UNIVERSIDADE FEDERAL DE ALAGOAS

CURSO: BACHARELADO EM SISTEMAS DE INFORMAÇÃO

DANIESE BOIA DA SILVA

EDELANE NUNES DA SILVA

UMA PESQUISA SOBRE A SEGURANÇA DA INFORMAÇÃO EM ESCOLAS MUNICIPAIS DA ÁREA URBANA DE GIRAU DO PONCIANO – AL

Arapiraca

2019

DANIESE BOIA DA SILVA
EDELANE NUNES DA SILVA

UMA PESQUISA SOBRE A SEGURANÇA DA INFORMAÇÃO EM ESCOLAS MUNICIPAIS DA ÁREA URBANA DE GIRAU DO PONCIANO – AL

Trabalho de Conclusão de Curso submetido ao Curso de Sistemas de Informação do Instituto de Computação da Universidade Federal de Alagoas como requisito parcial para a obtenção do Grau de Bacharel em Sistemas de Informação.

Orientador: Prof. Rômulo Nunes de Oliveira

Arapiraca
2019

DANIESE BOIA DA SILVA

EDELANE NUNES DA SILVA

UMA PESQUISA SOBRE A SEGURANÇA DA INFORMAÇÃO EM ESCOLAS MUNICIPAIS DA ÁREA URBANA DE GIRAU DO PONCIANO – AL

Este Trabalho de Conclusão de Curso (TCC) foi julgado adequado para obtenção do Título de Bacharel em Sistemas de Informação e aprovado em sua forma final pelo Instituto de Computação da Universidade Federal de Alagoas.
Maceió, 18 de 12 de 2019.

Banca Examinadora:

Prof. Me. RÔMULO NUNES DE OLIVEIRA - UFAL
Orientador

Prof. Dr. RODOLFO CARNEIRO CAVALCANTE - UFAL
Examinador

Prof. Me. KELCIANE CAVALCANTE DE LIMA - UFAL
Examinador

Dedico este trabalho a Deus primeiramente, pela vida e por tudo que tem me concedido. À minha querida mãe Gisélia e meu pai Adão, que sempre incentivaram os estudos. Aos meus irmãos, Lucas e Matheus e minhas irmãs, Elizandra, Keliany e Maria Quitéria pelas infinitas cobranças. Dedico também a minha avó Jardira, por compreender minha ausência e pelas vezes que deixei de visitá-la durante o tempo dedicado a este trabalho. Ao meu namorado, companheiro e esposo Lenilson, por todo apoio e paciência e momentos compartilhados em todos estes anos. Amo todos vocês!

Por fim, ao Prof. Rômulo, por todo auxílio, contribuição e por fazer parte desta minha jornada.

Edelane Nunes da Silva

Dedico este trabalho a meus pais, meus colegas, ao Prof. Rômulo, a Kelciane e a uma amiga muito especial.

Daniese Boia da Silva

AGRADECIMENTOS

Agradecemos a Deus primeiramente, pela vida, pelas pessoas especiais que tem colocado em nosso caminho, por estar presente em todos os momentos de nossa vida, concedendo-nos força para alcançar nossos sonhos e por sempre nos proteger.

Agradecemos de forma especial ao nosso orientador Prof. Rômulo Nunes de Oliveira, por ter aceitado o convite e o desafio de orientar este trabalho, também por ter continuado, mesmo quando as situações e acontecimentos pudesse fazê-lo desistir. Pelo seu profissionalismo, dedicação, empenho, o nosso reconhecimento e agradecimento por tudo.

Nossos agradecimentos à Kelciane Cavalcante de Lima, nossa tutora em várias disciplinas, por sua dedicação, atenção e pela amizade firmada. Por ter sempre nos ajudado com paciência durante todo o curso.

Agradecemos também à Nayara Rosy Felix da Silva, também tutora, por fazer parte da nossa formação, pelo auxílio e paciência.

Ao Prof. Bruno Almeida de Jesus pela gentileza e cordialidade e pelo tempo dedicado.

Aos demais tutores, professores e coordenadores do curso que contribuíram significativamente para nossa formação.

Aos diretores e funcionários das escolas que diretamente e indiretamente contribuíram e permitiram realizar este estudo fornecendo todos os dados necessário para o bom andamento da pesquisa.

Agradecemos profundamente aos amigos, colegas do curso e a todos que nos apoiaram nesta caminhada.

RESUMO

A evolução tecnológica possibilitou que informações, antes processadas manualmente, passassem a ser automatizadas. Estas mudanças permitiram que diversas organizações, inclusive instituições de ensino, passassem a utilizar sistemas e tecnologias para produzir, tratar e armazenar seus dados e informações. Essas necessitam estar sempre disponíveis de forma íntegra, confiável e segura. Assim que uma informação é criada, é de grande importância que ela seja protegida. A informação é um dos bens mais valiosos de qualquer ambiente organizacional, e, por esta razão, é comum este ativo enfrentar diversos obstáculos, tais como, ameaças, vulnerabilidades e ataques. A segurança da informação é um fator fundamental e deve ser tratada e priorizada nas grandes e pequenas organizações, sejam elas públicas ou privadas. Portanto, existe uma série de mecanismos de segurança que podem ser adotados como barreiras para impedir que ameaças cheguem a causar sérios incidentes as informações. O objetivo geral deste trabalho é investigar a realidade situacional das escolas municipais localizadas na área urbana de Girau do Ponciano - Alagoas com relação à segurança da informação, observando as práticas e os procedimentos adotados para proteger as informações nestas instituições e qual o conhecimento dos colaboradores sobre o assunto. Para alcançar este objetivo foi primeiramente realizada uma revisão bibliográfica baseada em fontes secundárias, que permitiu desenvolver o questionário para coleta de dados. Os resultados obtidos mostraram que os ambientes educacionais estudados possuem vulnerabilidades que podem ser exploradas por diferentes ameaças e trazer sérios riscos e incidentes para suas informações. O estudo de caso mostrou que o cenário atual das escolas em relação a segurança da informação ainda é crítico, porém com a adoção de alguns mecanismos de segurança, assim como, a implantação de políticas de segurança da informação e a realização de capacitações para conscientizar os funcionários podem minimizar as falhas na segurança e preservar as informações contra futuras eventualidades.

Palavras-chave: Segurança da Informação. Ameaças. Mecanismos de segurança. Políticas de segurança da informação.

ABSTRACT

Technological evolution has enabled information, previously processed manually, to be automated. These changes have enabled many organizations, including educational institutions, to use systems and technologies to produce, process and store their data and information. These need to be always available in a complete, reliable and secure manner. Once information is created, it is of great importance that it be protected. Information is one of the most valuable assets of any organizational environment, and for this reason, it is common for this asset to face many obstacles, such as threats, vulnerabilities and attacks. Information security is a key factor and should be addressed and prioritized in large and small organizations, whether public or private. There are then a number of security mechanisms that can be adopted as barriers to prevent threats from causing serious information incidents. The general objective of this work is to investigate the situational reality of municipal schools located in the urban area of Girau do Ponciano - Alagoas regarding information security, observing the practices and procedures adopted to protect the information in these institutions and what is the knowledge of employees about the subject. To achieve this objective, a bibliographic review based on secondary sources was first performed, which allowed the development of the questionnaire for data collection. The results showed that the studied educational environments have vulnerabilities that can be exploited by different threats and bring serious risks and incidents to their information. The case study showed that the current scenario of schools in relation to information security is still critical, but with the adoption of some security mechanisms, as well as the implementation of information security policies and training to raise awareness. Employees can minimize security breaches and preserve information against future eventualities.

Keywords: Information Security. Threats. Security mechanisms. Information Security Policies..

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
TCC	Trabalho de Conclusão do Curso
NBR	Norma Brasileira
SI	Sistema de Informação
TIC	Tecnologia da Informação e Comunicação
TI	Tecnologia da Informação
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
PWC	PriceWaterhouseCoopers
APF	Administração Pública Federal
PSI	Política de Segurança da Informação
CETIC	Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
CIA	*Confidentiality, Integrity, Availability (*Confidencialidade, Integridade, Disponibilidade*)*
DoS	*Denial of Service* (Ataque de Negação de Serviço)
DDoS	*Distributed Denial of Service* (Ataque Distribuído de Negação de Serviço)
IDS	*Intrusion Detection System* (Sistema de Detecção de Intruso)
TCP	*Transmission Control Protocol* (Protocolo de Controle de Transmissão)
VPN	Rede Privada Virtual
APF	Administração Pública Federal

SUMÁRIO

1 INTRODUÇÃO

A informação tornou-se um ativo indispensável e de uso corrente no dia a dia de diversos ambientes corporativos. Esses ambientes vêm produzindo eletronicamente um grande volume de dados e informações com o uso de Sistemas de Informação (SI) e de Tecnologia da Informação e Comunicação (TIC) como ferramenta de apoio. O uso dessas ferramentas vem crescendo bastante, inclusive nos ambientes escolares, tanto para uso didático, quanto administrativo.

As escolas são exemplos de ambientes que dependem e produzem diariamente dados e informações importantes da vida escolar dos alunos e da própria instituição. É grande volume de informações manuais armazenadas em armários, gaveteiros, prateleiras e, atualmente, com o auxílio da tecnologia, passaram a produzir mais informações, principalmente digitais. Nesse sentido, além de gerenciar a guarda, as escolas devem também garantir a segurança dessas informações manuais e digitais.

Segundo Pimenta e Quaresma (2016), para que os ambientes organizacionais tenham sempre as suas informações disponíveis de forma rápida, integra e confidencial é necessário que possuam sistemas e Tecnologia da Informação (TI) capazes de responder às suas necessidades e exigências, além disso, devem garantir a segurança das informações armazenadas, processadas e divulgadas por essas tecnologias.

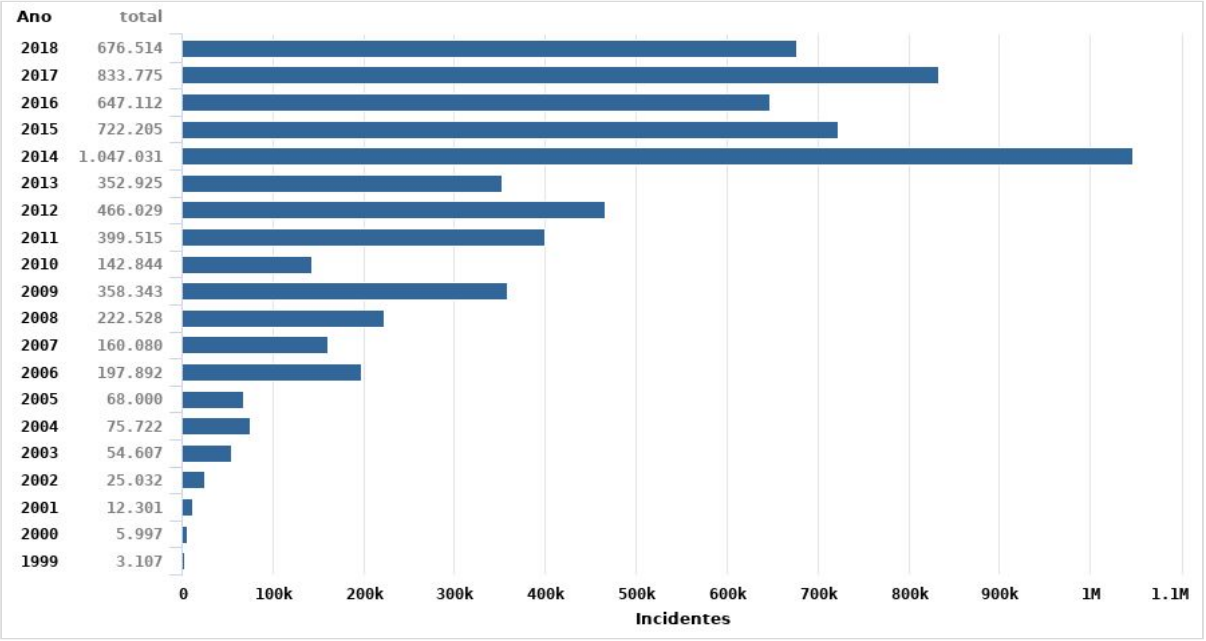
Desse modo, com o uso frequente dos serviços proporcionados por meio dos computadores, inclusive através da Internet, diversas pessoas e ambientes organizacionais vêm sendo alvo constante de ataques maliciosos e de roubos às suas informações. Esses ataques podem causar grandes impactos que vão desde a perda da informação, prejuízos financeiros e até mesmo à extinção da própria organização. Nesse sentido, é importante perceber o quanto a informação é um ativo essencial para sobrevivência dos ambientes corporativos e institucionais, sendo necessário preservá-la para que não seja alterada ou acessada por pessoas não autorizadas e mal intencionadas (OLIVEIRA, 2011).

Conforme Sêmola (2014, apud ALBUQUERQUE JUNIOR; SANTOS, 2014), existem informações fundamentais que se apresentam como importante diferencial competitivo. Desse modo, esses ambientes devem se preocupar com a segurança de suas informações a fim de se

tornarem mais competitivos, ágeis e dinâmicos no desempenho das suas atividades e negócios.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT.br), que faz o levantamento anual dos incidentes de segurança que lhes são reportados, recebeu em 2018 um total de 676.514 notificações de incidentes relacionados a segurança da informação. São notificações sobre ataques de negação de serviços, tentativas de fraudes, varreduras e propagação de códigos maliciosos, ataques a servidores Web, computadores comprometidos, entre outros incidentes reportados. Se comparado ao ano de 2017 em que o total de incidentes reportados foi de 833.775, o ano de 2018 foi 19% menor. Conforme o gráfico na Figura 1, 2014 mostrou-se o ano com a maior ocorrência de incidentes, o número chegou a 1.047.031 (CERT.br, 2019).

Figura 1 - Total de Incidentes Reportados ao CERT.br por Ano.



Fonte: (CERT.br, 2019)

A Pesquisa sobre estado global da segurança da informação de 2018 da PWC (PriceWaterhouseCoopers) também traz alguns destaques sobre a segurança da informação. A pesquisa teve como foco verificar como as organizações estão lidando com os riscos de cibersegurança associados às novas tecnologia e a privacidade e proteção dos dados. Foram entrevistados 9.500 executivos de 122 países e uma das principais conclusões da pesquisa está

relacionada aos funcionários. Segundo os dados, 30% dos funcionários atuais continuam sendo a principal origem de incidentes de segurança (PWC, 2018).

Para Lurnardi, Dolci (2006), muitas organizações, tanto públicas quanto privadas, ainda não estão preparadas para lidar com a segurança da informação. Pesquisas relacionadas à segurança da informação na Administração Pública Federal (APF) mostram que o nível de adoção de práticas relativas às políticas e responsabilidades de segurança da informação em um período de 2012 a 2014 e o nível de maturidade dos órgãos e entidades da APF está muito abaixo do esperado, deixando a APF exposta a diversos riscos (GUIMARÃES, 2018).

A empresa de segurança da informação, SonicWall, também traz dados detalhados sobre os perigos digitais em seu relatório de ameaças cibernéticas de 2019. A empresa registrou no mundo todo 10,52 bilhões de ataques de malware em 2018, se comparado aos anos de 2015 a 2017, é um número mais alto já registrado (SONICWALL, 2019). Só no primeiro semestre de 2018 foram registrados 5,99 bilhões de ameaças a servidores, computadores e outros sistemas de rede em todo mundo. Em relação ao ano 2017, quando foram comprovado 2,97 bilhões de casos, o registro de ameaças é 102% maior (SONICWALL, 2018).

De acordo com o relatório, os tipos de ataques que envolvem *Ransomware* são os mais preocupantes. *Ransomware* é um programa malicioso que "sequestra" a máquina do usuário e cobra um resgate para devolver os dados. Foram registrados 181,5 milhões de casos de *Ransomware* só nos primeiros seis meses de 2018, um aumento de 229% em relação ao primeiro semestre do ano 2017 (SONICWALL, 2018). Esse tipo de ataque traz consequências como a perda temporária ou permanente de informações; perdas financeiras associadas à restauração do sistema, interrupção de serviços regulares, custos, perda de confiança dos clientes até mesmo danos à reputação da empresa.

Diante desse cenário, Sêmola (2014, apud ALBUQUERQUE JUNIOR; SANTOS, 2014) destaca que para proteger a informação medidas de segurança da informação podem ser aplicadas, visto que cada organização tem características próprias com necessidades particulares. Desse modo, para conseguir evitar que as informações sejam roubadas e causem algum prejuízo para a organização é preciso que a organização crie e implante práticas, procedimentos e políticas que devem ser seguidas por todos os colaboradores, internos e externos, a fim de diminuir os riscos, melhorar o controle e impedir que ameaças provenientes

do uso inadequado de informações venha pôr em risco a confiabilidade dessas informações, impedindo assim, o avanço de ataques cibernéticos como também a perda de informação importantes para a organização, seja elas armazenadas em meio digital ou não.

Medidas como Políticas de Segurança da Informação (PSI) podem ser adotadas nas mais diversas organizações, sejam elas de pequeno ou grande porte, públicas ou privadas. Ambientes educacionais, objetos de estudo deste trabalho, devem perceber a importância da adoção de mecanismos de segurança, bem como a implantação de uma PSI, para que assim, consigam proteger suas informações e tecnologias, pois, por meio desses mecanismos que muitos funcionários, usuários e colaboradores passam a ter conhecimento das normas que devem seguir e também dos riscos que podem vir acontecer por sua inadimplência.

Conforme destaca Pontes (2014, p.24), uma PSI tem a finalidade de garantir que os recursos de informática e a informação sejam usados adequadamente. Ela deve descrever critérios apropriados para o correto manuseio, armazenamento, transporte e o descarte das informações, como também deve informar às pessoas quais são suas obrigações para com a proteção da tecnologia e da informação. Desse modo, é conveniente que a PSI seja criada antecipadamente para evitar a ocorrência de algum incidente com a segurança, ou depois, para evitar que algum evento ocorrido venha se repetir (FERREIRA; ARAÚJO, 2008, apud ULLMANN, 2015). Além disso, a realização de treinamentos é outro importante mecanismo que contribui para garantir um nível adequado de segurança para as informações da organização pois visa conscientizar e orientar os funcionário a seguir as práticas e regras de segurança definidas na PSI e usarem adequadamente os ativos tecnológicos e informacionais.

Nesse sentido, tendo em vista a importância da informação para as organizações e a necessidade de protegê-la através dos métodos e técnicas que busquem contribuir para o aumento da segurança da informação, principalmente nos ambientes educacionais, objeto de estudo deste trabalho, a presente pesquisa se propõe investigar a situação atual das escolas municipais da área urbana de Girau do Ponciano-AL em relação a segurança da informação. Desta forma, procura-se responder a seguinte questão de pesquisa: Qual a situação atual das escolas municipais localizadas na área urbana de Girau do Ponciano-Alagoas com relação à segurança da informação?

1.1 Justificativa

Os ambientes educacionais cada vez mais fazem uso dos SI e TIC para facilitar o trabalho do corpo docente e administrativo da escola. O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) apresenta os indicadores da pesquisa sobre o uso das tecnologias de informação e comunicação na sociedade brasileira. Os resultados da pesquisa TIC Educação 2017 mostram 98% das escolas públicas possuíam pelo menos um computador de mesa, 82% delas possuem computador portátil, 28%, tablet e 91% das escolas públicas já contavam com conexão sem fio à Internet (CGI.br/NIC.br, 2018).

Mesmo sendo alto o percentual de escolas que possuem computadores e Internet, segundo a pesquisa, parte das escolas não permitem que os alunos utilizem esses computadores e apenas 30% das escolas permitiam o acesso à rede Wi-Fi por eles (CGI.br/NIC.br, 2018). Parte dos motivos para essa restrição se dá ao fato da baixa qualidade de conexão, pois a quantidade excessiva de acessos simultâneos a rede pode prejudicar a Internet, deixando-a mais lenta. Além disso, existe também a restrição de manter o controle de acesso devido os riscos que os estudantes podem sofrer se não souberem fazer uso adequado e seguro das tecnologias, ou seja, ser expostos a outros riscos relacionados à segurança.

