo apontado como o mais íntegro padrão para o funcionamento da Segurança da Informação no mundo, podendo ser implementado a ele um sistema de defesa fundamentado em controles e práticas estabelecidos por normas e práticas internacionais (CARVALHO, 2009).

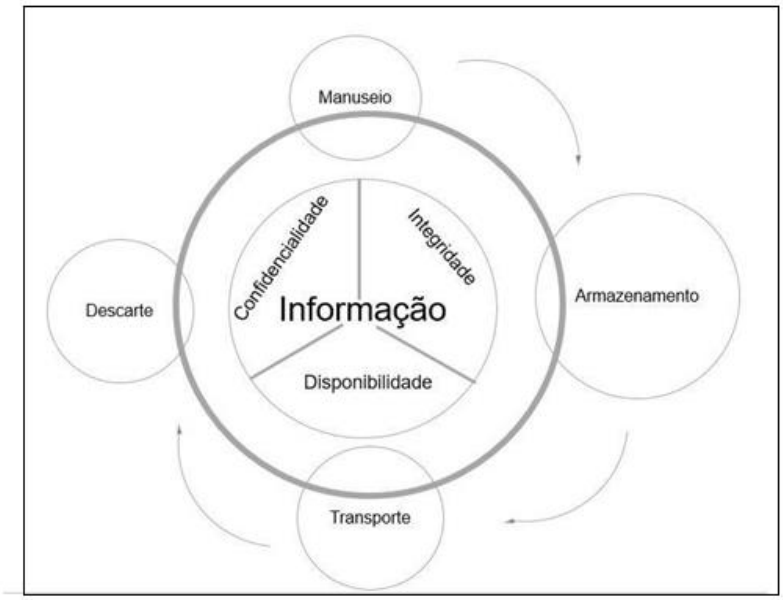
A lei Sarbanes-Oxley ou SOX, como também é conhecida, é uma norma internacional aprovada em 2002 em convenção americana como resultado das desordens contábeis e financeiras de empresas como Enron, WordCom e Tyco, que elanguesceram o mercado de capitais. Sendo composta por 1.107 artigos que determinam punições severas para quem tentar burlar, passiveis de multas de até US$ 5 milhões e até 20 anos de prisão aos infratores (CARVALHO, 2009).

2.1 Características Conceituais sobre Informação e Sistema da Informação

Segundo Rezende (2011), todo sistema, utilizando ou não recursos de tecnologia da informação, que manipula ou gera informações podem ser genericamente considerados sistema de informação. De acordo com o próprio conceito de sistema, é árduo conceber algum sistema que não fere informação, independentemente de seu nível, tipo e uso.

A informação apresenta-se em grande dimensão atualmente, disponibilizadas nos mais diversos meios de comunicação, estabelecendo de todos a seleção e organização das informações para a sua efetivação e utilização. O ciclo da vida da informação, figura 01, é composto e identificado pelos momentos vividos pela informação e que a colocam em risco. Esses momentos acompanham os ativos físicos, humanos e tecnológicos que fazem uso, alteram ou descartam a informação (REZENDE, 2011, p. 40).

Figura 1 - Ciclo de Vida da Informação



Fonte: Adaptado de SÊMOLA, 2003, p. 11

2.2.1 Sistemas de Informação

O sistema de informação, a despeito do seu nível ou classificação, tem como propósito auxiliar os métodos de tomada de decisões nas instituições. Se os sistemas de informação não sugerir atender a esse objetivo, sua existência não será significativa (REZENDE, 2011). O foco dos sistemas de informação está direcionado para a gestão da instituição, pois este está relacionado com os quesitos de qualidade, produtividade, perenidade e competividade no serviço público.

Os sistemas de informação poderão contribuir significativamente para a solução de muitos problemas, desse modo o esforço das instituições deve-se concentrar nos níveis superiores dos sistemas de informação que contenham um processo estratégico, no seu modelo de gestão, que detenha a segurança necessária para efetiva guarda e distribuição das informações.

2.3 Segurança da Informação

Conforme a Norma ABNT NBR ISO/IEC 27002, “a Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade da gestão, maximizar o retorno sobre os serviços e a transparência”.

> A Segurança refere-se aos ativos de informação porque é resultado de instrumentos como diretrizes, normas, bens, em conjunto com outros processos da gestão do negócio. Devem-se diferenciar os ativos da Tecnologia da Informação – *hardware* e *software*, basicamente – dos ativos que fazem parte do escopo da Segurança da Informação. Normalmente, os ativos de TI são equivocadamente avaliados como sendo os mesmos da Segurança da Informação (RAMOS, 2008)

Considerando à diversidade dos sistemas, e a multiplicação de usuários e das aplicações, e como consequência do aumento das ameaças, a Segurança da Informação tornando-se um processo cada vez mais significativo nas instituições públicas. Desse modo, torna-se necessária avaliar o objeto da segurança, para adotar métodos de obtenção de sistemas ou equipamentos. Há a necessidade de se constatar o retorno do investimento, ou seja, se o montante do investimento é condizente com o ativo que se quer investir. (CARVALHO, 2009).

O fato de existir uma Política de Segurança da Informação já é considerado motivo de sucesso, porque sua elaboração deve estar de acordo com os propósitos, atividades e finalidades da gestão do município. Além do mais, deve considerar a cultura organizacional de cada setor, empenho e suporte de todos os níveis funcionais, para que sua execução seja efetiva. (CARVALHO, 2009).

> Divulgar a política de segurança da informação é fator importante e deve alcançar todos os níveis setoriais da administração pública, sejam eles chefes setoriais, servidores ou comissionados, para que seja efetiva, no todo. Após a formalização da política da segurança pública, faz-se necessário treinamento e qualificação, diferenciado para cada grupo para que haja entendimento correto dos requisitos de Segurança da Informação, da análise de riscos e da gestão de riscos (CARVALHO, 2009, p. 20).

Com a implementação de um eficiente processo de gestão de incidentes de segurança, associado à constante medição e aperfeiçoamento de sua gestão, ou seja, identificar os riscos e tratamento de uma maneira ordenada e contínua que conseguirá tomar decisões considerando os componentes do risco e os objetivos para que as ações assegurem para que estes mesmos riscos se deparem em níveis aceitáveis (CARVALHO, 2009).

As redes de computadores, em particular a Internet, rede que conecta milhões de computadores em todo o mundo, veio para democratizar o acesso às informações, contudo, conectado a isto, há que se analisar as condições de segurança envolvido neste processo. Nesse caso, é fundamental que se tenha muito bem caracterizado os critérios para uma boa utilização e proteção das informações. A política de segurança é a realização destes critérios (CARVALHO, 2009).