O fato é que os gestores das escolas não deveriam se preocuparem apenas com esse quesito da segurança pois, mesmo impedindo que os alunos tenham acesso à Internet por meio da rede da escola, não significa que apenas eles estariam imunes aos riscos expostos ao navegar pela Internet. As informações da escola também correm sérios riscos, visto que, qualquer informação importante para escola, estando guardadas ou não em meios tecnológicos, podem estar vulneráveis a ameaças internas e externas. Pessoas que trabalham ou não nesses ambientes podem ter acesso a vários dados importantes armazenados tanto em meio digital, quanto meio físico (impresso, escrito em papel, entre outros). Para Pimenta e Quaresma (2016), um dos elementos que podem provocar vulnerabilidades e danos eventuais aos SI são os usuários, sendo pois, conveniente verificar se estão instruídos a utilizar as práticas corretas e seguras no desempenho de suas tarefas ao utilizar os sistemas e tecnologias.

O volume de informações que diariamente os ambientes educacionais produzem e o uso cada vez maior de tecnologias para gerenciar e armazenar essas informações, muitas

vezes é administrada por usuários/funcionários que muitas vezes não dar a total atenção, preocupação ou mesmo não são treinados para lidar com a segurança dessas informações. Furnell e Thomson (2009) apontam que um dos grandes problemas e ameaças verificados na implementação de práticas e procedimentos na segurança da informação são os usuários. Esses que trabalham diretamente com as informações, devem ser informados e instruídos para as questões de segurança, especialmente para os efeitos negativos que uma falha ou quebra de segurança podem provocar (Kruger; Kearney, 2008). Rhee, Kim e Ryu (2009) vão além, destacando que "a falta de prática do usuário representa uma ameaça maior para a segurança de uma organização do que qualquer outra vulnerabilidade na segurança da informação".

Uma falha, uso inadequado ou desconhecimento dos riscos de um usuário traz muitas consequências para o ambiente organizacional, como a perda e sequestro de informações valiosas, prejuízos financeiros, competitivos, morais entre outros. Dessa forma, é preciso que os usuários conheçam o patrimônio tecnológico e informacional da organização. Como Deitos (2002) afirma, não conhecer o patrimônio tecnológico expõe a empresa a diversos riscos. Dessa forma, é indispensável que a organização direciona suas metas e estratégias para uma boa gestão e proteção das informações e das TIC. Para isso, é importante estabelecer mecanismos de segurança que vise proteger as informações de ameaças que exploram as vulnerabilidades presentes nos ativos que mantém essas informações.

Discutir a segurança da informação em ambientes educacionais a partir da realidade situacional das escolas justifica-se pela necessidade de se entender o quão o tema é importante e o quanto pode e deve ser discutido e praticado nesses ambientes. Para tanto, é necessário compreender a segurança da informação, identificar que ameaças podem afetar estes ambientes e conhecer os mecanismos de segurança que podem ser efetivamente aplicados.

Dessa forma, investigar inicialmente a realidade situacional das escolas municipais localizadas na área urbana da referida cidade em relação a segurança de suas informações é o passo inicial para compreender a importância dada às informações e tecnologias existentes nesses ambientes. Espera-se que o resultado desta pesquisa traga contribuições para os ambientes educacionais de modo geral e principalmente para as escolas estudadas, por meio da identificação e entendimento dos gargalos enfrentados, para que assim percebam que proteger os ativos informacionais é responsabilidade de todos e uma necessidade constante para garantir a segurança das informações e das tecnologias da escola.

1.2 Objetivos

1.2.1 Geral

O objetivo geral deste trabalho é investigar a realidade situacional das escolas municipais localizadas na área urbana de Girau do Ponciano - Alagoas com relação à segurança da informação, observando as práticas e os procedimentos adotados para proteger as informações nessas instituições e qual o conhecimento dos colaboradores sobre o assunto.

1.2.2 Específicos

O desenvolvimento deste trabalho se divide em etapas para que se possa chegar com êxito ao objetivo geral. Portanto, para o cumprimento do objetivo geral definiu-se os seguintes objetivos específicos:

- Apresentar os conceitos relacionados à segurança da informação e seus princípios.
- Descrever os principais incidentes, vulnerabilidades, ameaças, ataques e riscos para a segurança da informação e apresentar alguns mecanismos de segurança.
- Entender a importância de se estabelecer uma Política de Segurança da Informação.
- Apresentar a pesquisa sobre situação atual das escolas com relação à segurança da informação.

1.3 Metodologia

Para a realização deste trabalho, será abordada uma pesquisa bibliográfica, constituída principalmente de livros, monografias, artigos e de materiais já publicados na Internet. Desse modo, visa compreender os fundamentos básicos da segurança da informação.

Esta pesquisa também será descritiva de natureza quantitativa e qualitativa onde pretende-se realizar um estudo de caso utilizando como instrumento um questionário/entrevistas envolvendo todos os diretores das sete escolas municipais existentes na área urbana da cidade de Girau do Ponciano-AL. O objetivo do questionário é realizar o levantamento dos dados necessários para investigar a situação atual das escolas em relação a

segurança da informação. Os objetivos secundários é dar suporte às análises dos resultados referente às práticas e os procedimentos adotados para proteger as informações nas instituições e qual o conhecimentos dos colaboradores sobre o assunto.

A pesquisa foi realizada entre 29 de maio de 2019 à 20 de junho 2019, em horários de maior disponibilidade dos diretores. Eles também contaram com o auxílio dos assistentes administrativos, secretários escolares e coordenadores, visto que esses também trabalham diretamente com as informações da escola.

O questionário[1] contém questões fechadas e abertas e entrevistas semiestruturadas para a coleta de dados aplicado junto a direção das escolas e foi elaborado segundo os objetivos determinados neste estudo, assegurando sigilo aos entrevistados e das próprias escolas e, antes do início do mesmo, para efeito de esclarecimento, incluiu-se um texto sucinto de apresentação.

Com base nas respostas obtidas, tornou-se possível confeccionar gráficos, realizando-se assim, a descrição dos dados. A partir disto, foi realizada uma análise crítica da descrição dos dados obtidos, e comparando-os às questões de pesquisa e as indicações dos autores que constam no referencial teórico.

1.4 Organização da Monografia

Este trabalho está estruturado em quatro capítulos. O Capítulo 1 introduz o tema, a justificativa, definição do problema da pesquisa, os objetivos gerais e específicos, e como está organizado este trabalho. O Capítulo 2 apresenta o referencial teórico do trabalho, no qual se tem o levantamento das informações e conceitos a respeito do tema abordado. Já o Capítulo 3 apresenta a análise e resultados da pesquisa sobre a segurança da informação nas escolas estudadas. Por fim, no Capítulo 4 são apresentadas as considerações finais do trabalho, incluindo os objetivos atingidos, as principais dificuldades encontradas durante a realização deste trabalho, propostas para trabalhos futuros sobre o assunto e a conclusão do trabalho.

[1] Consultar Apêndice A

2 REVISÃO DE LITERATURA

Este capítulo faz uma leitura sobre os conceitos encontrado na literatura relacionados à segurança da informação, os principais riscos, mecanismos e Política de Segurança da Informação. Antes de discutir o tema segurança da informação, faz-se necessário compreender os termos relacionados à informação, SI e TI.

Para entender a devida atenção que é dada a informação é preciso compreender que as organizações "coletam, processam, armazenam e transmitem informações em diferentes formatos, incluindo o eletrônico, físico e verbal" (ABNT NBR ISO/IEC 27002, 2013, p.4). Assim, antes de se tornar o que de fato pode ser considerado informação, é importante compreender a distinção entre dados, informação e conhecimento.

Os dados são "sequências de fatos ainda não analisados, representativos de eventos que ocorrem nas organizações ou no ambiente físico, antes de terem sido organizados e arranjados de uma forma que as pessoas possam entendê-los e usá-los" (LAUDON; LAUDON, 2010, p.12). Um dado pode ser processado pela TI, porém só se torna informação após adquirir algum significado. É importante frisar que a perda de algum dado pode prejudicar informação.

Nesse contexto, as organizações gera suas informações a partir de seus dados, quando estes são processados e analisados se tornam informação e, a partir de então, são úteis nos processos de tomada de decisão e no desenvolvimento de atividades dentro da organização. Desse modo, a informação é entendida como o conjunto de dados que possuem significado e, se fornecida na forma e no tempo preciso produz conhecimento (RODRIGUES, 2000). O conhecimento, por sua vez, é compreendido como um conjunto de informações que tem valor para a organização, este conhecimento é obtido com base nas experiências com o uso da informação.

A TI auxilia as organizações no processamento e análise das informações. Batista (2004, p. 59) define que Tecnologia de Informação "é todo e qualquer dispositivo que tenha a capacidade para tratar dados e/ou informações, tanto de forma sistêmica como esporádica, independentemente da maneira como é aplicada".

Nesse sentido, os meios utilizados para garantir a continuidade dos processos da organização fazem parte do seu SI. Para Baars (et al, 2018), "no contexto da segurança da

informação, um sistema de informação é toda a combinação de meios, procedimentos, regras e pessoas que asseguram o fornecimento de informações para um processo operacional". Desse modo, todos os meios utilizados para o processamento e transferência de informações fazem parte da infraestrutura de um sistema de informação, assim, os SI não se referem apenas às TI que uma organização utiliza, mas também, como as pessoas interagem com essa tecnologia em apoio aos processos de negócio.

É fundamental ter um bom SI à disposição da organização no momento da tomada de decisões. Para que isso seja possível é necessário uma estrutura informacional que atue com agilidade e com segurança, assim, as informações fornecidas serão de forma estruturada, diversificadas e relevantes para o processo decisório. Segundo Teles e Amorim (2013), mesmo com inúmeros benefícios, caso os SI sejam implantados sem o devido planejamento e acompanhamento, seus impactos podem ser catastrófico, especialmente se o pessoal da organização resistir às mudanças, principalmente quando a organização passa a utilizar tecnologias. Nesse contexto, devido a informação ser um ativo importante para o ambiente organizacional, pode ficar exposta a ameaças e vulnerabilidades. Garantir que essa informação fique segura é um desafio que as organizações têm que lidar (ALBUQUERQUE JUNIOR; SANTOS, 2014).

Para proteger adequadamente esse importante ativo é preciso saber destacar quais ativos e consequentemente que informações são mais importante para a organização, para isso, é necessário compreender a segurança da informação, sua importância, saber classificar a informação que circunda pela organização e que princípios cercam essas informações, além de disso, é preciso conhecer quais ameaças podem afetar os ambientes organizacionais e quais medidas ou mecanismos de segurança podem ser adotados para atingir um nível adequado de segurança da informação. Todos esses temas são tratados nos tópicos a seguintes.

2.1 Segurança da Informação

Conforme Vinna (2015), as informações são criadas a partir da coleta, processamento e análise dos dados, e por meio da aplicação do conhecimento humano, acaba gerando novos conhecimentos, estes por sua vez, voltam para aprimorar as informações. Nesse contexto, a informação e o conhecimento adquirido constitui um imprescindível recurso estratégico para

o sucesso da empresa, pois sua importância está diretamente relacionada a maneira como ela auxilia a tomada de decisões e o alcance das metas da organização.

Como destaca Stair e Reynolds (2011, p.6), “informações valiosas podem ajudar as pessoas e suas organizações a desempenhar tarefas de forma mais eficiente e eficaz”. Assim, tanto os dados quanto às informações precisam ser administrados adequadamente como os outros ativos importantes da empresa, pois poucas organizações sobrevivem sem dados e informações de qualidade (VIANNA, 2015).

Segundo a norma ABNT ISO/IEC 27002 (2005, p.1), um ativo é definido como “qualquer coisa que tenha valor para organização”. Existe dentro da organização ativos de diversas formas, incluindo a própria informação, as pessoas, ativos tecnológico, físico ou lógico, processos e atividades de negócio, as instalações físicas e até de maneira intangível, como a sua própria reputação (ABNT NBR ISO/IEC 27005, 2011). Todos esses ativos contribui para se extrair informações valiosas. Nesse sentido, proteger a informação é essencial para os negócios de uma organização. Segundo Pimenta e Quaresma (2016), o recurso mais precioso para a organização é a informação, garantir a sua segurança é um dos seus maiores desafios.

Nos dias atuais, está cada vez mais comum nos depararmos com notícias de ataques cibernéticos em diversos países, inclusive no Brasil. São ataques a grandes e pequenas empresas, agências, órgãos, instituições governamentais, roubo de dados, vazamentos de informações sigilosas, tentativas de fraudes, entre outras formas maliciosas utilizadas por criminosos para obter vantagens. Esses ataques virtuais acontecem a todo instante e, na maioria das vezes só é percebido pelas empresas, instituições, organizações ou mesmo usuários comuns quando se tem algum prejuízo, tanto financeiro quanto moral. Nesse contexto, inicialmente o principal bem atacado por esses criminosos cibernéticos é a informação, a partir dela que esses criminosos conseguem tirar outras vantagens.

É evidente que uso das tecnologias nos ambientes organizacionais tem mudado a forma como as organizações produzem, tratam e protegem a informação. Conforme Carvalho, Reis e Alves (2017), mesmo que os sistemas computacionais atuais tenham sido desenvolvidos e pensados na segurança das informações, com o aumento do uso da Internet e de aplicações em rede, os riscos de ataques e invasões contra seus usuários são maiores, principalmente quando os próprios, por falta de conhecimento ou mau uso dessa tecnologia,

abre portas para esses ataques. Nesse contexto de insegurança que cerca as pessoas e os diversos ambientes organizacionais surge a segurança da informação.

A segurança da informação é a proteção da informação e de outros ativos informacionais contra o acesso, divulgação, modificação, destruição ou utilização por pessoas não autorizadas. Para Sêmola (2003, p.43) segurança da informação é "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade". Albuquerque Júnior e Santos (2014) argumentam que a segurança da informação vai além de questões técnicas, é necessário considerar também os aspectos tecnológicos, humanos, administrativos e organizacionais.

A segurança da informação não está restrita apenas a tecnologia, ela engloba os diversos meios nos quais se pode obter, armazenar e proteger as informações. Promon (2005) destaca que a segurança da informação não está relacionada apenas com os sistemas e redes corporativas, a segurança envolve a identificação das diversas vulnerabilidades e a correta identificação dos riscos que podem acometer os diversos ativos de informação, sejam eles digital ou impresso. Assim, o principal objetivo da segurança da informação é garantir a confidencialidade, a integridade e a disponibilidade desses ativos de informação, sendo necessário ir além da segurança lógica, é preciso abordar também a segurança física, prevenindo o acesso não autorizado, dano e interferência as informações, instalações físicas e equipamentos da organização (PROMON, 2005).

Os conceitos relacionados à segurança da informação também pode ser encontrado formalmente na norma ABNT NBR ISO/IEC 27002:2005. Segundo a norma, segurança da informação é "a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio". A mesma norma prevê ainda que a segurança da informação está diretamente relacionada com a "preservação da confidencialidade, da integridade e da disponibilidade, além de outras propriedades como autenticidade, responsabilidade, não repúdio e confiabilidade" (ABNT NBR ISO/IEC 27002, 2005, p.x).

De acordo com os conceitos expostos acima, percebe-se um aspecto comum a todos eles, os elementos: confidencialidade, integridade e disponibilidade – conhecidos por muitos autores como tríade CIA (*Confidentiality, Integrity, Availability*). Esses elementos são considerados como três pilares ou princípios básicos da segurança da informação. A próxima

Seção (2.1.1) descreve cada um deles e acrescenta outros princípios considerados também importantes para segurança da informação.

2.1.1 Princípios da Segurança da Informação

Dantas (2011, p. 11) afirma que "a informação para ser utilizada necessita garantir três características fundamentais: a integridade, a disponibilidade e a confidencialidade, dessa forma, devem ser preservadas, pois são tidas como princípios da segurança da informação". Nesse contexto, Dantas (2011, p.11) ressalta ainda que "toda ação que venha a comprometer qualquer uma dessas qualidades estará atentando contra a sua segurança".

Estes princípios básicos da segurança da informação são definidos segundo a ABNT NBR ISO/IEC 27002 (2005) da seguinte forma:

- **Integridade -** é a garantia da exatidão e completeza da informação e dos métodos de processamento, ou seja, essa característica não deve permitir que a informação seja alterada, destruída ou modificada por pessoas não autorizadas.
- **Disponibilidade -** é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. Assim, a disponibilidade é quebrada quando a informação que se queira utilizar não esteja disponível para ser acessada no momento preciso.
- **Confidencialidade -** é a garantia de que a informação esteja disponível somente por pessoas autorizadas a terem acesso. Assim, quando se permite que pessoas não autorizadas tenham acesso ao seu conteúdo ocorre a quebra da confidencialidade.

Além desses princípios, a ABNT NBR ISO/IEC 27002 (2005) acrescenta outros: a autenticidade, a responsabilidade, o não repúdio e a confiabilidade. Dantas (2011) conceitua esses princípios da seguinte maneira:

- **Autenticidade -** visa garantir a veracidade da autoria da informação, ou seja, de onde vem o dado ou informação, quem realmente produziu aquela informação.
- **Confiabilidade -** visa garantir que a informação é confiável, vinda de uma fonte e que expressa uma mensagem verdadeira.

- **Não repúdio -** visa garantir que a informação chegará ao destino certo e não será repudiada, ou seja, não é possível negar o envio ou recebimento de uma informação ou dado;
- **Responsabilidade -** é o compartilhamento de responsabilidades por todos os que produzem, manuseiam, transportam e descartam a informação, seus sistemas e redes de trabalho.

Nesse contexto, quando alguém tem a necessidade de utilizar alguma informação, espera-se que as mesmas estejam disponíveis no momento e local determinado, que sejam corretas, confiáveis e mantidas fora do alcance de pessoas não autorizadas. Esses princípios da segurança devem ser observados quando a organização for também classificar as informações.

2.1.2 Classificação da Informação

Todo ambiente organizacional possuem informações que podem ser extremamente importantes e não podem ser acessadas ou divulgadas para outras pessoas, como também possuem informações que não são tão importantes, podendo estas serem acessadas e divulgadas sem tantas restrições. Nesse sentido, cada informação possui um grau de importância, por esse motivo é necessário que a organização as classifiquem.

Segundo Spanceski (2004, p.17), "A classificação da informação é importante para que as organizações possam determinar o nível de proteção de suas informações". Assim, para assegurar que as informações importantes sejam protegidas é preciso classificá-las, pois isso também contribui para a manutenção dos princípios da segurança da informação. Silva (et al, 2003) destaca que a classificação é um meio que permite definir procedimentos para a gestão da informação, tal como a destruição, armazenamento ou transporte da informação.

De acordo com ABNT ISO/IEC 27002 (2013, p.25), um dos objetivos da classificação da informação é "assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização." Ainda no item 8.2.1, a referida norma recomenda que: "A informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada".

A ABNT NBR ISO/IEC 27002 (2013) não determina qual classificação deve ser estabelecida para as informações, recomenda apenas seja classificada levando-se em conta os níveis de sensibilidade e criticidade para organização, de forma a definir os níveis de proteção e as medidas especiais de tratamento.

Nesse contexto, para assegurar que a informação receba um nível adequado de proteção, é necessário conhecer o negócio da organização e as atividades que são realizadas e, a partir de então, iniciar a classificação. Alguns autores (WADLOW, 2000; ABREU, 2001; BORAN, 1996, apud LAUREANO, 2005), classifica as informações em níveis de prioridade, respeitando a necessidade e manutenção das atividades da empresa. Desse modo, as informações são classificadas por esses autores da seguinte forma:

- Secreta – são informações essenciais para as atividades da organização e devem ser acessadas por um número restrito de pessoas, pois tem como objetivo de preservar sua integridade. Se pessoas não autorizadas tiverem acesso a esse tipo de informações podem prejudicar bastante a organização.
- Confidencial – são informações que devem permanecer limitada ao ambiente organizacional pois sua perda ou divulgação podem causar muitos danos. Portanto, só podem acessar essas informações em estrita necessidade.
- Interna – são informações que não devem ser acessados por pessoas externas, porém, se for acessada indevidamente, as consequências do seu uso não causará grandes danos. Ainda assim, é importante manter a sua integridade.
- Pública – são informações que não possuem restrições para sua divulgação, ou seja, podem ser divulgadas para o público em geral.

Conforme o exposto, as pessoas que fazem parte da organização devem estar cientes em relação ao grau de importância das informações, ou seja, elas precisam estar atentas que cada informação deve possuir a sua classificação e salvaguarda, como também, se cada uma delas tem permissão para serem acessadas. Isso tudo para impedir que pessoas não autorizadas obtenham informações indevidas no decorrer de seu acesso, armazenamento, transporte ou mesmo descarte (MAIOR; SANTOS; DAL LACQUA, 2006).

Neste sentido, como a classificação da informação também contribui para a preservação dos três princípios básicos que constitui o paradigma da segurança da informação (confidencialidade, integridade, disponibilidade), torna-se importante conhecer os riscos,

vulnerabilidades, ameaças que podem prejudicar as informações e outros ativos informacionais, para assim, adotar adequadamente os mecanismos de segurança.

2.2 Incidentes, Vulnerabilidades, Ameaças, Ataques e Riscos

Ao longo desses anos, os incidentes de segurança da informação vem aumentando consideravelmente. Um dos principais motivos para o aumento desses incidentes é o advento da Internet, porém, além da Internet, outros fatores também contribuem para a ocorrência de incidentes.

Segundo a norma ABNT NBR ISO/IEC 27002 (2005), um incidente de segurança da informação é uma série de eventos indesejados ou inesperados, que pode significativamente comprometer e ameaçar as atividades e os negócios da organização. De acordo com Cert.Br (2012, p. 50), "Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação ou de redes de computadores". Sêmola (2003), por sua vez, define incidente como o fato resultante da ação de uma ameaça, na qual explora uma ou mais vulnerabilidades presentes nos ativos informacionais, ocasionando assim, a violação dos princípios da segurança da informação (confidencialidade, integridade e disponibilidade).

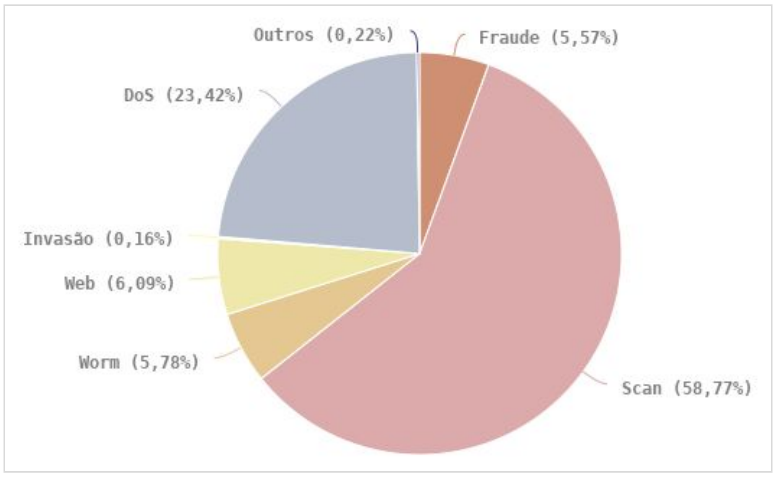
Nesse contexto, um incidente de segurança pode impactar negativamente e diretamente os negócios, atividades e serviços de uma organização pública ou privada, o relacionamento com fornecedores e parceiros ou mesmo prejudicar a reputação da empresa.

Como incidentes de segurança da informação, Ferreira e Araújo (2006) citado por Kozen (2013) destaca alguns exemplos:

- Roubo de informações;
- Disseminação de vírus ou de outros códigos maliciosos;
- Perda de informações ou de equipamentos que armazenam dados importantes;
- Usar ou acessar sem autorização um sistema, sem que o proprietário tenha conhecimento ou dado permissão prévia;
- Ataques de negação de serviço e de engenharia social;
- Descumprimento da Política de Segurança da Informação.

A Figura 2 mostra o percentual de incidentes reportados ao Cert.br no ano 2018 distribuídos por tipos.

Figura 2 - Incidentes reportados ao CERT.br em 2018.



Fonte: (CERT.br, 2019)

Como pode ser observado na Figura 2, 58,77% das notificações reportadas corresponde a ataques de varredura de redes (*Scan)*. Esse tipo de ataque é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e quais serviços estão sendo disponibilizados por eles. Os atacantes utilizam muito essa técnica para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados (CERT.br, 2019).

Nesse contexto, é importante notar que além da Internet, outros fatores também podem contribuir para impulsionar o crescimento dos incidentes de segurança. Um desses fatores são vulnerabilidades existentes nos sistemas que pode ser identificadas e exploradas por ataques de varreduras.

2.2.1 Vulnerabilidades

Para Dantas (2011, p.24), “vulnerabilidades são fragilidades que de alguma forma podem vir a provocar danos”. Sêmola (2003) destaca que as vulnerabilidades consiste em fraquezas presentes nos ativos de informação, que, ao serem exploradas, permitem a ocorrência de incidente de segurança da informação. A ABNT NBR ISO/IEC 27002 (2005,

p.3) define a vulnerabilidade como sendo a “fragilidade de um ou grupo de ativos que pode ser explorada por uma ou mais ameaças”.

Dessa forma, as vulnerabilidades estão diretamente relacionadas às fraquezas, falhas ou ausência de uma proteção que pode ser intencionalmente ou acidentalmente exploradas por ameaças que podem efetuar ataques, resultando assim, na quebra de um ou mais princípios da segurança da informação. Moreira (2001, p.22) complementa os conceitos anteriores destacando que a vulnerabilidade “é o ponto onde qualquer sistema é suscetível a um ataque”. Desse modo, compreende-se que um sistema que possua alguma vulnerabilidade está sujeito a sofrer ataques. Nesse contexto, essa vulnerabilidade ao ser explorada é causa para possíveis incidentes de segurança. No entanto, segundo Dantas (2011), às vulnerabilidades, por si só, não provocam incidentes, pois são elementos passivos que precisam de uma condição favorável ou de um agente causador.

Lyra (2015) afirma que é possível que um ativo de informação apresente vulnerabilidades que nunca poderão ser efetivamente exploradas. Ainda assim, é preciso que a organização sempre procure identificar possíveis falhas existentes em seus ativos informacionais, para assim, tentar corrigi-las da melhor maneira. Conforme Moreira (2001), as vulnerabilidades podem surgir de diversas causas, sendo que cada ambiente pode ter diversas vulnerabilidades e cada vulnerabilidade pode se apresentar em diversos ambientes.

Nesse sentido, as vulnerabilidades podem surgir de vários aspectos. Para melhor entendê-las, alguns autores diferenciam e classificam as vulnerabilidades em naturais, físicas, de hardware, de software, meios de armazenamentos (mídias), humanas, comunicações e organizacionais (DANTAS, 2011; SÊMOLA, 2003):

- Naturais - vulnerabilidades naturais se relacionam com as condições do meio ambiente ou da natureza, são eventos independem de previsibilidade e da vontade humana que podem colocar em risco as informações de organizações. Exemplos: organizações localizadas em áreas vulneráveis, enchentes, terremotos, incêndios, tempestades, acúmulo de poeira, aumento umidade, falta de energia, de temperatura etc.
- Físicas - vulnerabilidades físicas estão relacionadas aos ambientes em que estão sendo gerenciadas ou processadas as informações. Exemplo: instalações prediais inadequadas, falta de extintores, detectores de fumaça, cabos de energia e de rede

desordenados e antigos; portas ou janelas destrancadas, acesso desprotegido às salas de computador, paredes suscetíveis a assalto físico.

- Hardware - vulnerabilidades de hardware podem ser defeitos de fabricação ou de configuração dos equipamentos. Exemplos: falha nos recursos tecnológicos, a conservação inadequada dos equipamentos (desgaste, obsolescência, má utilização); a falta de configuração de suporte, sistemas mal configurados; erros de instalação.
- Software - vulnerabilidades desse tipo são formadas por todas aplicações que possuem pontos fracos que acabam permitindo acessos indevidos aos sistemas de computador, principalmente sem o conhecimento do usuário ou do administrador da rede. Essas vulnerabilidades podem ser encontradas em erros na instalação ou na configuração indevida de programas, o uso inadequado de e-mail, que permitem a execução de códigos maliciosos, editores de texto que permitem a execução de vírus de macro, entre outros que acaba acarretando acessos indevidos, vazamento de informações, perda de dados ou indisponibilidade do recurso quando necessário.
- Meios de armazenamentos (mídias) - mídias são os suportes físicos ou magnéticos utilizados para armazenar as informações. Exemplos: CD/DVD ROM; disquetes; fita magnética; discos rígidos dos computadores, *pen drive*, servidores entre outros meios. As vulnerabilidades desse tipo pode advir da utilização incorreta, de prazo de validade e expiração, defeito de fabricação, local de armazenamento em áreas insalubres, radiação eletromagnética, etc.
- Humanas - vulnerabilidades humanas é um ponto de grande preocupação para muitos especialistas, pois estão relacionadas principalmente com o desconhecimento de medidas de segurança. A origem dessa vulnerabilidade pode ser: falta de treinamento para a execução das atividades inerentes às funções de cada um; compartilhamento de informações confidenciais; falta de comprometimento dos funcionários; inadimplência nas atividades de rotina; erros; omissões; descontentamento; desleixo na elaboração de senhas no ambiente de trabalho; sabotagens, destruição da propriedade ou dados etc.
- Comunicação - incluem todos os pontos fracos que abrangem o tráfego das informações através de cabos, satélite, fibra óptica, ondas de rádio, telefone, Internet, que pode resultar em acessos não autorizados ou perda de comunicação.

- Organizacional - estas vulnerabilidades se relacionam a planos, políticas e procedimentos e a tudo que possa compor a infraestrutura de controles da organização. Exemplo: falhas ou ausência de processos, ausência de políticas de segurança e treinamento; procedimentos e rotinas; falta de planos de contingência etc.

É importante que a organização saiba identificar as vulnerabilidades existentes em seu ambiente para que, além de eliminá-las, também se previnam das ameaças que por ventura venham explorar essas vulnerabilidades. Também é importante adotar medidas de segurança ou reavaliar se as medidas existentes estão sendo eficientes na identificação dessas vulnerabilidades, visto que elas possibilitam incidentes de segurança que acabam afetando principalmente as atividades e os processos da organização, causando impactos negativos para sua própria imagem, seus clientes, produtos e demais envolvidos.

2.2.2 Ameaças

A norma ABNT NBR ISO/IEC 27002 (2005, p.3) define ameaças como: “a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização”. Para Dantas (2011, p.30), ameaças “são agentes ou condições que, ao explorarem as vulnerabilidades, podem provocar danos e perdas”. Para Sêmola (2003, p.47) as ameaças são agentes ou condições que exploram vulnerabilidades causando incidentes e comprometendo as informações e ativos, causando impactos aos negócios da organização e comprometendo confidencialidade, integridade e disponibilidade de suas informações.

Para que incidente de segurança ocorra é necessário que exista uma vulnerabilidade e que esta seja explorada por alguma ameaça. Assim, as organizações além de se preocuparem com as vulnerabilidades que podem estar presentes em seus ativos informacionais, devem também ficar atentas às potenciais ameaças, visto que podem causar sérios danos aos sistemas informatizados e a própria informação.

Alguns autores preferem classificar as ameaças. Beal (2008, apud LYRA, 2015), classifica as ameaças em acidentais e propositais. As ameaças acidentais estão relacionadas a erros de programação, falhas de hardware, desastres naturais, dentre outras. As ameaças propositais estão relacionadas com fraudes, roubos, invasões etc. Segundo Dias (2000, apud

LYRA, 2015), às ameaças propositais se divide em ativas, na qual o atacante altera informações e passivas, o atacante não altera as informações.

As ameaças também são classificadas por outros autores segundo a sua intencionalidade, na qual as divide em três grupos: naturais, involuntárias e voluntárias ou intencionais (DANTAS, 2011, SÊMOLA, 2003).

- Naturais - são ameaças resultantes de fenômenos da natureza, como por exemplo: furacões, tsunamis, enchentes, terremotos;
- Involuntárias - são ameaças resultantes de ações não intencionais, às vezes causadas pelo desconhecimento. Exemplos: erros, acidentes, ações inconsciente de usuários.
- Voluntárias ou intencionais - são ameaças premeditadas, provocadas por agentes humanos com finalidade de gerar danos. Exemplos desse tipo ameaça: invasões, fraudes, roubos e furtos de informações, hackers, espiões, criadores e disseminadores de vírus de computador, dentre outras.

Observados os conceitos apresentados, percebe-se que todos possuem pontos em comuns e que, independentemente da classificação adotada, as ameaças podem surgir de várias formas, sendo que as mais comuns estão relacionadas à falhas humanas e ambientais (PONTES, 2014). Essas ameaças são confirmadas através de alguns estudos realizados.

Dantas (2011, p.36) destaca os tipos ameaças mais frequentes com base em pesquisas de segurança da informação realizadas nacionalmente. São elas:

- Vírus, worm, cavalo de tróia (trojan horse);
- Phishing, pharming e spyware;
- Adware; spam;
- Roubo de dados confidenciais da empresa e de cliente, da propriedade da informação e da propriedade intelectual;
- Acesso não autorizado à informação;
- Perda de dados de clientes;
- Roubo de laptop, portáteis e de hardware;
- Má conduta e acesso indevido à network por funcionários e gerentes, bem como abuso de seus privilégios de acesso e utilização indevida da rede wireless;
- Ataque de negação de serviço, invasão de sistemas e da network;
- Acesso e utilização indevida da Internet e dos recursos dos sistemas de informação;
- Degradação da performance, destruição e/ou desfiguramento da network e do web site;
- Software de má qualidade, mal desenvolvido e sem atualização;
- Fraude financeira e de telecomunicações;
- Interceptação de telecomunicações (voz ou dados) e espionagem;
- Sabotagem de dados e da network;
- Desastres naturais;
- Cyber-terrorismo;

Pontes (2014) ressalta que quando se identifica uma ameaça se descobre a motivação que pode levar a um possível ataque. Os funcionários da própria organização podem ser considerados fonte de ameaças. Laudon e Laudon (2010) consideram que os funcionários são ameaças internas da organização, visto que, devido terem acesso a informações privilegiadas, podem introduzir erros inserindo dados incorretos nos sistemas, como também, podem deixar de seguir as regras impostas para uso adequado dos sistemas e equipamentos.

Também torna-se importante destacar outros agentes humanos, os *hackers e crackers*. Eles são considerados ameaças externas para a segurança da informação, porém existem algumas diferenças entre eles:

- **Hacker:** É considerado um indivíduo que obtém acesso não autorizado aos sistemas de computador por meio da exploração de vulnerabilidades (LAUDON; LAUDON, 2010). Eles possuem um vasto conhecimento avançado na área de tecnologia, no entanto, usam suas habilidades para aprimorar, espionar, copiar ou invadir sistemas sem gerar prejuízos, usando seus conhecimentos para o bem na tentativa de identificar possíveis vulnerabilidades nos sistemas.
- **Cracker:** Os crackers são hackers que utilizam técnicas para invadir sistemas de segurança com intenções de danificar dados e obter vantagens ilícitas, ou seja, tem intenções meramente criminosas. Suas ações além de serem ameaçadoras, podem gerar prejuízos para organizações ou pessoas.

Diante das diversas ameaças apresentadas, observa-se que várias são oriundas do meio eletrônico, projetadas para executarem ações maliciosas contra computadores, redes e sistemas, com intuito de acessar dados sem autorização, alterar seu conteúdo, deletá-los, deixá-los indisponíveis, entre outras ações que acabam prejudicando tanto os processos quanto a própria imagem da organização.

Assim, as principais ameaças que acometem com frequência os meios eletrônicos são identificadas como códigos maliciosos (Malware). A seguir, além dessas ameaças, assinalamos outras ameaças que podem prejudicar a segurança das informações em ambientes organizacionais.

2.2.2.1 Códigos Maliciosos (Malware)

Códigos maliciosos (Malware) “são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador” (CERT.br, 2012, p.23). Eles podem comprometer ou infectar um computador de diversas formas: explorando vulnerabilidades existentes nos programas instalados; pelo acesso de páginas maliciosas da Internet; pela execução de arquivos infectados em anexos de mensagens recebidas por e-mails ou em mídias removíveis, etc.

Eles incluem uma variedade de ameaças, algumas popularmente conhecidas, outras que vão surgindo. Dessa forma, é preciso estar atentos para saber identificar essas ameaças como também se proteger delas, tendo em vista que os principais surtos dessas ameaças se dão por ações humanas. A seguir será apresentada uma descrição resumida dos principais códigos maliciosos:

- **Vírus -** vírus são softwares maliciosos que se propaga inserindo cópias de si mesmo com a finalidade de infectar outros programas e arquivos de computador.
- **Vermes (Worms) -** também é são programas maliciosos, porém são capazes de se propagarem automaticamente através das redes, enviando cópias de si mesmo de computador para computador, se aproveitando das vulnerabilidades e falhas existentes na configuração de softwares instalados em computadores (CERT.br, 2012).
- **Bots e botnets -** são programas maliciosos capazes de se propagar automaticamente, de modo similar ao worm, explorando vulnerabilidades no sistema operacional e falhas na configuração de softwares instalados no computador. Vários computadores numa rede são infectados por bots formam as chamadas botnets. “Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos Bots” (CERT.br, 2012).
- **Spywares (programa espião) -** são programas projetados para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros (CERT.br, 2012). Existem alguns tipos específicos de spywares denominados de keylogger e screenlogger. O primeiro tem a capacidade de capturar, armazenar e enviar as teclas digitadas pelo usuário no teclado de um computador para um indivíduo mal intencionado. Já screenloggers é uma variação do keylogger, a diferença é que esse

tipo de software armazena a posição do cursor e a tela apresentada no monitor no momento em que usuário faz uso do mouse, capturando as teclas digitadas pelos usuários em teclados virtuais (CERT.br, 2012).