A Política de Segurança da Informação foi produzido pelo *Security Officer* em concordância com o código de ética da instituição, ligado às leis vigentes no país, sendo reconhecido internacionalmente com as melhores práticas e padrões de segurança. O propósito da política de segurança da informação é analisar os princípios e diretrizes da segurança seguidas pela organização, que necessitará ser seguida pelos integrantes.

> Na política de segurança da informação encontram-se a implementação da Segurança da Informação, a formalização para proteção, controle e monitoramento das informações e dos ativos de informação. Também é na política de segurança da informação que encontra o comprometimento da alta administração com a proteção da informação, o que embasa a colaboração de todos os integrantes no ciclo de vida da informação (BEAL, 2005).

Ferreira (2003) define que o efeito da utilização planejada de objetivos, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas são envolvidos pelo Sistema de Gerenciamento de Segurança da Informação (SGSI), ou *Information Security Management System (ISMS*). O organismo municipal que concretize um SGSI compreenderá os ativos que estão sendo

protegidos, o gerenciamento de riscos, os objetivos de controles e controles implementados.

2.4 Estabelecendo uma Política de Segurança da Informação

Estabelecer uma política de segurança da informação é de fundamental relevância para as instituições públicas nas ações de prevenção da segurança, tendo grande importância para o sucesso da gestão. Por ter uma grande abrangência divide-se em três blocos: diretrizes e normas, procedimentos e instruções, todos atribuídos respectivamente às camadas estratégica, tática e operacional (NBR ISO/IEC 27001, 2006).

> As diretrizes têm o papel estratégico de expressar a importância que a organização dá a informação, comunicando também aos servidores seus valores e seu comprometimento com a aplicação e incorporação da segurança à cultura da administração municipal. Além disso, devem as diretrizes expressar as preocupações dos executivos e definir uma linha de ação orientando as atividades táticas e operacionais (CARVALHO, 2009, p. 32).

Ela ainda define as responsabilidades dos detentores das informações, os índices e indicadores do nível de segurança, controles de conformidade legal, requisitos de capacitação de usuários, mecanismos de controle de acesso físico e lógico, registro de incidentes, auditorias e gestão da continuidade dos negócios (NBR ISO/IEC 27001/2006). Para tanto, os:

> Critérios normatizados para admissão e demissão de funcionários, criação e manutenção de senhas, descarte de informação em mídia magnética ou em papel, desenvolvimento e manutenção de sistemas, uso da Internet, acesso remoto, uso de notebooks, contratação de serviços terceirizados e classificação das informações, são alguns exemplos de normas de uma típica Política de Segurança da Informação (SEMOLA, 2003, p. 106).

O planejamento da política de segurança deve ser feito tendo como diretriz o caráter geral e abrangente de todos os pontos, incluindo as regras que necessitam ser acatada por todos. Essas regras devem especificar procedimentos e controles necessários para proteção das informações, quem pode acessar o que e como e quais sistemas poderão ser acessados. Esse caráter geral permite à política controlar, ou melhor, servir de orientação para

todas as demais condutas referentes à Segurança da Informação (NBR ISO/IEC 27001, 2006). Em relação às orientações da NBR ISO/IEC 27001 (2006), aconselha-se as seguintes orientações:

> [...] (i) Definição de Segurança da Informação, resumo das metas, do escopo e a importância da segurança para a instituição, enfatizando seu papel estratégico como mecanismo para possibilitar o compartilhamento da informação e o andamento dos negócios. (ii) Declaração de comprometimento do corpo executivo, apoiando as metas e os princípios da Segurança da Informação. [...] (BRASIL, NBR ISO/IEC 27001, 2006).

Considerando o avanço tecnológico no século XXI, é comum compreender o quanto é complicado a evolução e, especialmente, a preservação e inovação da Política de Segurança da Informação em toda a sua dimensão. Percebe-se como fator de mudança no que foi proposto nesse estudo, não a proposta de nova política de segurança pública, mas a transformação metodológica da inserção de modelos de segurança já utilizados no âmbito da administração privada de grandes empresas. O que se propõe é a adoção dos mecanismos mencionados para adoção de um modelo de gestão pública que tenha a dinamismo e proteção dos dados.

Com a evolução da tecnologia, os ataques cibernéticos estão sendo aprimorados a cada dia e cada vez frequentes. Com toda essa evolução os hackers estão causando ataques cada vez mais arrasador, com isso, em fevereiro de 2020 foi aprovado o Decreto Federal nº 10.222 que aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber) que tem como intuito, proteger o espaço cibernético (REUTERS, 2019).

3. Método

Primeiramente, foi realizado um levantamento bibliográfico em livros, artigos acadêmicos e buscas em bancos de dados, acerca do tema exposto. A coleta dos dados ocorreu de forma online, onde obtivemos 15 (quinze) participantes, respondendo um total de 23 (vinte e três) perguntas de múltiplas escolhas.

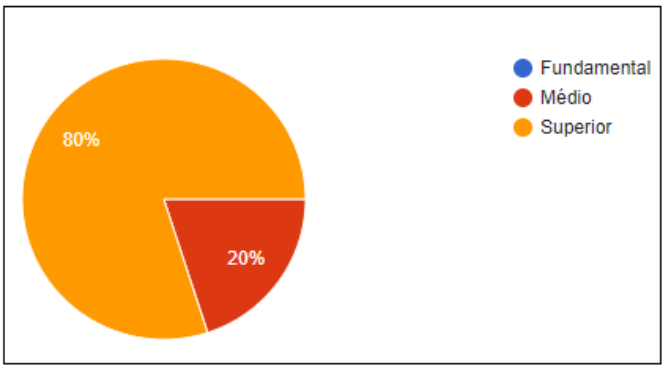
O estudo foi aplicado junto à secretaria de administração e finanças de um determinado município do Estado de Goiás com o propósito de verificar se os colaboradores dessa instituição têm conhecimento relacionado à segurança da informação. Foi montado um questionário estruturado que aborda assuntos referentes ao tempo que cada colaborador trabalha na instituição, como também, assuntos relacionados à gravidade da perda ou vazamentos de informações da instituição. Além disso, foi abordado tópicos relacionados à troca de senhas e se existe treinamento fornecido pela instituição e, principalmente, se a administração possui algum tipo de política voltada para segurança da informação.

4. Resultado e Discussões

Os colaboradores que responderam de forma voluntária ao questionário, consistiram em 60% do sexo masculino e 40% do sexo feminino como mostra o gráfico abaixo.

Diante das respostas obtidas, foi constatado que 80% dos entrevistados possuem formação acadêmica e 20% ensino fundamental, não tivemos nenhum entrevistado que se enquadrava no ensino fundamental, como pode ser visto no gráfico.

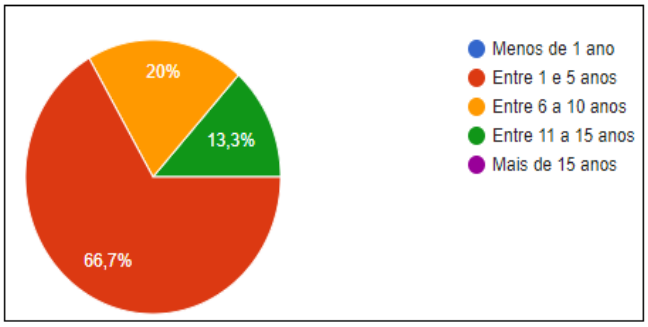
Figura 2 - Nível Educacional



Fonte: Elaborado pelo autor

Considerando o tempo que cada colaborador atua na instituição, apenas 66,7% dos colaboradores se enquadraram no período de 1 a 5 anos, 20% trabalham entre o período de 6 a 10 anos e 13,3% são colaboradores a mais de 11 anos como mostra no gráfico abaixo.

Figura 3 - Tempo de serviço na Instituição

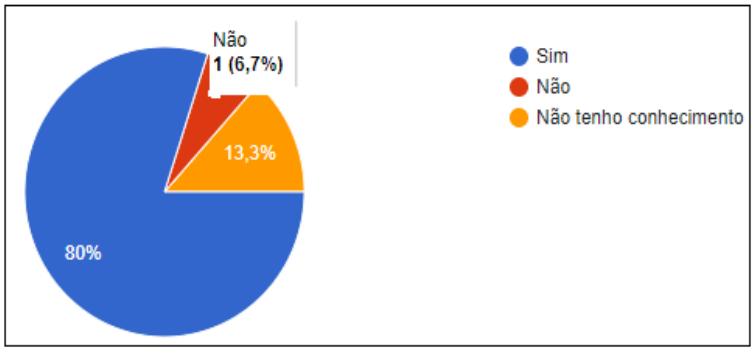


Fonte: Elaborado pelo autor

Foi possível constatar que existe um setor de Segurança da Informação na instituição, contudo, possui apenas 01(um) colaborador como pode ser visto no decorrer da pesquisa. Pode-se observar que 73,3% do efetivo atua no setor administrativo e apenas 20% trabalha no setor de finanças. Quando questionados se existe algum debate relacionado ao tema Segurança da Informação, 20% dos entrevistados responderam que nunca debate sobre tal assunto. Logo, obtivemos uma resposta bem expressiva para aqueles que as vezes discutem sobre o tema exposto com um total de 66,7% e 13,3% sempre debate sobre o assunto.

Dos 15 entrevistados, apenas 13,3% disseram não ter conhecimento se o computador usado para trabalhar possui algum programa antivírus. Enquanto 80% afirmaram que os computadores possuem programa antivírus e 6,7 responderam não possuem antivírus no computador.

Figura 4 – Proteção antivírus no computador



Fonte: Elaborado pelo autor

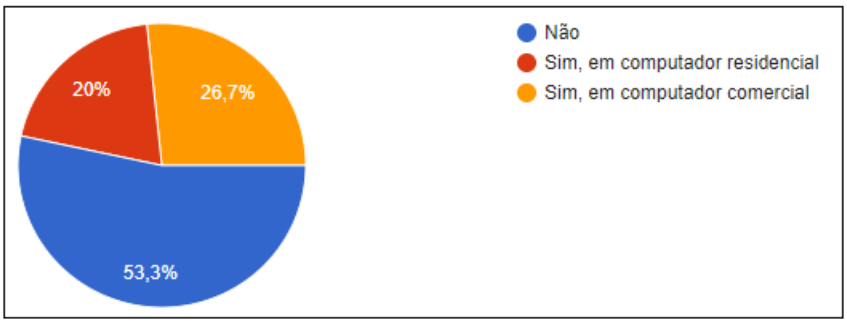
Ao executar algum arquivo removível, recomenda-se que seja utilizado algum programa antivírus para que o computador fique protegido de qualquer ameaça virtual. Diante disto, foi perguntado aos entrevistados se é executado tal ação. E, 26,7% responderam de forma afirmativa, já aqueles que não realizam tal ação ou que as vezes realizam obteve-se o mesmo percentual de 33,3%. Apenas 6,7% respondeu que nunca utiliza programa antivírus em arquivos de mídia removível.

Quando abordados em relação ao monitoramento do uso da internet por parte dos colaboradores de TI da instituição, 66,7% dos entrevistados responderam que existe monitoramento e apenas 20% não tem conhecimento em relação a esse monitoramento e 13,3% responderam que não existe monitoramento por parte dos colaboradores de TI. No entanto, quando questionados em relação ao conhecimento de vírus e de códigos maliciosos, como por exemplo: *Spam, Trojan, Malware e Phishing*, 60% dos entrevistados responderam ter conhecimento sobre tais vírus e códigos maliciosos, 33,3% não conhece e 6,7% não tem conhecimento.

Devido ao aumento de ataque de vírus *ransomware*, foi perguntado se algum dos colabores conhece ou já foi vítima de algum tipo de ataque virtual, e 53,3% negaram conhecer ou serem vítimas de tais ataques e 20% diz

conhecer ou já ter sofrido algum tipo de ataque virtual com computadores residenciais e 26,7% sofreu ou conhece alguém que tenha sofrido ataque virtual em computadores comercial, como mostra no gráfico.

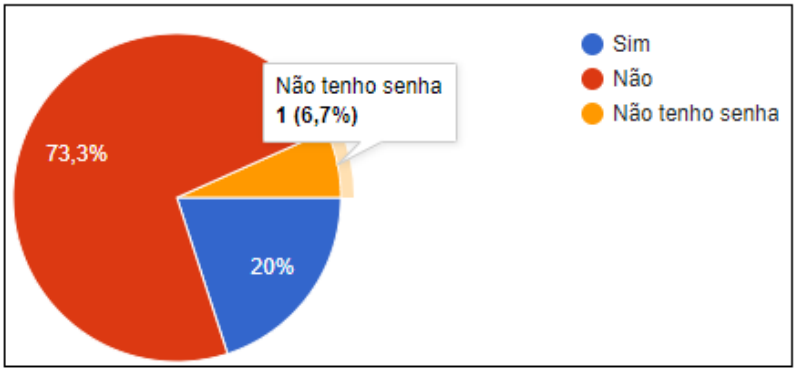
Figura 5 – Vítimas de ataques virtuais



Fonte: Elaborado pelo autor

Com relação a troca de senha do sistema 73,3% dos entrevistados responderam que não realiza a troca com frequência e 6,7% não possui senha no sistema operacional e 20% dos entrevistados a realizam, conforme figura 06 abaixo.