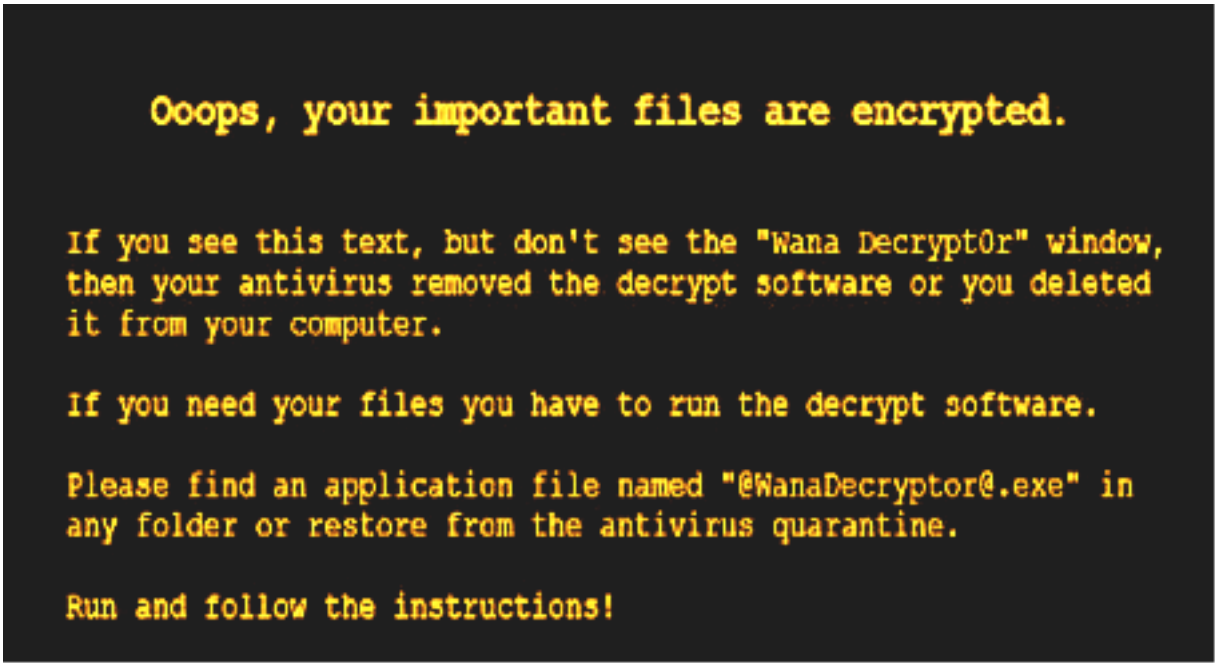
- **Adwares -** os Adwares é um tipo de programa projetado especificamente para exibir e executar automaticamente propagandas, seja por meio programa instalado no computador ou através de um navegador. Eles podem ser usados para fins legítimos ou maliciosos. Quando legítimo, tem sido incorporados a softwares e serviços na forma de patrocínio ou retorno financeiro ou para prestação de serviços gratuitos. Já adwares maliciosos geralmente executam propagandas direcionadas, com base na navegação do usuários, sem que ele saiba que está sendo monitorado (CERT.br, 2012).
- **Backdoor -** são programas que permitem o retorno de um invasor a um já computador comprometido, através da inclusão de serviços criados ou modificados para este fim (CERT.br, 2012). Assim, um atacante faz uso desse tipo de programa deixando brechas para remotamente retornar ao computador comprometido sempre que desejar e sem ser notado, de forma que não necessita recorrer aos mesmos métodos já utilizados para invadir.
- **Cavalo de troia (Trojan) -** é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuários (CERT.br, 2012). Ele é o meio utilizado para que os vírus e outros códigos maliciosos entrem no sistema do computador. Eles têm códigos encobertos criados para danificar ou explorar o computador no qual foi executado, abrindo porta no sistema para que um hacker roube ou altere dados e configurações. Geralmente os cavalos de tróia chegam através de mensagens de e-mail se apresentando como um presente (prêmios, fotos, cartão virtual, protetor de tela).
- **Rootkit -** é um conjunto de programas e técnicas maliciosas que permite mascarar e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido (CERT.br, 2012).
- **Spam -** o nome usado para se referir a grande quantidade de mensagens eletrônicas (e-mails) indesejadas que são enviadas para um grande número de pessoas sem que essas tenham solicitado. É um lixo eletrônico, porém além de se referir a e-mails indesejados, também se refere a outras formas de mensagens publicitárias em

websites, exibindo propagandas com intuito de aplicar fraudes em usuários desavisados. Eles são um dos grandes responsáveis pela propagação de códigos maliciosos, disseminação de golpes e venda ilegal de produtos etc. (CERT.br, 2012).

Além desses códigos maliciosos, novas ameaças vão surgindo e se aprimorando cada vez mais. A exemplo, podemos citar o *Ransomware*. Esse também é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, normalmente usando criptografia e que exige pagamento de resgate para estabelecer o acesso ao usuário (CERT.br, 2017). Geralmente os criminosos que utilizam essa ameaça para efetuar ataques exigem como meio de pagamento moedas digitais. A escolha não é aleatória, eles preferem esse meio devido ser quase impossível fazer rastreamento do criminoso, ou seja, ajudam a preservar sua identidade.

A Figura 3 mostra uma tela com o aviso de informando que o computador está infectado por *Ransomware* e a Figura 4 mostra o módulo da ameaça exibindo uma janela com instruções para o usuário informando o que aconteceu e como ele deve pagar o resgate. Como pode ser observado, o módulo ainda traduz as instruções para outros idiomas.

Figura 3 - Mensagem informando que o computador está comprometido por *Ransomware.*



Fonte: (SYMANTEC, 2017)

Figura 4 - Módulo de *Ransomware* exibindo uma janela com instruções para o usuário.

Fonte: (SYMANTEC, 2017)

Esse tipo de ameaça pode se propagar de diversas formas, sendo mais comum através de e-mails com o código malicioso anexado ou explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança. É importante salientar que mesmo fazendo o pagamento do resgate não é garantido que o acesso aos dados será restabelecido, por isso é importante a organização faça sempre cópias de segurança dos seus dados para não chegar ao ponto de ter que pagar para ter possivelmente seus dados novamente. Desse modo, muitos dos cuidados necessários para se proteger dessa ameaça geralmente são os mesmo recomendados para os outros códigos maliciosos. Esses cuidados serão tratados mais à frente na Seção 2.3.

2.2.2.2 Engenharia Social

O Cert.br (2012, p.115) define que engenharia social consiste em “uma técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações”. Com base na definição de Silva, Araújo e Azevedo (2013), a engenharia social é um conjunto de práticas na qual uma pessoa, com o uso ou não da tecnologia, procura manipular, persuadir,

influenciar e enganar outra pessoa com intuito de obter informações confidenciais e importantes de uma organização ou de outro indivíduo.

A pessoa que se utiliza de fraude, influência e persuasão contra empresas visando obter informações é chamado de engenheiro social (MITNICK; SIMON, 2003). Normalmente qualquer pessoa pode se tornar um engenheiro social, aplicando técnicas, analisando os ambientes com intuito de identificar pontos fracos e vulnerabilidades, manipulando pessoas, colhendo as informações que necessita, para então iniciar seu ataque (SILVA; ARAÚJO; AZEVEDO, 2013).

Se analisarmos mais profundamente, já fomos ou conhecemos alguém, até mesmo encontraremos alguma organização que tenha sofrido um ataque de engenharia social. Muitas pessoas e empresas atacadas nem percebem que foram alvos, visto que, um ataque de engenharia social geralmente deixa poucos rastros. Até mesmo as que descobrem o ataque, raramente vão admitir e divulgar o ocorrido com receio de prejudicar sua reputação (POPPER; BRIGNOLI, 2002).

Para Mitnick e Simon (2003) muitas organizações fazem grandes investimentos em tecnologia com vistas a melhorar os processos e serviços da empresa e diminuir os fatores que podem prejudicar a segurança das suas informações, como também, para fazer com que seus funcionários desenvolvam com mais eficiência suas atividades, porém essa importância dada ao fator tecnológico deixa a desejar em outro: o fator humano. Esse fator, que muitas vezes é tão esquecido, é uma das brechas mais exploradas pela engenharia social. Segundo Mitnick e Simon (2003), por mais que a organização adquira as melhores tecnologias, contrate a melhor empresa de segurança, treinem bem seus funcionários, por mais que os indivíduos sigam as melhores práticas recomendadas, eles ainda estarão completamente vulneráveis.

Nesse sentido, mesmo que a empresa invista em tecnologias avançadas de segurança, não estarão completamente seguras, pois, o ser humano é o elemento mais fraco da segurança, visto que, para que um simples ataque de engenharia ocorra com êxito, basta que as pessoas não conheçam as boas práticas de segurança, ou mesmo, sejam ignorantes em suas atividades dentro da organização (MITNICK; SIMON, 2003). Ainda conforme os autores, “a segurança não é um problema para a tecnologia - ela é um problema para as pessoas e a direção” (MITNICK; SIMON, 2003, p.4).

Desse modo, torna-se importante destacar as técnicas mais usadas nos ataques de engenharia social: (POPPER; BRIGNOLI, 2003, ALVES, 2010).

- **Engenharia social por telefone -** é considerado um dos típicos ataques de engenharia social mais comum. O uso do telefone para se passar por alguém que não é, simulando atendimento de suporte, ou alguma ação de emergência, tudo para roubar informações de funcionários ingênuos ou mesmo clonar ou grampear telefones, além também de tentar conseguir acesso a usuário e senhas.
- **Local de trabalho -** o engenheiro social pode ir pessoalmente ao local fazendo uma visita, se passando por um técnico em manutenção ou consultor disfarçado usando técnicas e o seu poder de persuasão para envolver a vítima ou, enquanto passeia pelos corredores do local, pode ir captando informações que estejam expostas;
- **Lixo -** as lixeiras da empresa pode conter muitas informações importantes que podem ser usadas por alguém mal intencionado para outros objetivos. Engenheiros sociais utilizam o método de vasculhar o lixo para tentar obter informações de sensíveis. É recomendável que a empresa faça a destruição dessas informações, pois mesmo que alguns documentos não representam ameaças ou não tenham valor, uma vez jogados no lixo estão sujeitos a cair em mãos erradas.
- **Engenharia Social On-Line -** para os engenheiros sociais que buscam obter senhas, a Internet na maior parte das vezes é o meio mais fácil de se conseguir acesso. Isso porque muitos usuários criam senhas fáceis e ainda as repetem em praticamente todas as contas de e-mails, em sites, em redes sociais, tornando o ataque ainda mais simples. Geralmente conseguem capturar senhas por meio de cadastros em que oferece brindes, então o usuário acaba fornecendo suas informações sem perceber que está caindo em um golpe, também por meio de e-mail se passando por administrador da rede ou mesmo enviando e-mails com anexos contendo vírus, worms e cavalos de tróia. Salas de bate-papo ou programas de mensagens também são canais explorado para se obter informações.
- **Persuasão -** um engenheiro social utiliza métodos básicos de persuasão como: insinuação, personificação, difusão de responsabilidade, conformidade, além da simples e velha amizade. Seja qual for o método utilizado, o objetivo é sempre o

mesmo: convencer a pessoa que passará a informação solicitada, de que o engenheiro social é alguém que ela pode confiar com as informações prestadas.

- **Engenharia Social Inversa -** esse é considerado o método mais avançado de obter informações ilícitas. O engenheiro cria uma personalidade na qual ocupa uma posição de autoridade, de forma que os funcionários lhe peçam informações. Ataques desse tipo permitem ao engenheiro social extrair dos funcionários informações valiosas, no entanto, requer muita preparação e pesquisa.
- **Olhar pessoas digitando -** o objetivo é descobrir as senhas das pessoas enquanto elas digitam no teclado.
- **Phishing -** trata-se de um golpe eletrônico por meio do envio de mensagens falsas com o objetivo de obter, sem o conhecimento da vítima, informações sigilosas.
- **Spoofing -** tem o objetivo de fraudar o número de telefone de forma que o número exibido pelo identificador de chamadas seja aquele desejado pelo fraudador.
- **Footprint -** objetivo dessa técnica é descobrir informações a respeito de algumas tecnologias usadas pela empresa, referentes principalmente ao acesso remoto, Internet e Intranet. O invasor faz uso de softwares especiais para coletar as informações desejadas.

Assim como outras ameaças, a engenharia social pode causar diversos incidentes para a segurança da informação de qualquer organização, visto que, o fator humano está ligado diretamente com esse tipo de ameaça. Para Lennert e Oliveira (2011, p. 27), “a Engenharia Social será a maior ameaça a continuidade dos negócios nas próximas décadas”. Dessa forma, se as organizações têm o objetivo de proteger sua rede, não pode confiar apenas na tecnologia (MITNICK, 2001).

2.2.3 Ataques

A norma ABNT ISO/IEC 27000 (2014, p.1) define ataque como “tentar destruir, expor, alterar, desativar, roubar ou ganhar acesso não autorizado ou fazer uso não autorizado de um ativo”. Beal (2008, p.14, apud LYRA, 2015, p.15) entende que um ataque é um “evento decorrente da exploração de uma vulnerabilidade por uma ameaça”, ou seja, um ataque corresponde à concretização de uma ameaça, que pode ser bem-sucedida ou não, por

meio de uma ação intencional e bem planejada (MARCIANO, 2006). Portanto, só a simples tentativa de acessar, destruir, alterar ou monitorar sem autorização um ativo informacional pode ser considerado um ataque.

Segundo Lyra (2015), os ataques podem afetar diferentes princípios da segurança da informação. Por exemplo, fere o princípio da disponibilidade quando um atacante invade uma rede corporativa e a deixa inoperante, se esse atacante porventura altera um arquivo, acaba ferindo o princípio da integridade, o ato de conseguir ter acesso a rede corporativa e ver informações privadas e confidenciais sem ser autorizado, já fere o princípio da confidencialidade.

Para Marciano (2006), os ataques podem ser originados de pessoas internas ou externas à organização, com o uso de recursos computacionais ou não. Porém, é importante destacar que os tipos de ataques mais comuns podem ter origem das ameaças descritas na Seção 2.2 ou de outras técnicas, principalmente em computadores conectados à Internet.

A seguir, apresentamos as principais técnicas de ataques por meio da Internet destacadas na Cartilha de Segurança para Internet (CERT.br, 2012):

- **Exploração de vulnerabilidades -** ocorre quando um atacante, aproveitando-se de uma vulnerabilidade (brechas), tenta executar ações maliciosas como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.
- **Varredura em redes -** trata-se de uma técnica que consiste em efetuar buscas minuciosas em redes. Essas buscas tem por objetivos identificar computadores ativos e coletar informações sobre eles, como programas instalados e serviços disponibilizados. Essa técnica pode ser usada de forma legítima ou maliciosa. É legítima quando usada por pessoas autorizadas para verificar a segurança da rede e dos computadores, para assim, corrigir falhas e aplicar medidas preventivas. É maliciosa quando os atacantes executam ações criminosas a partir das vulnerabilidades encontradas.
- **Falsificação de e-mail -** consiste em uma técnica na qual os atacantes alteram campos do cabeçalho de um e-mail, com intuito de aparentar que ele foi enviado de uma determinada origem, quando na verdade foi enviado de outra. Esse tipo de ataque é usado bastante para propagação de códigos maliciosos, envio de spam,

furto de identidade, fraudes, golpes de *phishing* para obter dados pessoais e financeiros.

- **Interceptação de tráfego -** essa técnica também é conhecida como *"sniffing"*. Por meio dela é possível inspecionar os dados que são trafegados pelas redes de computadores utilizando programas (*softwares*) específicos. Essa técnica pode ser usada tanto para fins legais como também para maliciosa. De forma legal, essa técnica contribui para detectar problemas, analisar desempenho ou monitorar atividades maliciosas nas redes e sistemas. De forma maliciosa, atacantes podem capturar informações sensíveis, senhas, números de cartão de crédito, entre outras informações que trafegam na rede através de conexões inseguras e sem criptografia.
- **Força bruta -** trata-se de uma técnica que consiste em adivinhar, por tentativa e erro, um nome de usuário e sua senha para então, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário. Computadores e dispositivos móveis que estejam protegidos por senhas podem tanto serem alvos de ataques por meio da rede, como também por meio físico, basta que o atacante consiga ter acesso ao equipamento.
- **Desfiguração de páginas -** é uma técnica utilizada para alterar o conteúdo de uma página de um site com intuito de furtar senhas de acesso à interface *web* usadas para administração remota, invadir servidores que hospedam aplicações *web*, explorar erros de aplicações, vulnerabilidades entre outros.
- **Negação de serviço (SoS e DDoS) -** DoS (*Denial of Service*) ou negação de serviço é uma técnica pela qual os atacantes utilizam-se de um computador para sobrecarregar alguma rede. O objetivo é deixar indisponíveis redes, serviços, operações e computadores conectados à Internet. Os atacantes podem se utilizar de conjuntos de computadores para efetuar os ataques tirando de operação um ou mais serviços ou computadores conectados à Internet, assim, esse tipo de ação é reconhecida como um ataque de negação de serviço distribuído ou DDoS (*Distributed Denial of Service*). Muitas pessoas podem usar ferramentas e fazer com que seu computador seja usado voluntariamente em ataques desse tipo, ou, podem ter seu computador infectado por *botnets,* desferindo ataques e sobrecarregando serviços nas redes sem o seu conhecimento.

Ataque físicos também pode ocorrer, como por exemplo roubo de equipamentos, *pen drives*, CD/DVD-ROM, disquetes ou outros meios de armazenamento de dados que são retirados da empresa para posterior análise ou destruição.

Diante das variadas técnicas utilizadas pelos atacantes, a norma ABNT NBR ISO/IEC 27002 (2013, p.97) orienta que o "mau funcionamento ou outro comportamento anômalo do sistema pode ser um indicador de um ataque de segurança ou violação na segurança atual e, portanto, convém que sempre seja reportado como um evento de segurança da informação".

Dessa forma, torna-se importante que funcionários e colaboradores estejam atentos aos comportamentos estranhos que algum dispositivo venha aparentar, como também, que a própria organização adote mecanismos de segurança. Para Knapp (*et al*, 2009), o primeiro e importante passo para preparar a organização contra eventuais ataques, sejam esses de origem interna ou externa, é desenvolvendo um conjunto de políticas de segurança da informação, além de medidas e mecanismos de segurança, tópicos tratados mais à frente nas seções 2.3 e 2.4 deste trabalho.

2.2.4 Riscos

Como já foi relatado, várias são as ameaças que, a partir das exploração das vulnerabilidades existentes, podem afetar os diversos ambientes organizacionais e colocar em risco a própria organização, suas informações e seus ativos. Desse modo, os riscos podem criar ou aumentar potenciais perdas e danos nas organizações (DANTAS, 2011).

Segundo Sêmola (2003), risco é a probabilidade de ameaças explorarem vulnerabilidades, ferindo os princípios da segurança da informação (confidencialidade, integridade e disponibilidade), causando possíveis impactos nos negócios. Já Araújo e Ferreira (2008, p.163 apud YAMAJI, 2013, p. 19) definem risco como "um possível evento/ação que, se efetivado, gera um impacto negativo, em função da exploração da fraqueza/vulnerabilidade, considerando tanto a probabilidade quanto o impacto de ocorrência".

A probabilidade pode ser entendida como "a possibilidade de uma falha de segurança acontecer", ou simplesmente, como a "chance de uma vulnerabilidade se tornar uma ameaça"

(LYRA, 2015, p. 17). Já o impacto pode ser considerado como o dano causado ao negócio quando um incidente acontece (Sêmola, 2003).

Diante dos argumentos expostos, pode-se entender o risco como a probabilidade de algo ou alguém malicioso aproveita-se de brechas ou fraquezas dos ativos informacionais. Estes riscos, se forem concretizados, podem causar incidentes de segurança. Estes incidentes podem gerar pequenos ou grandes impactos na organização. Desse modo, o impacto se refere aos possíveis prejuízos causados ao negócio por um incidente de segurança da informação. Como prejuízos podemos citar desde perdas financeiras, perdas de recursos, perda na qualidade dos serviços prestados, insatisfação dos clientes e colaboradores, prejuízo a própria imagem entre outros.

É importante ressaltar que o impacto de um mesmo incidente em diferentes organizações podem causar danos e prejuízos diferentes, visto que um mesmo ativo pode ter valor diferente para cada organização. Percebe-se assim, que se o ativo tiver um alto valor para o negócio, maior será o impacto caso ele sofra um incidente de segurança. Por exemplo, uma empresa que realiza vendas pela Internet, se acontecer do seu site ficar indisponível por minutos ou horas, sofrer um ataque de negação de serviço, por exemplo, provocará um impacto negativo bem maior do que a indisponibilidade do site de uma empresa que não realiza vendas pela Internet. Portanto, é necessário que cada ambiente organizacional reconheça os riscos que cada eventual incidente de segurança da informação representa.