Figura 6 – Troca periódica de senhas



Fonte: Elaborado pelo autor

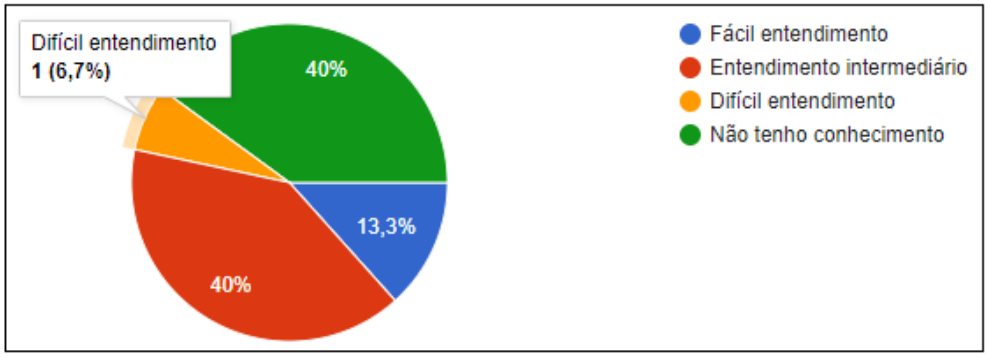
Outro fato que chamou muita atenção é que 60% dos entrevistados não conhecem se as senhas seguem algum padrão relacionado a política de segurança, 26,7% dizem que as senhas seguem um padrão e 13,3% não tem conhecimento em relação ao assunto. Foi abordado se ambos os colaboradores têm conhecimento em relação ao sequestro digital e banco de dados, 86,7% já ouviram falar do assunto exposto e apenas 13,3% não ouviu falar sobre o assunto.

Em relação a existência de algum tipo de treinamento de conscientização sobre segurança da informação por parte da instituição, no qual obtivemos um número bem expressivo de 86,7% dos entrevistados alegaram não receber nenhum tipo de treinamento de conscientização sobre segurança da informação por parte da instituição e apenas 13,3% afirmaram receber treinamento.

Como pode ser observado a instituição possui um setor de SI, contudo, observa-se que existe pouca divulgação em relação ao departamento de SGSI, por parte da instituição, pois 60% dos entrevistados alegam não ter conhecimento da existência desse departamento, enquanto 13,3% diz ter conhecimento e 26,7% alega não existir tal departamento. Foi realizado um levantamento referente ao conhecimento dos colaboradores em relação a política de segurança da informação existente na instituição, onde foi considerado uma escala linear de 1 a 5 respectivamente desconheço totalmente e conheço totalmente, 40% dos entrevistados consideraram o nível de conhecimento 3.

Contudo, quando questionados em relação a compreensão da política de segurança da informação na instituição, 40% dos entrevistados consideram não ter conhecimento de tal política por parte da instituição e 40% consideraram o entendimento como intermediário, 13,3% considera que a compreensão é de fácil entendimento e apenas 6,7% considera de difícil entendimento, conforme figura abaixo.

Figura 7 – Classificando a compreensão sobre Política de Segurança da Informação na instituição

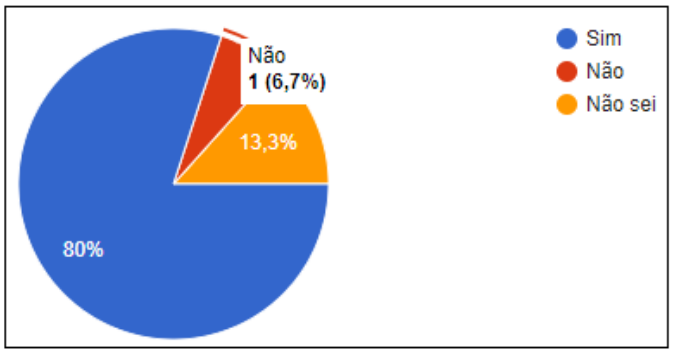


Fonte: Elaborado pelo autor

Os colaboradores, consideram que o vazamento das informações é muito prejudicial para instituição, pois, obtivemos um total de 60% das respostas, enquanto, 33,3% consideram o vazamento de informação apenas prejudicial e 6,7% acredita ser pouco prejudicial. Quando questionados em relação aos métodos de controle para acesso aos meios tecnológicos e informações não pública 73,3% responderam ser utilizado meios como usuário e senha e 26,7% utilizam certificado digital. Logo, os colaboradores também foram abordados em relação aos meios de proteção utilizados em seu ambiente de trabalho e os dois mais apontados foram antivírus com 53,3% e backup com 33,3% como os mais utilizados.

Dos 15 colaboradores entrevistados, 80% reconhece que existe um departamento de SI, seja ele, terceirizado ou não, 13,3% não soube responder e 6,7% disseram que não existe esse departamento, conforme figura 08.

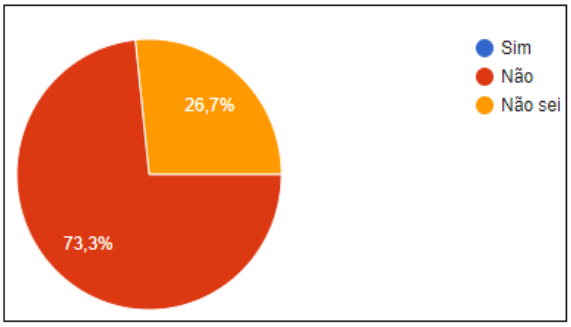
Figura 8 – Existência de departamento de SI



Fonte: Elaborado pelo autor

Porém, 73,3% reconhecem que não existe nenhuma campanha, cartilha ou recomendações relacionadas à segurança da informação por parte da instituição e 26,7% não soube responder.

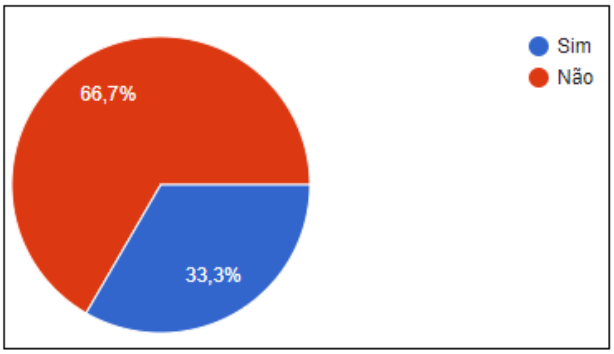
Figura 9 – Campanha institucional sobre SI na instituição



Fonte: Elaborado pelo autor

Como o trabalho foi estruturado nas normas ISO/IEC 27000, foi perguntado aos entrevistados se ambos tinham conhecimento de tal norma e 66,7% responderam que não conhecem e apenas 33,3% tem conhecimento.

Figura 10 – Conhece a norma ISSO/IEC 27000



Fonte: Elaborado pelo autor

5. Considerações finais

É notável, que mais de 50% dos entrevistados possuem uma alfabetização mais rebuscada e atuam na área pública por um período de tempo considerável. Logo, sabem da importância de proteger o computador contra possíveis danos causados por vírus, códigos maliciosos ou engenharia social, por esses motivos, grande parte dos entrevistados consideram importante uma varredura de antivírus em dispositivo móvel, visto que, existe uma grande probabilidade do dispositivo está com algum tipo de vírus que pode danificar de forma temporária ou permanente o computador. Devido ao aumento de ataques virtuais nos últimos tempos, metade dos entrevistados não foi vitima e nem conhece ninguém que possa ter sofrido algum ataque virtual. Contudo, um ponto de destaque que requer bastante atenção foi que cerca de 73,3% dos entrevistados não realiza troca periódica das senhas, tendo em vista, que um invasor pode descobri a senha e acessar dados confidenciais de forma discreta.

Ao se falar, sobre a política de segurança da informação na instituição, mesmo com todos os avanços tecnológicos cerca de 40% dos colaboradores entrevistados julgam não ter conhecimento dessa política dentro da instituição. Logo, 80% dos colaboradores reconhecem que existe um departamento de SI

dentro da instituição, outro ponto que chama muito a atenção, é que mais da metade dos entrevistados alegaram não existir uma campanha, cartilha ou recomendações relacionadas à segurança da informação. Aproximadamente, 66% dos entrevistados reconhecem que não tem conhecimento sobre a família ISO/IEC 27000, com isso, fica o seguinte questionamento, a falta de conhecimento em relação a política de segurança da informação na instituição, se da por falta de divulgação do órgão público ou por falta de iniciativa do colaborador?

A política de segurança de informações deverá ir além dos elementos que estão relacionados exclusivamente com sistemas de informação e os elementos computacionais, devendo estar integrada com as políticas de segurança e ao plano estratégico de informática da instituição municipal. Para trabalhos futuros, julga-se interessante analisar a profissionalização e divulgação do departamento de SI, e analisar a segurança da informação em nuvem e as novas ameaças.

6. REFERÊNCIAS

BRASIL. ABNT (Associação Brasileira de Normas Técnicas). Disponível em: http://www.abnt.org.br/abnt/conheca-a-abnt. Acessado em 30 de Julho de 2020.

_____. ABNT/IEC. Disponível em: https://www.cb26.org.br/iec. Acessado em 30 de Julho de 2020.

_____. ABNT NBR ISO/IEC 27001: Tecnologia da informação, técnicas de segurança, sistemas de gestão de segurança da informação, requisitos. Rio de Janeiro: ABNT, 2006.

_____. ABNT NBR ISO/IEC 27002: Tecnologia da informação, técnicas de segurança, código de práticas para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2007.

_____. Decreto Federal nº 10.222 de 05 de Fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em:

http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm. Acessado em 09 de Setembro de 2020.

BEAL, Adriana. Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

CARDOSO, Pedro. O que é *Ransomware*? TECHTUDO. 07 de maio de 2017. Disponível em: https://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html. Acessado em 31de março de 2019.

CARVALHO, Rodrigo de Oliveira. Segurança da Informação nas Organizações. Centro Universitário de Brasília – UNICEUB. Curso de Administração. Brasília, 2009. TCC de Graduação.

FERREIRA, F. Segurança da Informação. Rio de Janeiro: Ciência Moderna 2003

HORTA, Rodrigo Otávio da Silva. A gestão da segurança institucional na Administração Pública. Boletim Científico ESMPU, Brasília, a. 15 – n. 47, p. 277-293 – jan./jun. 2016.

RAMOS, Anderson. Security Officer 1: guia oficial para formação de gestores em Segurança da Informação. 2. ed. Porto Alegre: Zouk, 2008.

REZENDE, Denis Alcides; ABREU, Aline França de. Tecnologia da Informação a Sistemas de informação Empresariais: o Papel estratégico da informação e dos sistemas de informação nas empresas. 8 ed. São Paulo: Atlas, 2011.

REUTERS**.** Brasil sofreu 15 bilhões de ataques cibernéticos no 2º trimestre, diz estudo. FOBRES. 06 de agosto de 2019. Disponível em: https://forbes.com.br/last/2019/08/brasil-sofreu-15-bilhoes-de-ataques-ciberneticos-no-2o-trimestre-diz-estudo/. Acessado em 09 de Setembro de 2020.

SEMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva**.** Rio de Janeiro: Elsevier, 2003.

_____. Marcos. Você já fez uma análise de riscos de verdade. Rio de Janeiro, n. 41, 2002.

SOARES, André. Segurança institucional. Disponível em:_http://www.inteligenciaoperacional.com/index.php?option=com_content&view=article&id=227&Itemid=286. Acessado em: 01 de março de 2019.

ISSO (Organização Internacional de Padronização). Disponível em: https://translate.google.com/translate?hl=pt-

BR&sl=en&u=https://www.iso.org/home.html&prev=search&pto=aue. Acessado em 27 de Julho de 2020.

APÊNDICE A – Questionário de Avaliação.

1) Sexo?
[ ] Feminino
[ ] Masculino
[ ] Outros

2) Nível de escolaridade?
[ ] Fundamental
[ ] Médio
[ ] Superior

3) A quanto tempo trabalha na Instituição?
[ ] Entre 0 e 5 anos
[ ] Entre 6 a 10 anos
[ ] Entre 11 a 15 anos
[ ] Entre 16 a 20 anos
[ ] Mais de 20 anos

4) Você trabalha em qual setor na sua empresa?
[ ] Administração
[ ] Financeiro
[ ] Segurança da Informação (SI)
[ ] Outros

5) Com que frequência você discute assuntos relacionados à segurança da informação?