Nesse contexto, é importante que a organização saiba identificar o nível do risco e que ele se relaciona direta e indiretamente com diversas variáveis. Segundo a norma ABNT NBR ISO/IEC 27005 (2011, p.7), o nível de risco “expressa em termos da combinação das consequências e de suas probabilidades”. Sêmola (2003) propõe a seguinte equação para aferição do risco:

$$R = \frac{V \times A \times I}{M}$$

O nível do risco é representado pela variável (R), (V, A e I) são respectivamente as vulnerabilidades, ameaças e os impactos. O produto dessas variáveis (V, A e I) é dividido pelas medidas de segurança, representadas por (M). Por meio dessa equação é possível perceber que fatores como medidas de segurança e controles influenciam na medição do risco

e pode interferir diretamente na redução ou no aumento do risco (DANTAS, 2011), ou seja, quanto mais controles ou medidas de segurança forem implantadas, mais os impactos serão limitados e menor será o risco em que a organização estará sujeita.

Segundo Dantas (2011), ao utilizar a equação do risco é possível compreendê-lo de forma mais ampla, observando os elementos que influenciam na sua identificação e sua origem, para assim, fazer uma melhor análise e até mesmo, poder classificá-lo em categorias.

Assim, percebe-se que é necessário avaliar e tratar os riscos para que ocorra sua mitigação, tudo isso é possível se a organização adotar uma gestão de riscos, prática recomendada pela norma ABNT NBR ISO/IEC 27001:2013.

O processo para a correta gestão de risco de segurança da informação em uma organização é descrito na norma ABNT NBR ISO/IEC 27005:2011. Esta norma se aplica a todos os tipos de organização que tenham por objetivo gerenciar os riscos que poderiam comprometer a segurança da informação da organização.

O processo de gestão de risco tem início quando se é estabelecido o contexto. Em seguida, é executado o processo de avaliação de risco onde os mesmo são identificados, analisados e avaliados com base nos critérios definidos quando foi estabelecido o contexto.

Se o processo de avaliação de risco fornecer informações suficientes para que se determine de forma eficaz as ações necessárias para reduzir os riscos a um nível aceitável, então a tarefa está completa e o tratamento do risco pode suceder-se. Se por acaso as informações não forem satisfatórias, o processo de avaliação é reiniciado, revisando-se o contexto.

Na fase de tratamento, os riscos podem ser reduzidos, evitados, transferidos ou aceitos (KONZEN, 2013).

- Reduzidos: são adotados os controles ou mecanismo que ajudam a mitigar o risco encontrado;
- Evitados: quando opta-se por evitar adotar tecnologias ou processos para tratar riscos que podem gerar um risco ainda maior.
- Transferidos: quando opta-se por transferir o tratamento dos riscos identificados para outro setor ou terceiros. É uma alternativa quando o custo de implantação do projeto de tratamento é oneroso.

- Aceitos: decide-se por aceitar o risco e não tomar nenhuma ação para reduzir a probabilidade de impacto ou ocorrência do mesmo.

A eficácia da fase de tratamento depende dos resultados do processo de avaliação de riscos. Porém, se o tratamento não for satisfatório, faz-se outra análise de riscos.

A norma ABNT NBR ISO/IEC 27005 (2011) ressalta ainda que a atividade de aceitação do risco deve assegurar que os riscos residuais sejam aceitos pelos gestores da organização, principalmente nas situações em que as organizações preferem adiar ou omitir a implementação de controles por diversos motivos, como por exemplos, devido aos custos de se implementar tais controles. A norma também orienta que durante o processo de gestão dos riscos é importante que os mesmos e a forma como são tratados sejam comunicados ao pessoal das áreas operacionais e gestores, visto que, as informações sobre riscos identificados podem ser bastante úteis para o gerenciamento de incidentes e ajudar a reduzir possíveis prejuízos, mesmo antes da fase de tratamento do risco.

2.3 Medidas e Mecanismos para Controle da Segurança

A informação, independentemente do seu formato, é um ativo valioso e importante. Por esse motivo que os diversos ambientes organizacionais e os equipamentos utilizados para processar, armazenar e transmitir informações devem ser protegidos (FONTES, 2006). Sendo assim, os ambientes e equipamentos estando protegidos, também é possível que o processamento, acesso, armazenamento, transporte, divulgação e eliminação de tais informações seja feito de forma segura. Para isso, esses ambientes devem adotar medidas e mecanismos de segurança.

As medidas de segurança podem ser entendidas como práticas, procedimentos e mecanismos usados para proteger informações e ativos. Através delas é possível reduzir riscos, limitar impactos e impedir que ameaças explorem vulnerabilidades, (SÊMOLA, 2003).

Segundo Sêmola (2003, p.49), as medidas de segurança, além de serem consideradas controles, podem possuir características:

> • Preventivas: medidas de segurança que tem como objetivo evitar que incidentes venham a ocorrer. Visam manter a segurança já implementada por meio de mecanismos que estabeleçam a conduta e a ética da segurança na instituição.
> • Detectáveis: medidas de segurança que visam identificar condições ou indivíduos causadores de ameaças, a fim de evitar que as mesmas explorem vulnerabilidades.

> • Corretivas: ações voltadas à correção de uma estrutura tecnológica e humana para que as mesmas se adaptam às condições de segurança estabelecidas pela instituição, ou voltadas à redução dos impactos. Equipes para emergências, restauração de backups, plano de continuidade operacional, plano de recuperação de desastres.

Como medidas preventivas observa-se por exemplo, os regulamentos (políticas de segurança, normas e regras), procedimentos de trabalho, campanhas e palestras de treinamento e conscientização de usuários, mecanismos de prevenção de códigos maliciosos, como antivírus, *firewall,* usar criptografia, aplicar atualizações de segurança, etc. Como exemplos de medidas detectáveis: câmeras de vigilância; alarmes; sistemas de detecção de intrusos (IDS); análise de risco; antivírus (também previne) entre outros. Por fim, exemplos de medidas corretivas: planos de continuidade, restauração de backup; plano de recuperação de desastres.

Apesar de existirem diversas medidas de segurança e mecanismos de apoio e, mesmo a organização adotando grande parte deles, não significa que estará completamente segura nem tão pouco que essas medidas darão cem por cento de segurança. Moreira (2001) afirma que não existem ambientes totalmente seguros pois, até mesmo as medidas de segurança implementadas pelas empresas possuem vulnerabilidades.

Nesse sentido, é importante compreender que a segurança da informação de um ambiente organizacional não deve se limitar apenas em mecanismos tecnológicos como *firewall*, antivírus, IDS entre outros. É necessário uma abrangência maior, que envolva outros mecanismos. A norma ABNT NBR ISO/IEC 27002 (2013, p.4) diz que a segurança da informação é alcançada através da implementação de um conjunto adequado de controles, como políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware que precisam ser estabelecidos, implementados, monitorados, analisados criticamente, além de melhorados sempre que necessário para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos.

Os mecanismos de segurança são técnicas e/ou métodos utilizados para tentar controlar ou mesmo bloquear o acesso indevido às informações. Segundo Zanella (2017), eles podem reduzir o risco de ocorrência de crimes digitais e cibernéticos, atuando como uma proteção aos ativos da organização. De acordo com Baldissera e Nunes (2007), eles devem ser adquiridos, configurados e implementados com a finalidade de atingir o nível aceitável de risco.

Os principais mecanismos de segurança encontrados na literatura são descritos a seguir.

2.3.1 Controles de Acesso

A norma ABNT NBR ISO/IEC 27002 (2013, p.30) define que o objetivo do controle de acesso é “limitar o acesso à informação e aos recursos de processamento da informação”, ou seja, prevenir que pessoas não autorizadas tenham acesso físico ou lógico aos equipamentos, informações ou outro ativo de valor para a organização.

A norma também ressalta a importância de se definir perímetros de segurança para proteger as informações críticas ou sensíveis e as áreas que contenham as instalações de processamento da informação, sendo conveniente que estes perímetros sejam fisicamente sólidos, sem brechas que facilite uma invasão, que seja implantada uma área de recepção ou meios que controle o acesso físico ao local, além de construções de barreiras físicas e paredes e portas externas resistentes.

As portas externas devem ser protegidas adequadamente contra acesso não autorizados por meio mecanismo de controle (barras, alarmes, fechaduras). A norma orienta que seja estabelecida, documentada e analisada uma política de controle de acesso, baseada nos requisitos de segurança da informação e que sejam considerados de forma conjunta os controles de acesso físicos e lógicos.

Controles Físicos são conjunto de medidas com a finalidade de controlar o acesso das pessoas as áreas internas da organização. Usa-se registros e restrições de acesso para servir de barreira adicional ao acesso lógico. Como exemplos de controles de acesso físico temos: guardas de segurança (pessoas), chaves, fechaduras, cartões de controle de acesso, portas blindadas, detectores de metal, catracas com leitura biométrica, fechaduras com senhas.

Controles Lógicos pode ser compreendido como barreiras que controla ou impedem o acesso à informação de ambientes eletrônicos. Eles fazem a verificação da identidade dos usuários que solicitam entrada em recursos computacionais, como os próprios computadores, notebooks, smartphones, base de dados, entre outros sistemas e itens de hardware e software. Essa forma de segurança faz uso de mecanismos para de proteger as informações contidas

nesses equipamentos. Como exemplo, criptografia, assinatura digital, firewalls, antivírus, autenticação entre outros.

2.3.2 Autenticação

A autenticação é um mecanismo essencial de controle de segurança e muito comum. É fácil verificar a existência desse mecanismo em várias atividades hoje em dia. Por exemplo, para acessar a caixa de entrada de e-mail, redes sociais, fazer compras pela Internet, acessar um computador, sua conta bancária online ou em caixas eletrônicos, seja usando senha ou a digital. Em todos os casos, normalmente você precisará do código de usuário (próprio nome, CPF, número de matrícula, número de conta), ou seja, da sua identificação única daquele computador ou serviço, e de uma senha ou de outros mecanismos (cartão magnético, identificação digital, reconhecimento de voz) para se autenticar, ou seja, verificação da sua identidade.

Segundo Fontes (2006, p.54), por meio da identificação, o ambiente computacional é informado quem é a pessoa que está acessando a informação. Já a autenticação tem a finalidade de garantir que o usuário descrito no processo de identificação é realmente a pessoa que está afirmando ser. A identificação pode ser uma informação pública e de fácil conhecimento, enquanto que a autenticação deve ser mantida em sigilo, ou seja, se a autenticação, por exemplo, for uma senha, então não deve ser divulgada. Para Sêmola (2003, p.118), “os mecanismos de autenticação são fundamentais para os padrões de informatização, automação e compartilhamento de informações”.

Os métodos de autenticação se divide em três grupos distintos (CERT.br, 2012):

- Aquilo que você e - podem ser informações biométricas, como a impressão digital, a palma da sua mão, a voz ou a retina;
- Aquilo que você possui - um cartão de senhas bancárias, um token gerador de senhas;
- Aquilo que você sabe - perguntas de segurança, senhas etc.

Todas essas formas de autenticação possui custos. Segundo Fontes (2006), a senha é o método de menor custo e mais utilizado pois, além do baixo custo, possui um bom nível de

proteção. Apesar disso, é um método de autenticação que apresenta uma grande fragilidade devido muitos usuários optarem por senhas fracas e fáceis de serem descobertas.

Nesse contexto, é importante destacar que, independentemente do custo, as empresas que querem proteger suas informações devem implementar a solução mais adequada e coerente com os riscos e possíveis impactos que a organização pode sofrer caso o método de proteção seja violado. Além disso, é recomendado que os usuários sejam orientados a escolher senhas seguras. Conforme as orientações do Cert.br (2012), uma senha bem elaborada é aquela que é difícil de ser descoberta (forte), porém é fácil de ser lembrada. Não convém criar uma senha difícil que não consiga lembrá-la, como também, não convém criar uma senha fácil de ser lembrada se ela puder ser facilmente descoberta por um atacante.

Desse modo, Ferreira (2003, p.49 apud CARDOSO, 2013, p.36) recomenda que deve ser evitado a composição de senhas com os seguintes elementos:

- Nome do profissional;
- Ser igual à conta do usuário;
- Nomes de membros da família ou amigos;
- Nomes de lugares;
- Datas de nascimento;
- Placas ou marcas de carros;
- Números de telefone, cartão de crédito, carteira de identidade;
- Qualquer senha com menos de seis caracteres, dentre outros;

2.3.3 Firewall

O Firewall é um mecanismo de segurança que pode ser implementado com o uso de software, hardware ou ambos. Sua função basicamente é isolar a rede interna de uma organização da rede externa (como a Internet), permitindo ou bloqueando pacotes que entram e sai da rede. Desse modo, o firewall possibilita que administrador da rede controle o acesso a rede externa e os recursos da rede, gerenciando o fluxo de tráfego dos dados entre redes (KUROSE, 2010).

É uma ferramenta é bastante versátil, pois permite variadas configurações que pode ser adaptadas às mais diversas necessidades de uma organização, porém, como é um mecanismo conectado à rede, deve ser projetado ou instalado adequadamente, caso contrário, pode comprometer a rede, dando uma falsa sensação de segurança.

Kurose (2010) classifica os firewalls em três categorias: filtro de Pacotes, filtros de estados e gateways de aplicação.

O filtro de pacotes examina cada pacote que chega aplicando as regras específicas definidas pelo administrador e, baseado nessas regras, ele determina se deve deixar o pacote passar ou ser descartado. As regras de filtragem são baseadas no conteúdo do pacote como: IPs de origem e destino, números de portas de comunicação, tipo de protocolo, interface de rede.

Os filtros de estados basicamente é um aprimoramento do filtro de pacotes. A diferença é que os filtros de estado rastreiam conexões do tipo TCP (rede) e, a partir disso, faz a filtragem, determinando quais pacotes aceitar ou não. Além disso, pode permitir ou bloquear tráfego de com a porta, protocolo e o estado, como também monitorar toda a atividade a partir do momento que a conexão é aberta até ser fechada. Tem como vantagem a possibilidade de aumento no desempenho na transmissão dos dados.

Firewall do tipo gateway de aplicação "é um servidor específico de aplicação através do qual todos os dados da aplicação (que entram e saem) devem passar" (KUROSE, 2010, p.539). Por meio dele é possível atingir um certo nível de segurança, visto que ele é quem faz a conexão com o serviço de destino solicitado por um usuário.

Além desses firewall já citados, ainda existem outros, como por exemplo, o firewall pessoal e de Hardware.

O firewall pessoal "é um tipo específico de firewall que é utilizado para proteger um computador contra acessos não autorizados vindos da Internet" (CERT.br, 2012, p.57). Ele pode ser instalado no sistema operacional da máquina do usuário para proteger de ameaças da rede externa, como também internas.

Alguns sistemas operacionais comuns, como Windows, Linux, MacOS, já implementam em seu sistema esse tipo de firewall. Caso prefira não usar o do próprio sistema, existem diversas opções disponíveis (pagas ou gratuitas), como alguns pacotes de antivírus que, além de trazer outros softwares de segurança, também pode incluir firewalls. Alguns exemplos: ESET Internet Security, Kaspersky, Norton. É muito importante deixar o firewall pessoal sempre ativo, mesmo que a empresa já possua um firewall dentro da rede.

Já o Firewall de Hardware é um equipamento dedicado que possui um software de firewall instalado. Normalmente, ele tem uma performance maior que alguns firewall de software instalado em servidores comuns.

O firewall também dá a organização a possibilidade de aplicar regras de conduta para evitar ou impedir que os usuários acessem sites de rede sociais ou sites específicos, por exemplo, como também, para impedir que o usuário baixe arquivos de música, vídeos, jogos.

2.3.4 Sistema de Detecção de Intrusos (IDS)

Segundo Kurose (2010), um IDS é "um dispositivo que gera alertas quando observa tráfegos potencialmente mal intencionados", ou seja, é um sistema que tentam reconhecer ações ou comportamento intrusivos por meio de monitoramento e análises disponíveis em informações de um sistema computacional ou rede, emitindo alertas caso detecte acessos não autorizados aos recurso de rede.

Sêmola (2003) destaca que o IDS atua como um dispositivo complementar ao firewall, colaborando inteligentemente com processo de combate a ataques e invasões, visto que é orientado ativamente por uma base de dados dinâmica que possui informações sobre comportamentos suspeitos de pacotes de dados e assinaturas de ataques.

Existem também os IPS (Sistemas de prevenção de intrusão), também é um dispositivo, porém diferentemente dos IDS, eles não gera alertas, apenas filtra tráfego suspeito. Ambos (IDS,IPS), podem ser usados para detectar vários tipos de ataques, como mapeamento de redes, escaneamentos de portas ou de pilhas TCP, ataques de negação de serviço, vírus, worm, ataques de vulnerabilidades (KUROSE, 2010).

2.3.5 Redes Privadas Virtuais (VPN's)

A Internet é uma rede pública insegura, na qual as informações que trafegam por ela podem ser lidas e interpretadas por pessoas não autorizadas. Desse modo, não é viável que organizações façam uso diretamente de redes públicas para compartilhar suas informações ou mesmo se comunicar. Para evitar esse uso direto da rede pública, as organizações, nos dias atuais, tem a opção de utilizar redes privadas virtuais (VPNs).

Por meio de VPNs é possível garantir um nível de segurança na comunicação e compartilhamento de informações entre clientes e servidores, entre dois comutadores ou mais dispositivos. Quando as organizações for utilizar a Internet dentro da empresa, a conexão vai acontecer através da VPN. Ela cria um canal virtual (ou tunelamento) dentro da Internet que é criado devido ao uso dos servidores VPNs e, dentro desse canal é que vai ser feito a comunicação entre a organização e suas filiais de forma privada usando a estrutura de rede pública (Internet), porém todo o tráfego de informações serão criptografados, mesmo que criminosos consigam interceptar a comunicação, eles não conseguirão acessá-las. De acordo com Tanenbaum (2003, p.584), VPNs são "redes sobrepostas às redes públicas, mas com a maioria das propriedades de redes privadas".

2.3.6 Criptografia

A criptografia é considerada atualmente um dos principais mecanismo de segurança para de enviar informações pela Internet e se proteger dos riscos que ela possibilita. De acordo com Laureano (2006), a palavra criptografia tem origem grega a (kriptos = escondido, oculto e grifo = grafia,escrita). É definida como a arte ou ciência de escrever em cifras ou em códigos, para isso, utiliza um conjunto de técnicas para tornar uma mensagem incompreensível, por meio de um processo chamado cifragem, na qual que apenas o destinatário desejado consegue decodificar e ler a mensagem com clareza, no processo inverso, a decifragem. Com seu uso é possível (CERT.br, 2012, p.67):

- proteger os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas e a sua declaração de Imposto de Renda;
- criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- proteger seus backups contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
- proteger as comunicações realizadas pela Internet, como os e-mails enviados/recebidos e as transações bancárias e comerciais realizadas.

Existem basicamente dois tipos, a simétrica e a assimétrica:

- **Criptografia Simétrica -** este modelo utiliza a uma mesma chave secreta para codificar como para decodificar uma mensagem, informações ou arquivos, nesse processo, a chave utilizada deve ser conhecida por ambos os lados. Exemplos desse

método criptográfico: AES, Blowfish, RC2, RC4, RC5, 3DES e IDEA (CERT.br, 2012).

- **Criptografia assimétrica -** este tipo de criptografia, também reconhecida como chave pública, usa duas chaves distintas que se complementam: chave pública e a privada. A pública pode ser livremente divulgada, no entanto, a privada deve ser mantida em segredo por seu dono. Assim, uma informação codificada com uma das chaves, só pode ser decodificada com a outra chave do par. A escolha de qual chave usar para codificar depende da proteção desejada, se confidencialidade ou autenticação, integridade e não-repúdio. Exemplo de sistema que usam chaves assimétricas: RSA, DSA, ECC e Diffie-Hellman (CERT.br, 2012).