[ ] Nunca
[ ] Ás vezes
[ ] Sempre
[ ] Não tem relevância

6) Seu computador possui proteção antivírus?
[ ] Sim
[ ] Não
[ ] Não tenho conhecimento

7) Você executa o antivírus antes de executar algum arquivo presente em alguma mídia removíveis (pendrives, HD, DVD, CD-ROM)?

[ ] Sim
[ ] Não
[ ] Às vezes
[ ] Nunca

8) O uso da Internet é monitorado/controlada por algum aplicativo/órgão de TI na instituição?

[ ] Sim
[ ] Não
[ ] Não tenho conhecimento

9) Sabe o que é Spam, Trojan, Malware, Phishing?

[ ] Sim
[ ] Não
[ ] Não tenho conhecimento

10) Já foi vítima, ou conhece alguém que sofreu de algum tipo de ataque virtual? Caso afirmativo

[ ] Não
[ ] Sim, em computador residencial
[ ] Sim, em computador comercial

11) Troca de senha é realizada com frequência ou somente quando o sistema operacional solicita?

[ ] Sim
[ ] Não
[ ] Não tenho senha

12) A escolha das suas senhas segue alguma política de segurança?

[ ] Sim
[ ] Não
[ ] Não tenho conhecimento

13) Já ouviu falar sobre sequestro digital de computadores ou de banco de dados?

[ ] Sim
[ ] Não

14) Você já recebeu algum tipo de treinamento de conscientização sobre segurança da informação na instituição?

[ ] Sim
[ ] Não

15) Na instituição existe um Sistema de Gestão de Segurança da Informação?

[ ] Sim
[ ] Não
[ ] Não tenho conhecimento

16) Em uma escala de 1 a 5, como você conhece as políticas de segurança da informação existentes na instituição?

Desconheço totalmente 1 2 3 4 5 Conheço totalmente

17) Você tem algum conhecimento sobre política de segurança da informação na instituição, como você classifica a sua compreensão?

[ ] Fácil entendimento
[ ] Entendimento intermediário
[ ] Difícil entendimento
[ ] Não tenho conhecimento

18) Como você classifica ser prejudicial a perda ou vazamento das informações para sua instituição?

[ ] Não causa prejuízo
[ ] Prejudicial
[ ] Pouco prejudicial
[ ] Muito prejudicial

19) No seu setor, quais são os métodos utilizados para segurança do controle de acesso aos meios tecnológicos e informações não públicas?

[ ] Biometria
[ ] Certificado digital
[ ] Usuário e senha
[ ] Outros:_____

20) Quais os tipos de ferramentas são utilizados em seu ambiente de trabalho?

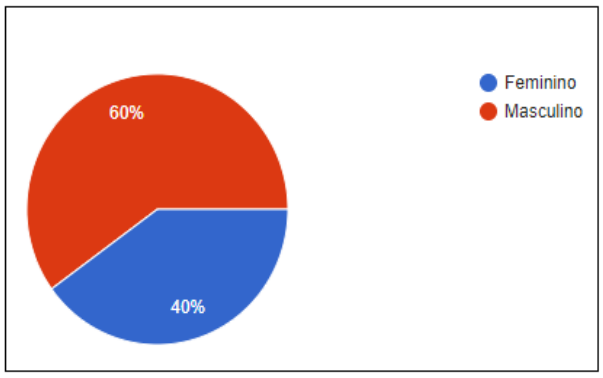
[ ] Antivírus
[ ] Ferramentas para controle ou monitoramento de e-mails
[ ] Ferramentas para controle ou monitoramento de acesso Web
[ ] Firewall
[ ] Backup
[ ] Outras:

21) Existe uma área, departamento, unidade ou equipe formal, seja ela, terceirizada ou não, responsável pela segurança da informação?
[ ] Não
[ ] Sim
[ ] Não sei

22) Existe algum tipo de campanha institucional, cartilha ou recomendações sobre segurança da informação na instituição?
[ ] Não
[ ] Sim
[ ] Não sei

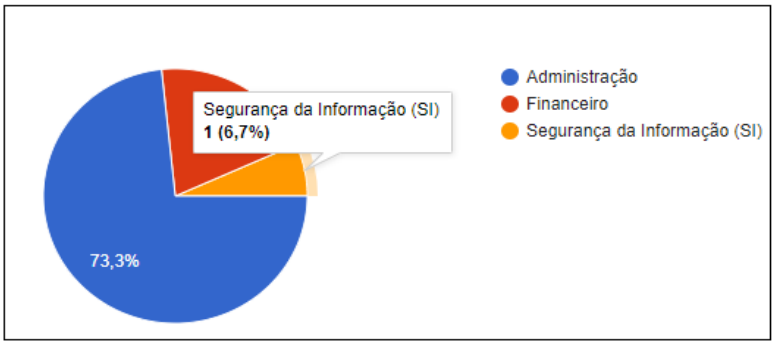
23) Você conhece ou já ouviu falar da família ISO/IEC 27000?
[ ] Não
[ ] Sim

APÊNDICE B – Percentuais de respondentes por sexo



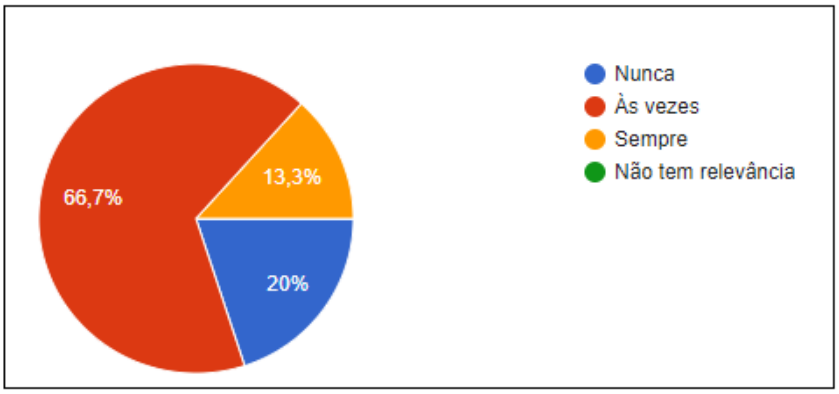
Fonte: Elaborado pelo autor

APÊNDICE C – Área de Atuação dos respondentes



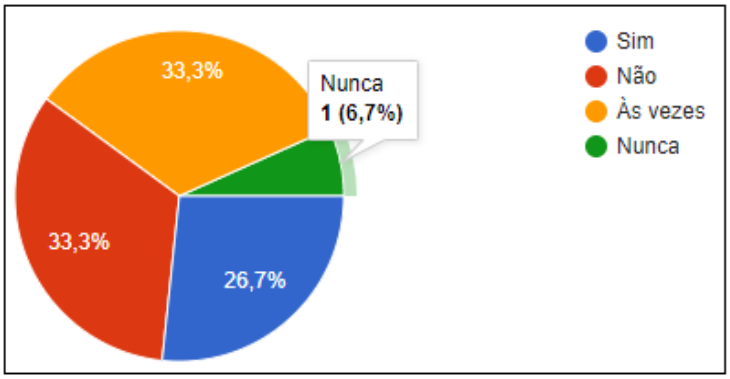
Fonte: Elaborado pelo autor

APÊNDICE D – Debate sobre Segurança da Informação



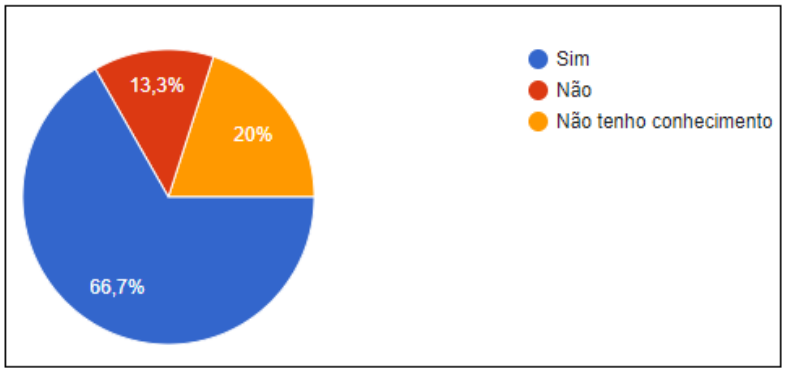
Fonte: Elaborado pelo autor

APÊNDICE E – Programa antivírus em arquivo removível



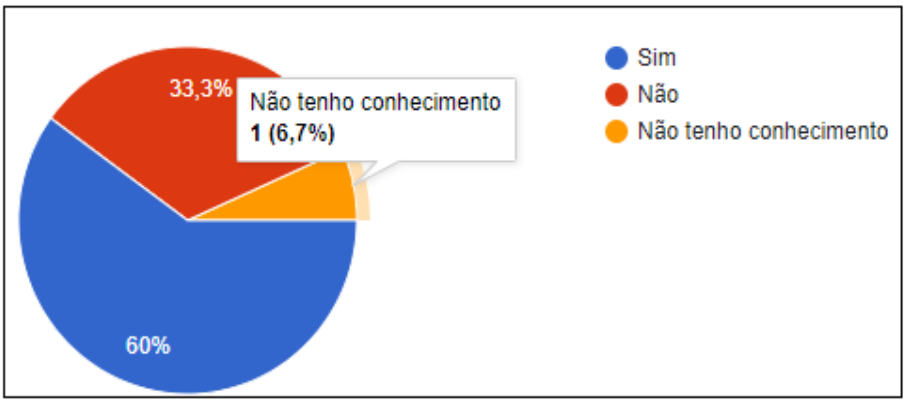
Fonte: Elaborado pelo autor

APÊNDICE F – Monitoramento de uso da internet



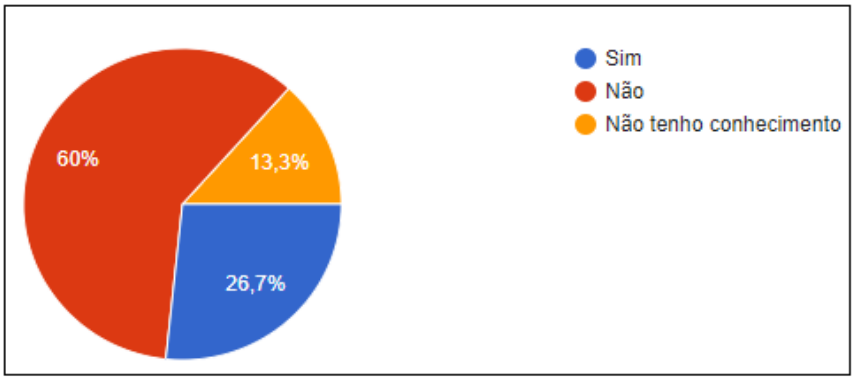
Fonte: Elaborado pelo autor

APÊNDICE G – Conhecendo vírus maliciosos



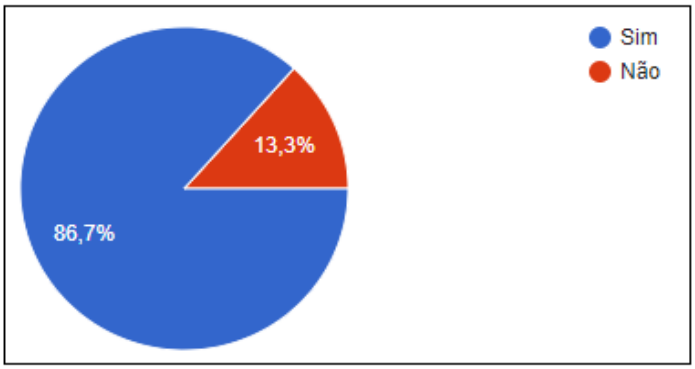
Fonte: Elaborado pelo autor

APÊNDICE H – Política de segurança na escolha das senhas



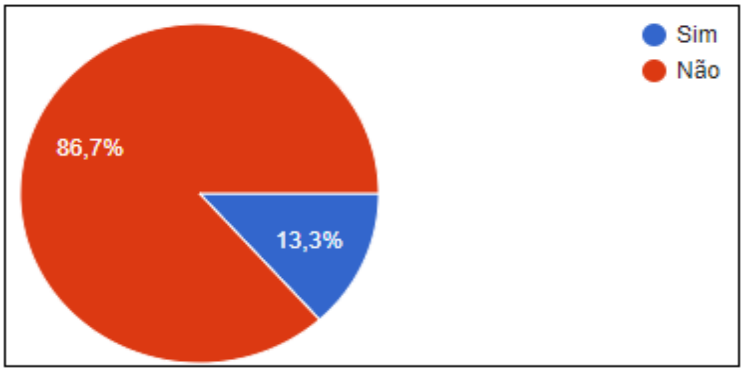
Fonte: Elaborado pelo autor