2.3.7 Assinatura Digital

Esse mecanismo, assinatura digital, permite comprovar a autenticidade e a integridade de uma informação, atestando que ela foi realmente gerada por quem diz ser e que não passou por alterações (CERT.br, 2012). Esse método é muito utilizado em conexões seguras, transações bancárias via Internet. Conforme Vianna (2015), por meio da assinatura digital é possível verificar as propriedades de autenticidade, integridade e não repúdio.

2.3.8 Certificado Digital

Segundo a Cert.br (2012), “certificado digital é um registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública”, ou seja, ele é um arquivo eletrônico que contém dados que comprovam a identidade de alguma instituição, empresa, pessoa, serviços na rede ou equipamentos.

A Autoridade Certificadora (AC), é a entidade responsável pela emissão e veracidade dos dados, como também a responsável por publicar informações sobre certificados que não são mais confiáveis. A pessoa que desejar adquirir um certificado digital deve dirigir-se pessoalmente a uma autoridade de registro portando seus de documentos pessoais. Sua a presença física é indispensável, visto que,esse documento eletrônico será a seu documento oficial no mundo virtual.

2.3.9 Registro de Eventos (*Logs*)

Segundo CERT.Br (2012, p.53), “Log é o registro de atividade gerado por programas e serviços de um computador. Ele pode ficar armazenado em arquivos, na memória do computador ou em bases de dados”. Por meio deles é permite ao administrador descobrir e detectar usos indevidos dos computadores, ataques de força bruta ou exploração de vulnerabilidades, rastrear ações, detectar problemas de hardware ou softwares, entre outros problemas. Eles muito importante para notificação de incidentes, pois permitem que diversas informações essenciais sejam detectadas.

2.3.10 Ferramentas Antimalware

Ferramentas antimalware são programas “que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, antispyware, antirootkit e antitrojan são exemplos de ferramentas deste tipo. ” (CERT.BR, 2012, p.55). Atualmente, existem programas antivírus com diversas funcionalidades como firewall, verificação automática de e-mails, antispyware entre outras.

Apesar das diversas funcionalidades, esses programas não detecta códigos maliciosos recém criados, pois eles fazem a proteção de acordo com base de dados contendo as assinaturas dos vírus de que podem eliminar. Assim, os vírus recém descobertos só podem ser detectados após a atualização da base de dados. Desse modo, possuir um bom antivírus é fundamental.

De acordo com Mendonça (2010, p.2), um bom antivírus deve analisar e eliminar todos os vírus conhecidos como também outros tipos de malware, fazer análises em tempo real dos arquivos obtidos pela Internet, fazer a verificação agendada de discos rígidos e unidades removíveis, como CDs, DVDs e pen drives, verificar e-mails e anexos, como também atualizar as assinaturas de vírus e malwares conhecidos pela rede diariamente.

Os programas antivírus existentes no mercado podem ser pagos, gratuitos ou online. O primeiro é preciso comprar a licença para poder utilizar, o segundo pode ser adquirido e instalado sem restrições e o online não precisa ser instalado, porém requer manter conexão

com a Internet, ele pode ser gratuito ou pago. Algumas opções pagas também oferece versões gratuitas, porém com menos recursos.

Mendonça (2010), destaca que em alguns testes de comparação de detecção de vírus, ambos (pagos e gratuitos), foram equivalentes. O Cert.br (2012), orienta que para escolher de antivírus que melhor se adapte a necessidade de cada ambiente é importante levar em conta o uso que se faz e as características de cada versão.

De acordo com Ferreira, Araújo (2008, p.92 apud CARDOSO, 2013, p. 40).

> O uso de software pirata está diretamente associado à propagação de vírus em ambientes informatizados. As políticas de segurança da informação devem seguir os seguintes procedimentos:
> • Uso obrigatório de software antivírus em todos os equipamentos;
> • Atualização periódica da lista de vírus e da versão do produto;
> • Verificação de todo o arquivo recebido anexado em e-mail, ou download, pelo software antivírus;
> • Disponibilização de treinamento adequado que oriente a utilização do software de antivírus para os usuários.

É importante que a organização esteja atenta e siga as devidas orientações sobre o uso e escolha de um bom programa antivírus no ambiente, porém de nada adianta se seus usuários não estiverem bem treinados e conscientizados sobre o uso correto dessa ferramenta.

2.3.11 Cópias de Segurança (*Backups*)

Muitas organizações adotam diversos mecanismos de segurança para proteger suas informações, porém, muitas vezes esquecem de um mecanismo extremamente importante: os *backups*.

É muito importante que a organização faça frequentemente cópias de segurança dos dados que estão armazenados nos computadores, não só para recuperar algum dado que por ventura tenha sido apagado ou alterado acidentalmente ou intencionalmente, mas também, para se recuperar de eventuais falhas (de hardware ou software), de ataques de códigos maliciosos, de perdas, danos ou furtos de equipamentos e dispositivos ou simplesmente para guardar os dados que são pouco utilizados ou raramente alterados no dia a dia do ambiente organizacional (CERT.BR, 2012).

Segundo orientações do Cert.br (2012), a realização de backups pode ser feita através do próprio sistema operacional que pode possuir ferramentas de backups, por meio de

programas externos ou ainda através de soluções simples como enviar a cópia do arquivo para um e-mail, salvar em mídias como *pen drives,* cartões de memórias, discos rígidos (HDs), CDs, DVDs, discos de Blu-ray ou online, usando serviços na nuvem. A escolha de qualquer uma das ferramentas deve ser analisada conforme tipo de equipamento, do programa que será usado, da conectividade, capacidade de armazenamento, custo e confiabilidade.

É necessário que os funcionários se atentem para uma escolha adequada, visto que um CD ou DVD, além de armazenarem pequenas quantidades de dados podem sofrer danos físicos e lógicos (perda, roubo, destruição, portar vírus). Os *pen drives* são indicado para transportar dados que podem ser constantemente modificados, porém também podem sofrer danos físicos e lógicos, além de que se algum arquivo for apagado pode não ser possível recuperá-lo com procedimentos convencionais. O disco rígido externo pode ser usado para grandes volumes, mas também podem apresentar falhas. Já o armazenamento na nuvem também pode ser uma boa opção. Existem serviços de backups e armazenamentos de arquivos na nuvem gratuitos, com limites de armazenamentos, porém é necessário conexão constante com a Internet.

A frequência de realização de backup vai depender da periodicidade com que se cria ou se modifica os arquivos, podendo ser diariamente se os arquivos forem modificados constantemente, semanalmente ou mensalmente para aqueles poucos alterados. É necessários tomar alguns cuidados básicos, como: manter nos backups apenas arquivos confiáveis; armazená-los em lugares que não fique expostos ao frio, calor, poeira ou umidade; armazená-los em dois ou mais lugares diferentes; evitar que pessoas não autorizadas tenham acesso a esses lugares; armazenar os dados que são sensíveis em formato criptografado, entre outros cuidados.

2.3.12 Cuidados com Programas Instalados

É importante que a instalação de programas não originais sejam bloqueados pois, muitos códigos maliciosos se propagam por meio de softwares piratas, como também, muitos fabricantes não permitem a realização de atualizações quando detectam versões não licenciadas (CERT.BR, 2012).

Segundo Ferreira, Araújo (2008, p.93 apud CARDOSO, 2013, p. 37), a organização deve ressaltar na política de segurança todos os programas de computador em uso e proibir a instalação de softwares que não sejam de propriedade da organização. É recomendado também manter os programas instalados sempre atualizados e com as versões mais recentes, visto que, as novas versões ou atualizações foram corrigidas as possíveis falhas e vulnerabilidades identificadas (CERT.BR, 2012).

2.3.13 Segurança em Redes Wi-Fi

Segundo o Cert.br (2012), a rede Wi-fi (sem fio) é um tipo de conexão que utiliza sinais de rádio para comunicação. É possível configurar uma conexão sem fio por meio de infraestrutura, utilizando um concentrador de acesso (Access Point -AP) ou um roteador wireless, ou ponto a ponto (ad-hoc), no qual um pequeno grupo de máquinas podem se comunique diretamente, sem a necessidade, por exemplo, de um roteador *wireless,* bastando apenas que os computadores tenham placa de rede Wi-Fi.

Devido a popularidade, facilidade de instalação e uso frequente em diversos ambientes, as redes sem fio também estão sujeitas a ameaças e ataques, por isso é extremamente importante que a organização gerencie bem o acesso a essa rede usando configurações adequadas. Dentre os mecanismos de segurança existentes para essa rede, o Cert.br (2012, p. 103) destaca:

> **WEP (Wired Equivalent Privacy):** primeiro mecanismo de segurança a ser lançado. É considerado frágil e, por isto, o uso deve ser evitado.
> **WPA (Wi-Fi Protected Access):** mecanismo desenvolvido para resolver algumas das fragilidades do WEP. É o nível mínimo de segurança que é recomendado.
> **WPA-2:** similar ao WPA, mas com criptografia considerada mais forte. É o mecanismo mais recomendado.

Como pode ser observado, é recomendado usar WPA2 por ser mais seguro, visto que possui um nível de criptografia mais forte. Além disso, as organizações também podem tomar outros cuidados, como (CERT.BR, 2012):

- Solicitar que seus funcionários habilitem a rede Wi-fi do computador ou outro dispositivo quando for usar a rede e desabilitá-la após o uso;
- Solicitar que seus funcionários evitem o acesso a serviços que não utilizem conexão segura ("https");

- Considerem o uso de criptografia nas aplicações, como por exemplo, para o envio de e-mails, conexões remotas ou ainda VPNs;
- Se a organização tiver restrições de acesso para poucos usuários é recomendado desabilitar a difusão (broadcast) do SSID, evitando que o nome da rede seja anunciado para outros dispositivos;
- Alterar as senhas originais, tanto de administração do concentrador de acesso ou roteador como de autenticação de usuários;
- Desabilitar o gerenciamento do roteador via rede sem fio, assim, para acessar funções de administração, será necessário conectar-se diretamente a ele usando uma rede cabeada. Desta maneira, um possível atacante externo (via rede sem fio) não será capaz de acessar o roteador para promover mudanças na configuração.
- Desabilitar a função WPS (Wi-Fi Protected Setup) a fim de evitar acessos indevidos.

O uso desses cuidados podem evitar acessos indevidos à rede sem fio dos diversos ambientes organizacionais. Por isso é importante que a organização tenha uma pessoa responsável e com conhecimento técnico para aplicar as configurações necessárias para manter a rede segura.

2.3.14 Cuidados ao Permitir a Navegação na Rede

Devido muitas ameaças digitais estarem ligadas ao acesso à Internet, é necessário que a organização faça o monitoramento dos acessos dos usuários, como também, é importante fazer restrições de acesso a algumas páginas que podem gerar algum risco. Ferreira, Araújo (2008, apud CARDOSO, 2013), recomenda que seja definido na política de segurança da informação regras de acesso à Internet no local de trabalho, visto que, o acesso pode prejudicar a produtividade da organização.

O uso do correio eletrônico, por exemplo, possibilita dentro das organizações a troca de informações e comunicações de forma eficiente, porém, também é por meio deles que muitos atacantes conseguem aplicar as mais variadas técnicas, golpes, além de disseminar códigos maliciosos, tudo com intuito de tentar invadir sistemas e computadores na intenção de descobrir informações sigilosas.

Em virtude dos risco que o uso do correio eletrônico pode submeter é necessário que as organizações abordam regras de uso e administração de e-mails em suas políticas de segurança, como também treinem e conscientizem seus funcionários para o uso adequado, considerando os aspectos de armazenamentos, conteúdo e transmissão de informações confidenciais por meio deles (FERREIRA, ARAÚJO, 2008, apud CARDOSO, 2013).

2.2.15 Conscientização e Treinamento em Segurança da Informação

A maior parte dos problemas originados internamente na organização é devido o desconhecimento dos usuários em relação aos procedimentos e conceitos básicos de segurança. É por esse e outros motivos que a organização deve manter uma rotina constante de conscientização, educação e treinamento para promover a segurança da informação no ambiente. A norma ABNT NBR ISO/IEC 27002 (2013, p.20) recomenda que que todos os funcionários da organização e partes externas recebam treinamento, educação, conscientização e atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

É preciso que a organização estabeleça regras, requisitos de segurança, e as responsabilidades legais para o uso correto dos recursos de TI existentes no ambiente, como também, conscientizem sobre dos riscos que podem ficar expostas. Esses procedimentos é importante para que os usuários comecem a entender os danos que eles podem causar usando de forma incorreta os recursos disponíveis.

Neste contexto, os passos iniciais para o processo de educação dos usuários dentro da organização é o estabelecimento de políticas e regras de segurança e logo em seguida a organização deve desenvolver um programa de conscientização orientando a todos como devem seguir tais regras para que a organização alcance um nível adequado de segurança da informação. No entanto, é preciso que as organizações não se limitem apenas em definir por escrito as regras das políticas, é necessário um esforço maior para orientar todos funcionários e colaboradores que trabalham com as informações, sistemas e computadores do ambiente organizacional, fazendo com que aprendam e sigam as regras (MITNICK; SIMON, 2003).

Com programas de conscientização e treinamento propostos e definidos pelos administradores, todos devem compreender os riscos que o uso indevido, por exemplo, de

redes sociais, e-mails com conteúdo suspeito, download de arquivo, troca de informações sobre a empresa podem trazer. Segundo Dhillon (2001), muitos problemas de segurança que acontecem é devido à ausência de medidas de segurança da informação, porém, mesmo existindo uma estrutura de medidas no ambiente organizacional, é preciso transmiti-las corretamente aos colaboradores através dos canais de comunicação adequados.

Desse modo, com a correta conscientização e treinamento, os usuários vão ser capazes de aplicar as regras e orientações de segurança definidas. Resumidamente, Pimenta e Quaresma (2016, p.536) afirmam que os usuários, além dos mecanismos de segurança definidos, devem adotar as seguintes medidas de segurança no seu posto de trabalho:

- Aplicar as atualizações de segurança recomendadas
- Utilizar e atualizar com frequência os programas antivírus e antispyware
- Realizar cópias de segurança com regularidade
- Utilizar senhas robustas e diferentes em cada aplicação
- Procurar enviar/transferir a sua informação de forma encriptada
- Não partilhar a informação do seu computador com outros
- Não compartilhar ou divulgar as suas senhas com os outros
- Ser responsável e cuidadoso na utilização da Internet e do correio eletrônico
- Ser cuidadoso na utilização de equipamentos de armazenamento externos
- Informar no caso de incidentes com vírus, roubos ou perdas de informação
- Estar ciente que todos os atos praticados têm consequências
- Utilizar um firewall.
- Bloquear o computador quando se ausentar
- Não utilizar software ilegal ou de compartilhamento de arquivos.

Para que os funcionários apliquem todas essas medidas é preciso que esses programas de treinamento e conscientização sejam realizados constantemente para que eles entendam a importância de tais medidas, visto que, com o passar do tempo surgem novas ameaças e técnicas, fazendo com que seja necessário reforçar e atualizar ainda mais os princípios da segurança da informação na mente dos funcionários e colaboradores.

2.4 A Importância da Política de Segurança da Informação na Organização

Todo ambiente organizacional, seja de pequeno, médio ou grande porte, lidam com informações sensíveis que precisam ser constantemente protegidas, por isso, é fundamental o que estes ambientes estabeleçam uma política de segurança da informação para evitar ou diminuir os riscos dessas informações sigilosas serem acessadas indevidamente. Conforme estabelece a norma ABNT NBR ISO/IEC 27002 (2013, p.8) “Convém que um conjunto de

políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes".

Segundo Dias (2000, apud LAUREANO, 2010, p. 56), a política é um mecanismo preventivo de segurança das informações e processos de uma organização. Através dela a organização define um padrão de segurança a ser seguido pelo corpo técnico, gerencial e usuários, internos ou externos. O desenvolvimento de uma política de segurança da informação deve ser o primeiro e mais importante passo para proteger as informações da organização contra eventuais ameaças e ataques, quer estes tenham origem interna ou externa (KNAPP et al, 2009). De acordo com Sêmola (2003, p.34), a elaboração de uma política de segurança deve oficializar o posicionamento da empresa com relação ao tema e apontar as melhores práticas para o manuseio, armazenamento, transporte e descarte de informações de acordo com a faixa de risco delimitada.

Por meio de uma política de segurança a organização estabelece a hierarquia dos riscos de informação, identificando metas aceitáveis de segurança, quais os mecanismo que será usado para atingir essas metas, como também, precisará estimar o custo para atingir o nível aceitável de risco (LAUDON; LAUDON, 2010)

Antes de se implementar a política é preciso passar por etapas para a sua elaboração como a de planejamento e definição. Essas etapas envolvem conhecimentos abrangentes sobre segurança, organização, cultura, pessoas e tecnologias. Normalmente é uma tarefa difícil e trabalhosa porém, de acordo com Spanceski (2004), a maior dificuldade é na implementação da política criada, pois é preciso que todos os funcionários conheçam a política, compreendam e sigam as normas e procedimentos estabelecidos.

Uma PSI deve: descrever o que está sendo protegido e por quê; definir prioridades sobre o que precisa ser protegido em primeiro lugar e com qual custo; estabelecer um acordo explícito com várias partes da empresa em relação ao valor da segurança; fornecer ao de departamento de segurança um motivo válido e autoridade para dizer "não" quando necessário e sustentá-lo; como também, deve impedir que esse departamento tenha desempenho insignificante (LAUREANO, 2005).

Ao desenvolver uma política de segurança, é necessário que ela esteja de acordo com os objetivos de negócio da organização. O responsável pela sua elaboração deve levar em consideração que existem funcionários que não têm conhecimento da linguagem técnica, além

de deixar claro o quanto esse documento é importante para evitar que os empregados a encare como perda de tempo e não cumpra as regras estabelecidas (MITNICK; SIMON, 2003).

Ferreira e Araújo (2008) citado por Pontes (2014) diz que uma política deve ser: simples; compreensível; aprovada e assinada pela alta administração; estruturada, permitindo a sua implantação por fases; alinhada com as estratégias de negócios da organização, padrões e procedimentos já existentes; orientadas aos riscos; flexível; protetora dos ativos de informação, privilegiando os de maior valor e importância; positiva, não apenas concentrada em ações proibitivas ou punitivas.

É importante considerar que para uma efetiva implementação de uma política de segurança é necessário realizar programas de treinamento, conscientização e divulgação da mesma, destacando sua importância e benefícios, como também, os danos e consequências que podem acontecer caso alguém deixe de seguir as regras estabelecidas (SPANCESKI, 2004).

Mitnick; Simon (2003) ressalta que a política não deve ser um documento inalterável, é preciso que seja atualizada conforme o surgimento de novas tecnologias ou a medida que surgem novas vulnerabilidades, ameaças e ataques, sendo também necessário que a organização estabeleça procedimentos regulares com objetivo de identificar novas ameaças. Para a norma ABNT NBR ISO/IEC 27002 (2013, p.10) é conveniente que "as políticas para a segurança da informação analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia".

É necessário que a política e documentos auxiliares estejam disponíveis em lugares acessíveis para que sejam examinados com frequência, além de facilitar para que os funcionárias façam consultas em caso de dúvidas relacionada às políticas e procedimentos de segurança (MITNICK; SIMON, 2003).

Como estabelece a norma ABNT NBR ISO/IEC 27002 (2013, p.9) "Políticas de segurança da informação podem ser emitidas em um único documento, 'política de segurança da informação' ou como um conjunto de documentos individuais, relacionados". A própria norma dá exemplos de políticas com tópicos específicos que podem ser adotadas na organização, como políticas de controle de acesso, classificação e tratamento da informação; segurança física e do ambiente; tópicos orientados aos usuários finais, como uso aceitável dos ativos; mesa limpa e tela limpa; transferência de informações; dispositivos móveis e trabalho

remoto; restrições sobre o uso e instalação de software; backup; transferência da informação; proteção contra códigos maliciosos; entre outras.

Segundo Laudon e Laudon (2010), a política de segurança dá origem a outras políticas que determinam o uso aceitável dos recursos de informação da organização e quais membros terão acesso a esses ativos. De acordo com o autor, uma política de uso aceitável, por exemplo, é definido qual o uso aceitável dos recursos de informação e equipamentos de informática, como computadores, notebooks, dispositivos sem fio, telefones, Internet. Por meio dessa política a organização deve deixar claro as orientações relacionada à privacidade, à responsabilidade do usuário e ao uso pessoal das redes e equipamentos de tecnológicos.

Uma política de mesa e tela limpa, por exemplo, deve ser adotada para prevenir que acessos não autorizados cause danos às informações da organização. De acordo com a norma ABNT NBR ISO/IEC 27002 (2013, p.56), "Convém que seja adotada uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação...".

É importante que a organização adote uma política de mesa e tela limpa, ela contribui para a redução dos riscos de acesso não autorizado perda e dano da informação durante e fora do horário normal de trabalho. Esse tipo de política deve estabelecer que informações sensíveis e críticas, contidas em papéis ou em mídias eletrônicas, sejam guardadas em lugar seguro, como armários com chaves, cofres, principalmente se não estiverem em uso. Computadores também devem ser mantidos desligados ou com proteção de telas controlados por senhas ou outros mecanismos de autenticação. Também deve ser evitado o uso não autorizado de outros dispositivos como impressoras, multifuncionais, scanners, máquinas fotográficas digitais, mantendo sempre o cuidado de remover imediatamente as informações sensíveis contidas nestes dispositivos (ABNT NBR ISO/IEC 27002, 2013).

De acordo com Spanceski (2004), as políticas se divide em três tipos: Regulatória, Consultiva e Informativa.

- Regulatória - é definida como se fosse uma série de especificações legais. Uma política desse tipo descreve com riqueza de detalhes o que deve ser feito, quem deve fazer, fornecendo algum tipo de parecer relatando qual ação é importante. Elas devem assegurar que a organização está seguindo os procedimentos e normas para

seu ramo de atuação. São implementadas devido às necessidades legais impostas à organização (FERREIRA, 2003, apud SPANCESKI, 2004).

- Consultiva - políticas consultivas são bastante recomendadas, porém não são obrigatórias. Elas apenas sugere quais ações ou métodos devem ser utilizados para a realização de uma tarefa, esclarecendo as atividades cotidianas da organização aos seus funcionários e colaboradores de maneira bastante direta.
- Informativa - uma política desse tipo tem apenas caráter informativo, não existem riscos caso não seja cumprida. Porém, apesar de não ser tão exigente, pode contemplar uma série de observações importantes ou advertências severas.

Independentemente do tipo de política, o importante é que as organizações não deixem de adotar em seu ambiente políticas de segurança a fim de garantir que as informações e recursos de informática serão usados de maneira adequada e de acordo com critérios definidos. Dessa maneira, a organização consegue manter um controle adequado da informação, como também, informa cada pessoa quais suas obrigações na proteção da tecnologia e da informação. Além disso, por meio da política, são identificados os mecanismos necessários para alcançar os requisitos propostos, visto que, a adoção de um conjunto de ferramentas de segurança é ineficiente sem a existência orientadora de uma política de segurança da informação. Como sugere Laureano (2005, p. 57-58):

> - Uma boa política hoje é melhor do que uma excelente política no próximo ano;
> - Uma política fraca, mas bem-distribuída, é melhor do que uma política forte que ninguém leu;
> - Uma política simples e facilmente compreendida é melhor do que uma política confusa e complicada que ninguém se dá o trabalho de ler;
> - Uma política cujos detalhes estão ligeiramente errados é muito melhor do que uma política sem quaisquer detalhes;
> - Uma política dinâmica que é atualizada constantemente é melhor do que uma política que se torna obsoleta com o passar do tempo;
> - Costuma ser melhor se desculpar do que pedir permissão.

Portanto, embora o estabelecimento de uma política de segurança da informação imponha a adoção de novas práticas difíceis de se implementar, é melhor que a organização a tenha do que nunca venha se preocupar com essa questão.

3 A PESQUISA SOBRE SEGURANÇA DA INFORMAÇÃO NAS ESCOLAS

Este capítulo irá abordar a pesquisa que foi realizada nas 7 instituições públicas do município de Girau do Ponciano em sua área urbana. A pesquisa teve como objetivo investigar a realidade situacional das escolas municipais com relação a segurança da informação, observando as práticas e os procedimentos adotados para proteger as informações nestas instituições e qual o conhecimento dos colaboradores sobre o assunto.

3.1 Preparação para Coleta de Dados

Para a preparação foi discutido qual instrumento seria utilizado para realizar a coleta de dados, optou-se por utilizar o questionário físico (Apêndice A) que teve sua aplicação realizada entre 29 de maio de 2019 à 20 de junho de 2019.

O questionário continha questões fechadas e abertas que foram escolhidas de acordo com o objetivo deste estudo e com base na literatura estudada, assim como uma entrevista semiestruturada que foi aplicada junto aos diretores escolares. Todos os entrevistados tiveram seu sigilo garantido e, a pedido deles, o nome das escolas também foi mantido em sigilo. Antes das entrevistas era lido um texto sucinto de apresentação para fins de esclarecimento.

3.2 Análise Crítica dos Resultados

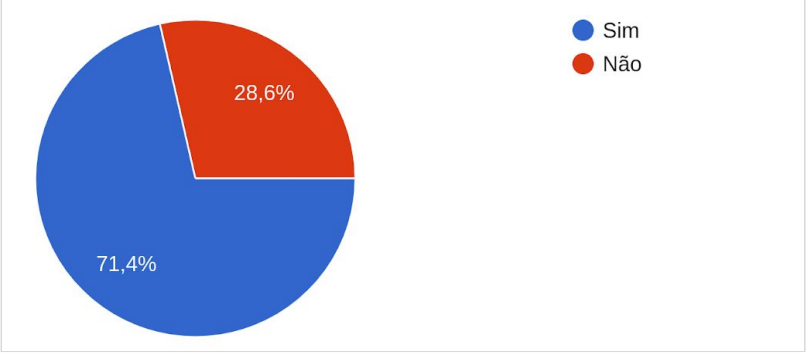
Os resultados a seguir representam as afirmações dadas pelos respondentes desta pesquisa. Para cumprir com os objetivos da pesquisa, foram selecionados apenas alguns os resultados. Desse modo, para verificar o resultado completo da pesquisa, consulte o Apêndice B.

A educação básica ofertada pelo município em suas escolas compreende desde a educação infantil ao ensino fundamental (1º ao 9º ano). Algumas escolas disponibilizam a modalidade de educação de jovens e adultos (EJA). Quanto aos horários de funcionamento das escolas, 85,7% funcionam em períodos matutinos e vespertinos e 42,9% delas funcionam no período noturno. Recentemente o município também oferta em uma das escolas o ensino

integral, atendendo apenas a educação infantil. A média[2] de alunos matriculados nas escolas pesquisadas foi de 474 alunos, sendo que a quantidade mínima foi 150 e máxima foi 1200 alunos. A quantidade de funcionários também é relevante, 42,9% das escolas possuem um quantitativo entre 30 a 50 funcionários e em 57,1% delas o número é bem maior, ficando entre 50 a 100. Essa quantidade de alunos e funcionários é bem significativa, podendo impactar tanto positivamente quanto negativamente a segurança da informação nessas escolas.

Conforme Figura 5, nota-se por parte dos entrevistados (28,6%) o desconhecimento com a questão da segurança da informação e, apesar dos demais entrevistados (71,4 %) informarem ter conhecimento sobre o assunto, demonstraram um pouco de insegurança ao responder, não sabendo nos explicar se é ou como é aplicada a segurança da informação.

Figura 5 - Conhecimento dos entrevistados sobre segurança da informação.



Fonte: Elaborado pelos autores (2019).

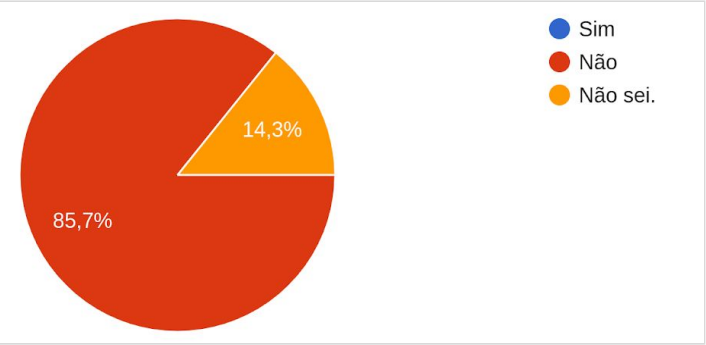
Observou-se que alguns funcionários, inclusive alguns que trabalham diretamente com as informações, acreditam que segurança da informação é um dever apenas de departamentos como secretaria e direção escolar. Dessa forma, fica evidente que existe uma carência de treinamento, conscientização e educação dos funcionários para com a segurança da informação nos ambientes escolares.

Com base nas respostas obtidas, Figura 6, existe também a necessidade de se estabelecer uma política de segurança da informação nesses ambientes, visto que 85,7% informaram não possuir uma política de segurança da informação explícita e 14,3% responderam não saber da existência de alguma.

[2] Média referente aos alunos matriculados no ano 2019.

Ao se implantar uma PSI corretamente, com o devido treinamento e divulgação, todos os funcionários passarão a ficar cientes de suas responsabilidades para com a segurança das informações no ambiente escolar.

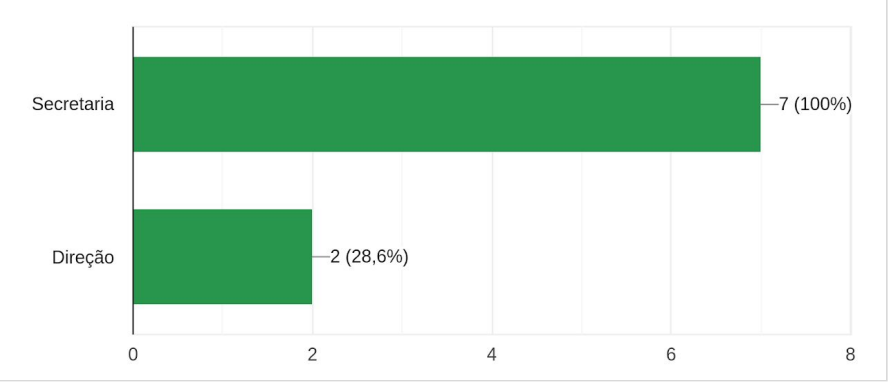
Figura 6 - Utilização de uma política de segurança da informação.



Fonte: Elaborado pelos autores (2019).

Todos os entrevistados informaram que as informações são produzidas e manipuladas manualmente e digitalmente, sendo portanto, guardadas em armários (aço, madeira), *pen drives* e computadores localizados na secretaria da escola. Destes, 28,6% além de armazenarem na secretaria, também guardam informações importantes na sala da direção (Figura 7).

Figura 7 - Respostas sobre o local de produção e guarda das informações.



Fonte: Elaborado pelos autores (2019).

A secretaria das escolas possuem no mínimo dois e no máximo seis funcionários responsáveis distribuídos nos horários de funcionamento das escolas. Como pode ser observado na Figura 8, quando chega um novo funcionário no setor, 28,6% dos entrevistados responderam não ser passado as responsabilidades referente a segurança das informações utilizadas na escola. Apesar da quantidade ser relativamente baixa, se estes funcionários não

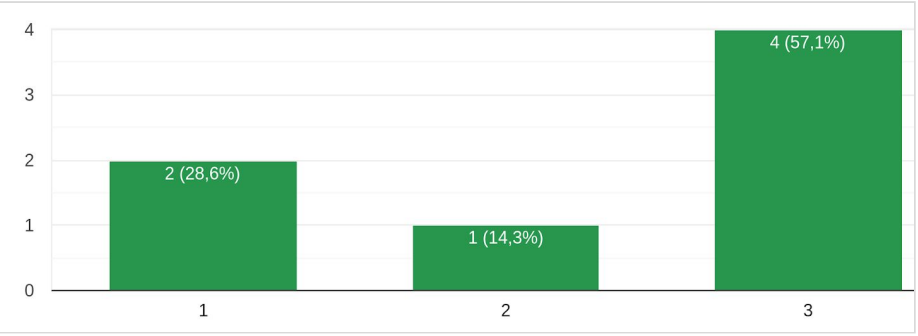
estiverem bem treinados e conscientes de suas responsabilidades perante as informações que produzem, manipulam e armazenam, podem representar sérios riscos para a segurança da informação.

Figura 8 - Responsabilidades sobre a segurança da informação para novos funcionários

Fonte: Elaborado pelos autores (2019).

Com base nas respostas informadas pelos entrevistados, todas as escolas possuem computadores. Como pode ser observado na Figura 9, foi levantado o número de computadores instalados nestas escolas, porém os que estão em funcionamento são utilizados para fins administrativos. Esta é uma questão importante, pois quanto maior o número de computadores, principalmente conectados à rede, maior será a possibilidade das vulnerabilidades existentes nesses computadores serem exploradas.

Figura 9 - Quantidade de computadores que as escolas possuem.



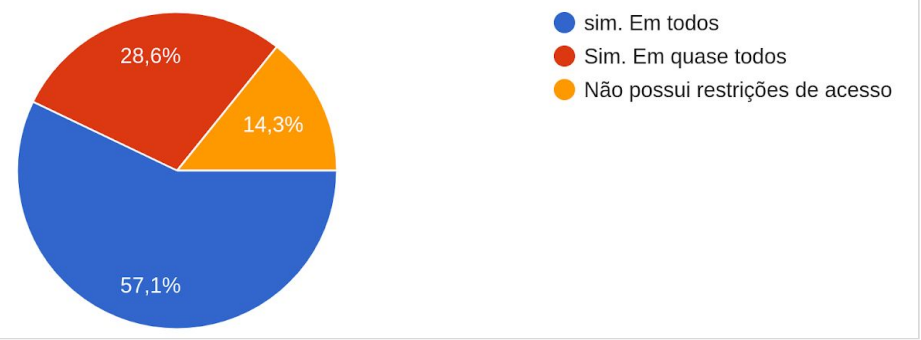
Fonte: Elaborado pelos autores (2019).

Nenhuma das escolas com mais de um computador conectado a rede possui um servidor de arquivos com o objetivo de proporcionar um local principal para o armazenamento compartilhado de arquivos com demais computadores na rede.

Dessa forma, mesmo usando apenas os computadores existente para compartilhar e armazenar as informações, percebe-se que estas são produzidas e armazenadas sem um correto gerenciamento, o que pode ser considerado um risco, visto que informações importantes podem ser acessadas ou alteradas por pessoas não autorizadas ou mesmo indevidamente pelos próprios funcionários, considerando que o setor possui vários responsáveis nos diferentes horários de funcionamento da escola.

Apesar disso, o risco das informações serem acessadas ou alteradas por pessoas não autorizadas pode ser diminuído bastante com o correto controle de acesso (físico e lógico) aos ambientes onde essas informações são manipuladas e armazenadas. Com base nas resposta dos entrevistados (Figura 10), quando questionados sobre a escola restringir ou controlar o acesso físico de pessoas a determinadas salas/departamentos, 57,1% disseram sim, todos as salas/departamentos possuem restrições/controles de acesso físico e que estas são obedecidas por todos, enquanto que 28,6% possuem restrições em quase todos, a mesma porcentagem responderam que as restrições algumas vezes não são obedecidas e, 14,3% responderam não possuir restrições de acesso.

Figura 10 - Controle de acesso físico aos setores.



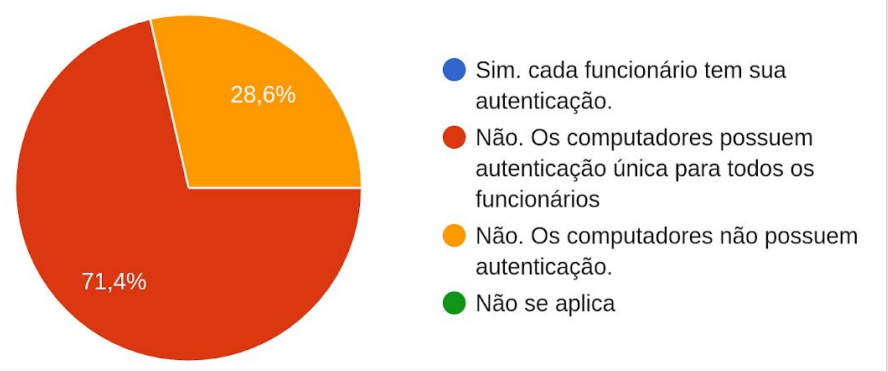
Fonte: Elaborado pelos autores (2019).

Questionamos se era permitido que outros funcionários, que não os responsáveis pelo setor, acessassem os computadores principais onde as informações são manipuladas e armazenadas, 85,7% responderam não, somente o responsável pelo setor tinha permissão para acessar os computadores e 14,3% responderam que era permitido, porém com autorização. É importante que esses ambientes mantenha esse controle de acesso aos recursos informacionais, proibindo o acesso de pessoas externas e até mesmo os próprios funcionários internos que não são responsáveis pelo setor. Esse já é um passo para evitar a quebra da

confidencialidade e integridade das informações. Porém, além de controles físicos, é importantes também adotar controles lógicos.

Controles lógicos evitam que informações, principalmente contidas nos meios digitais, sejam acessadas, alteradas ou mesmo excluídas acidentalmente ou propositalmente por pessoas internas ou externas à organização. Perguntamos aos entrevistados se para acessar os computadores da escola era necessário autenticação, 42,9% responderam que todos os computadores possuíam autenticação, 28,6% disseram que em quase todos. Porém, um ponto que destacamos como uma falha de segurança da informação nos ambiente escolares é o fato de que 71,4% as instituições utilizam apenas uma única autenticação comum aos funcionários ou simplesmente não utilizam autenticação alguma (28,6%), Figura 11.

Figura 11 - Autenticação para utilizar os computadores.



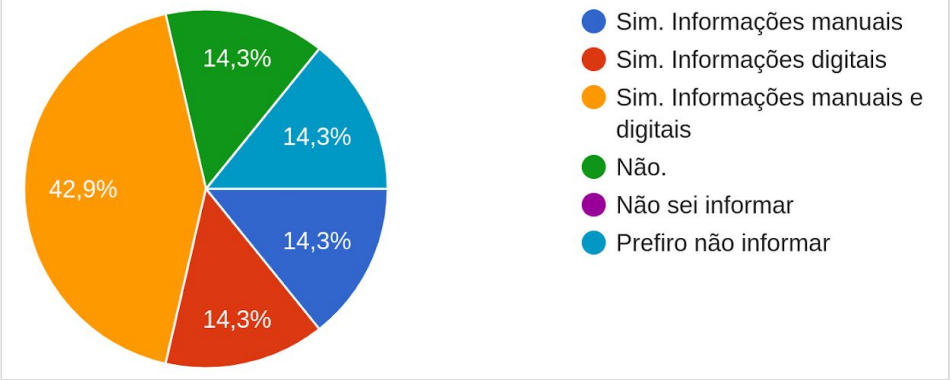
Fonte: Elaborado pelos autores (2019).

Dessa forma, os funcionários que trabalham com as informações nos diferentes horários de funcionamento da escola, utilizam as mesmas senhas para se autenticar aos computadores. O compartilhamento de senhas é considerado um risco para a segurança das informações de qualquer organização. Usar um único usuário e senha nos computadores para todos os funcionários que trabalham no setor não é seguro para as informações produzidas, visto que fica fácil da senha ser descoberta por qualquer outro funcionário da escola ou pessoa externa, como também, todos poderão ter acesso às informações com perfil de administrador.