APÊNDICE I – Sequestro digital e banco de dados



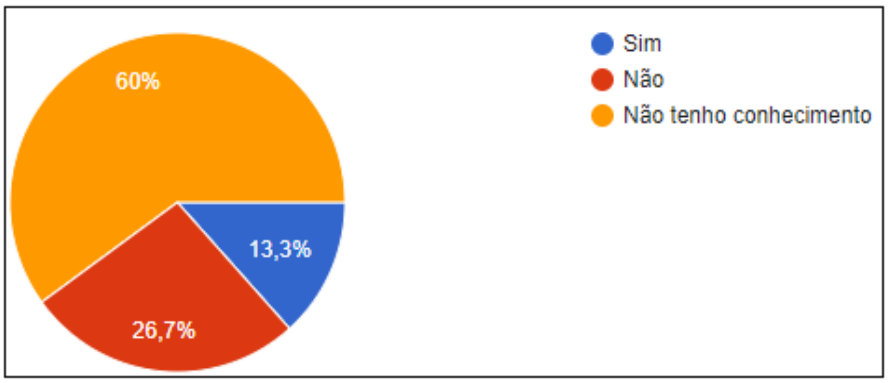
Fonte: Elaborado pelo autor

APÊNDICE J – Treinamento de conscientização sobre segurança da informação na instituição



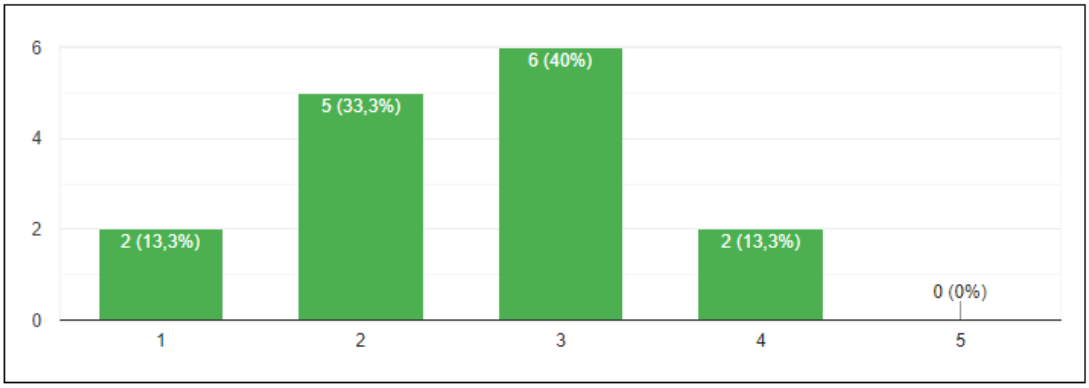
Fonte: Elaborado pelo autor

APÊNDICE K – Existência do departamento de SGSI na instituição



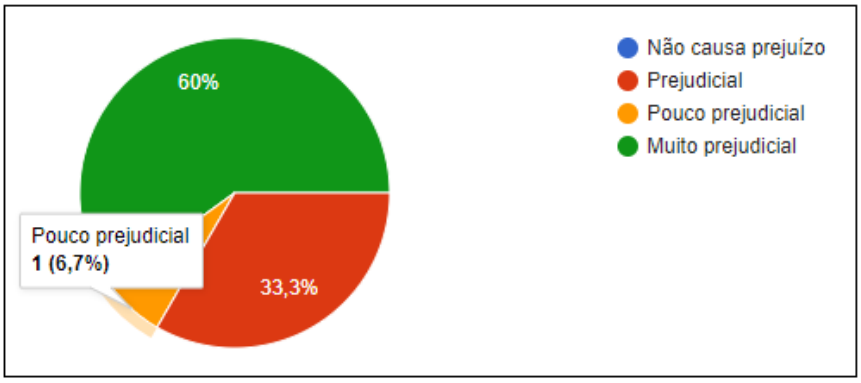
Fonte: Elaborado pelo autor

APÊNDICE L – Conhecimento sobre Política de Segurança da Informação na instituição



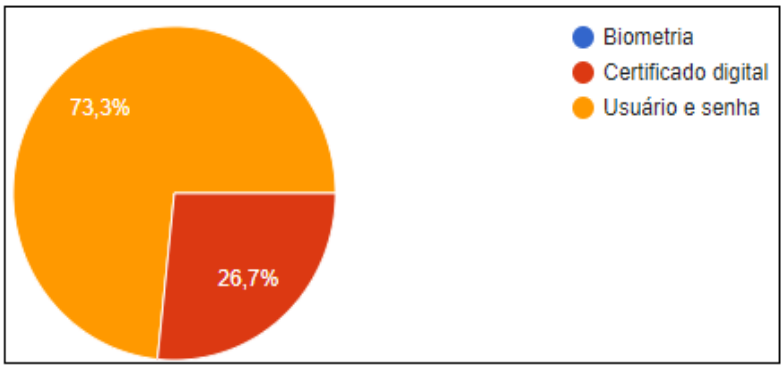
Fonte: Elaborado pelo autor

APÊNDICE M – Vazamento de Informação



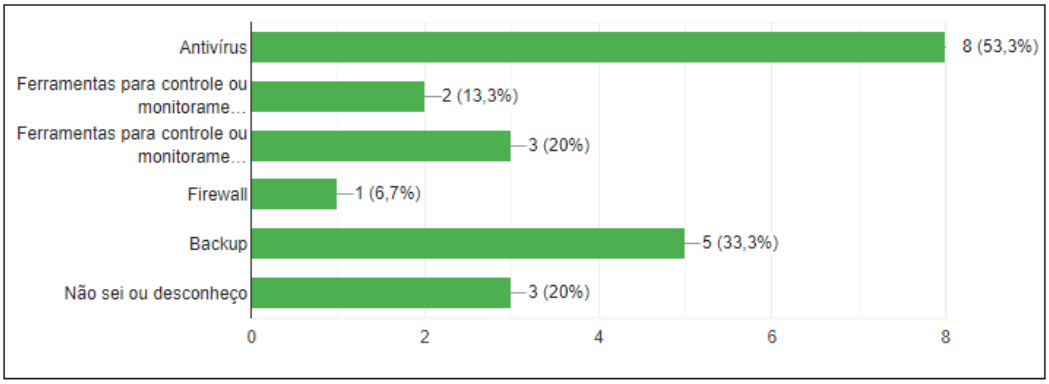
Fonte: Elaborado pelo autor

APÊNDICE N – Acesso as informações não públicas



Fonte: Elaborado pelo autor

APÊNDICE O – Ferramentas de proteção



Fonte: Elaborado pelo autor