Como pode ser observado na Figura 12, 42,9% das escolas já procuraram informações (manuais e digitais) que eram importantes e não encontraram. Esse fato além de ocasionar a quebra do princípio da confidencialidade das informações, também prejudica a

disponibilidade, posto que, no momento preciso, a informação procurada não estava disponível.

Figura 12 - Procuraram dados e informações importantes e não encontraram.

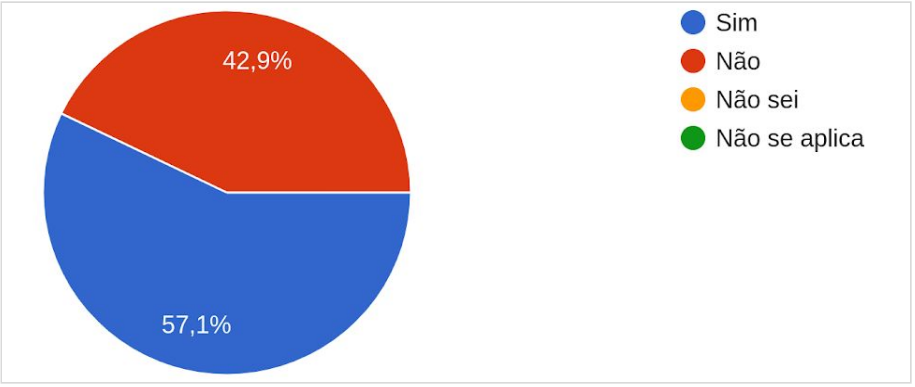


Fonte: Elaborado pelos autores (2019).

Por essas e outras ameaças que podem afetar os recursos informacionais que é importante que as escolas adotem controles fisícos e lógicos para assegurar a confidencialidade, integridade e disponibilidade das informações.

Algo que não condiz com as boas práticas de segurança da informação e que é realizado em 42,9% das instituições, é o fato dos funcionários não fazerem uso de bloqueio ou proteção de tela quando se ausentam por algum momento dos computadores (Figura 13). Esse tipo de ação pode colocar em risco a confidencialidade e a integridade das informações, por isso a importância da instituição adotar uma política de segurança da informação, definindo tópicos específicos como a política de mesa e tela limpa para orientar os funcionários quanto às práticas corretas ao se ausentar do setor por algum momento.

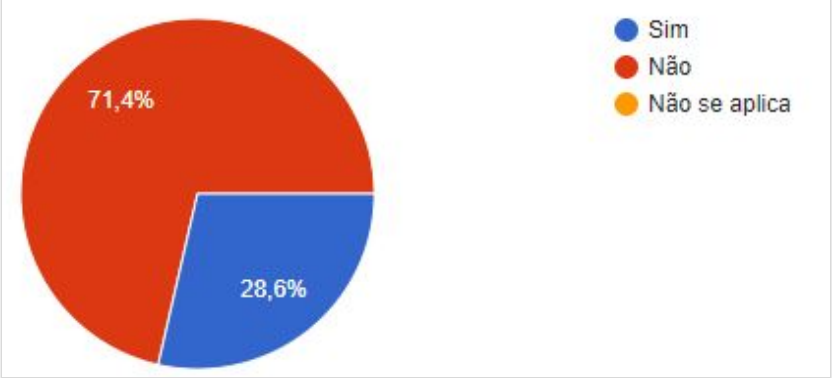
Figura 13 - Usam o bloqueio de tela do computador quando se ausentam.



Fonte: Elaborado pelos autores (2019).

Outro ponto a ser destacado e que pode colocar em risco as informações em 71,4% dos ambientes estudados (Figura 14), é o fato de que se um funcionário deixar a escola em que trabalhava, as senhas na qual esse funcionário utilizava para acessar os computadores bem como e-mails da instituição não são alteradas, o que pode ocasionar num sério problema, visto que esse funcionário poderá ainda ter acesso às informações até mesmo fora do ambiente escolar. Por esse motivo é importante que as escolas sempre alterem suas senhas regularmente, principalmente quando funcionários que tinham conhecimento das senhas não trabalham mais na escola.

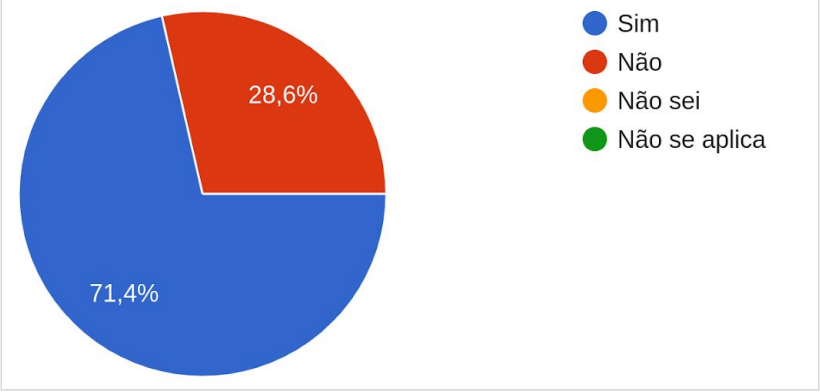
Figura 14 - Alteração das senhas utilizadas por funcionários afastados.



Fonte: Elaborado pelos autores (2019).

Perguntamos aos entrevistados se a escola fazia cópias de segurança com regularidade, 71,4% disseram que faziam (Figura 15). É muito importante que as escolas façam regularmente cópias de segurança de seus dados, observando principalmente qual o melhor local para guardá-las.

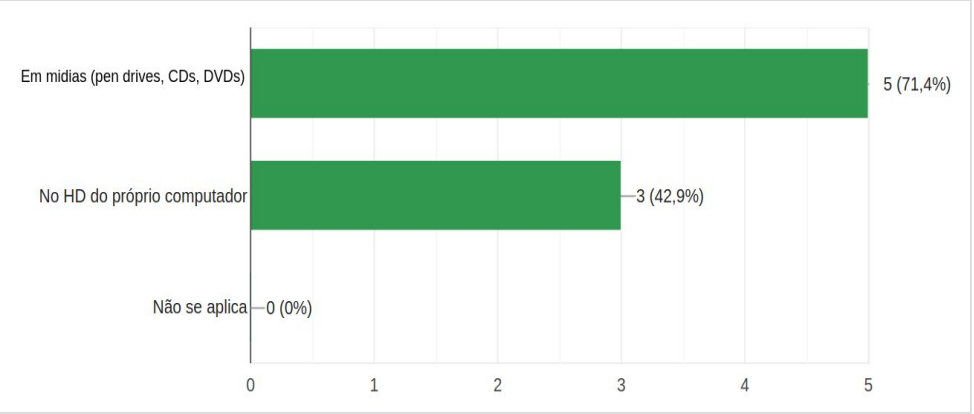
Figura 15 - Realização de cópias de segurança com regularidade.



Fonte: Elaborado pelos autores (2019).

Como pode ser observado na Figura 16, 71,4% informaram que armazenam as cópias de segurança em mídias (pen drives, CDs, DVDs). Durante a entrevista, os diretores informaram que a mídia mais utilizada é o *pen drive*. Dos entrevistados, 42,9% responderam que as cópias de segurança são armazenadas também no HD do próprio computador da escola.

Figura 16 - Local de armazenamento das cópias de segurança.



Fonte: Elaborado pelos autores (2019).

A prática de armazenar cópias de segurança nos próprios computadores normalmente é considerado um fator de risco pois, se uma ameaça, por exemplo, de *Ransomware*, conseguir explorar alguma vulnerabilidade existente nos computadores e sistemas e acabar criptografando todos os dados existentes, isso afetará também as cópia de seguranças que ali forem armazenadas.

Outro ponto a ser observado é o uso de *pen drives*. É preciso armazená-los em lugares seguros, que seja difícil o acesso de pessoas não autorizadas, como também, é importante criptografá-los se informações importantes e sigilosas estiverem armazenadas neles, assim, caso alguém não autorizado tenha acesso, não conseguirá visualizar tais informações ou mesmo copiar os dados existentes, posto que precisará informar a senha para ter acesso a essas informações.

Todas as escolas possuem Internet e uma conexão sem fio (Wi-fi) com senha de segurança para ser acessada. Como pode ser observado na Figura 17, 57,1% restringem o acesso para a área administrativa e direção escolar.

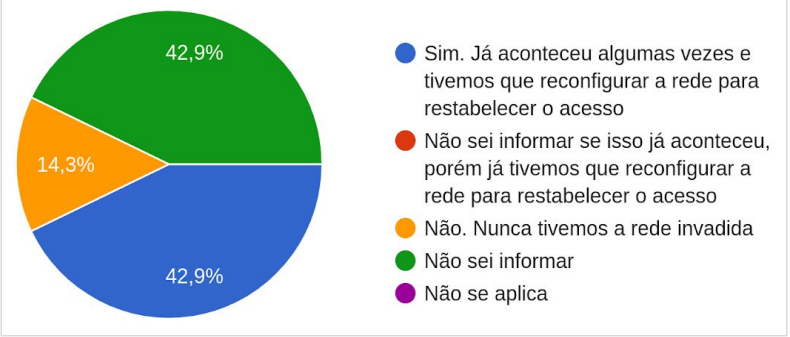
Figura 17 - Acesso à rede sem fio (Wi-fi).

Fonte: Elaborado pelos autores (2019).

Apesar da maioria das escolas restringir o acesso à rede, segundo os entrevistados, todos os computadores e dispositivos em funcionamento nas instituições ficam conectados na mesma rede. Consideramos essa ser uma situação potencialmente perigosa para os sistemas de informação das instituições, visto que 42,9% das escolas informaram que já tiveram sua rede invadida, necessitando reconfigurar toda rede para restabelecer o acesso. A mesma porcentagem (42,9%) não souberam informar se isso já havia ocorrido (Figura 18).

Invasões ou acessos indevidos às redes e sistemas são considerados incidentes para a segurança da informação. É preciso que estas instituições saibam identificar as vulnerabilidades existentes em suas redes e sistemas, para assim, evitar que estes incidentes venham impactar negativamente suas informações.

Figura 18 - Invasões à rede sem fio.

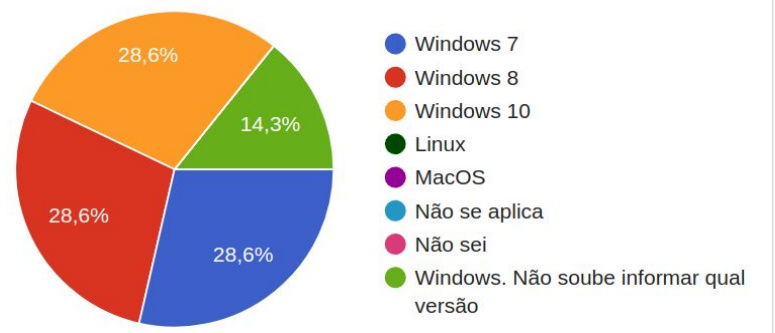


Fonte: Elaborado pelos autores (2019).

Abordou-se também o sistema operacional utilizado. Conforme figura 19, todas as escolas utilizam diferentes versões do sistema operacional *Windows*. Este sistema com relação a segurança pode apresentar sérios problemas, como por exemplo: facilidade de instalação de aplicativos e programas sem licença; acesso fácil ao sistema com perfil de administrador, o

que pode facilitar a instalação de programas maliciosos, reduzindo ainda mais o nível de segurança para as informações manipuladas nesses sistemas.

Figura 19 - Sistemas Operacionais instalados nos computadores das escolas.



Fonte: Elaborado pelos autores (2019).

Se comparado aos sistemas baseados em GNU/Linux, os usuários têm por padrão acesso restrito ao modo gráfico e com perfil limitado, sem autorização para instalar ou executar tarefas administrativas, o que aumenta ainda mais o nível de segurança, além de ser considerado um sistema difícil de ser infectado por códigos maliciosos.

Questionamos também se os sistemas operacionais e os programas instalados eram atualizados com frequência. Como pode ser observado na Figura 20, 85,7% dos entrevistados disseram que sim, porém, como visto anteriormente na Figura 19, apenas 28,6% utilizam a versão mais recente do sistema.

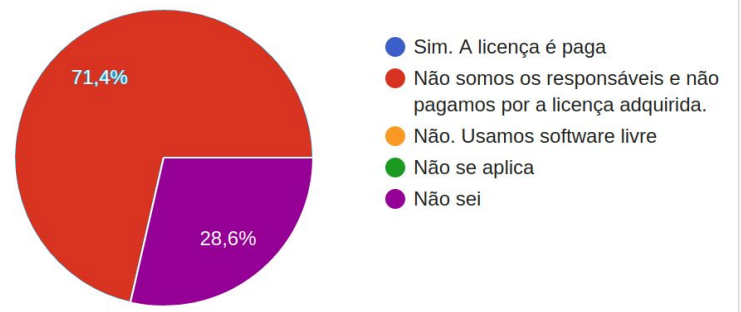
Além de ser importante manter os programas instalados sempre atualizados e com as versões mais recentes, isso deve ser uma prática constante para a segurança das informações, tendo em vista que nas novas versões ou atualizações foram corrigidas as possíveis falhas e vulnerabilidades identificadas.

Figura 20 - Atualizações dos sistemas e programas instalados.

Fonte: Elaborado pelos autores (2019).

Observou-se que as escolas utilizam um sistema que por padrão é proprietário, ou seja, é necessário adquirir a licença para usufruir das funcionalidades. Conforme a Figura 21, 71,4% dos entrevistados informaram que a escola não é responsável e não paga por a licença adquirida e 28,6% não souberam informar se o sistema é licenciado.

Figura 21 - Licenciamento dos sistemas e programas instalados.

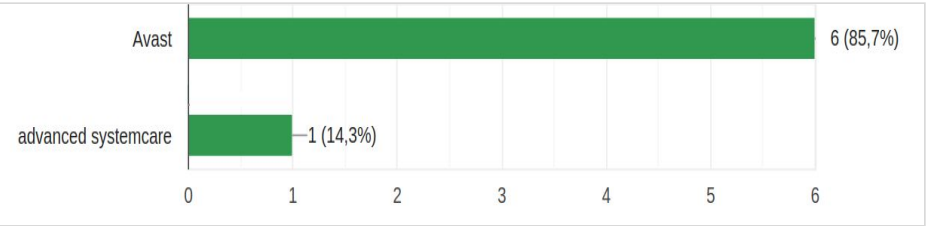


Fonte: Elaborado pelos autores (2019).

É importante que a organização saiba a procedência dos sistemas e programas instalados, bem como não permitir a instalação de programas não originais, visto que muitos códigos maliciosos se propagam por meio de softwares piratas, como também, muitos fabricantes não permitem a realização de atualizações quando detectam versões não licenciada.

Outro ponto a ser destacado é o uso do antivírus. Como pode ser observado na Figura 22, todas as escolas fazem uso de antivírus, observa-se que 85,7% delas utilizam o mesmo antivírus (Avast) e apenas 14,3% utiliza outro software de proteção. Todas elas, além de utilizarem a versão gratuita do programa, também faz uso apenas do firewall que vem instalado nos próprios no roteadores e sistemas operacionais instalados nos computadores.

Figura 22 - Uso de antivírus.



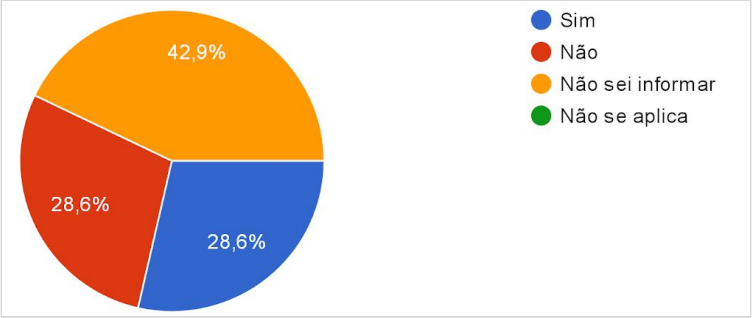
Fonte: Elaborado pelos autores (2019).

As versões gratuitas disponibilizadas pelos antivírus oferecem um nível de proteção com menos recursos que muito vezes é considerado baixo, porém orienta-se que para escolher

um antivírus que melhor se adapte a necessidade de cada ambiente é importante levar em conta o uso que se faz dos recursos e as características de cada versão disponibilizada.

Observa-se na Figura 23 que 28,6% dos entrevistados disseram que os computadores da escola já foram infectados por algum tipo de código malicioso e, uma mesma porcentagem informaram que nunca foram. Porém, observa-se que 42,9% dos entrevistados não souberam informar se já foi identificado esse tipo de problema com os computadores da escola.

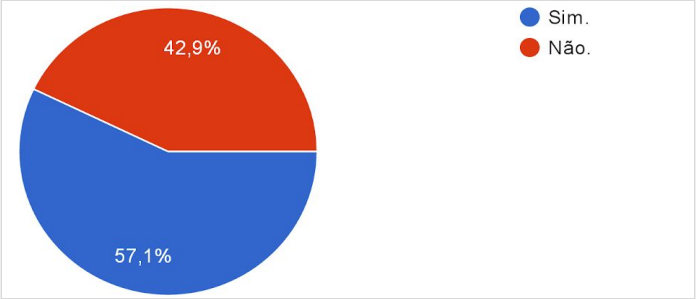
Figura 23 - Computadores já foram infectados por códigos maliciosos.



Fonte: Elaborado pelos autores (2019).

Esse é um fato que deve ser analisado, visto que 42,6% (Figura 24) também disseram não saber identificar se um computador estaria infectado por algum *Malware*, além disso, todos os entrevistados informaram que os funcionários não recebem orientação sobre o que é e como funciona um software malicioso, porém, consideram importante uma capacitação para docentes, funcionários e alunos sobre o tema segurança da informação.

Figura 24 - Saberia identificar um computador infectado.



Fonte: Elaborado pelos autores (2019).

Algo que também não condiz com as boas práticas de segurança e que pode colocar em risco as informações armazenadas nos recursos tecnológicos é observado em 85,7% das instituições pesquisadas (Figura 25). É permitido que docentes, funcionários e alunos insiram

mídias como por exemplo, *pen drives*, entre outras, nos computadores principais onde os dados e informações são manipuladas e armazenadas.

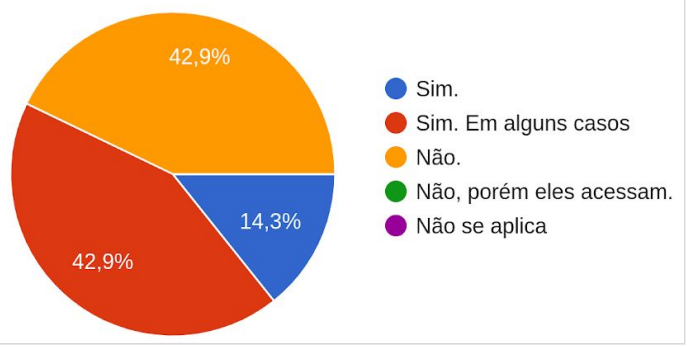
Figura 25 - Permite inserir mídias pessoais nos computadores.

Fonte: Elaborado pelos autores (2019).

Mídias podem ser infectadas por códigos maliciosos e, quando infectadas, servem como meio de propagação para essas pragas virtuais. Desse modo, não é seguro permitir que mídias, que não as da própria escola, sejam inseridas nos computadores nos quais são usados principalmente para manipular e armazenar as informações da escola, pois, por mais que os computadores tenham antivírus instalado, esse pode acabar não identificando as ameaças escondida nessas mídias, principalmente se a versão instalada do software é limitada.

Observa-se, Figura 26, que 42,9% das escolas permitem em alguns casos o uso dos computadores para fins pessoais. Permitir o uso de computadores da escola para fins pessoais, como acessar e-mails, redes sociais, páginas desconhecidas e que não oferecem segurança, permitir a instalação de programas, downloads de músicas, vídeos, jogos e arquivos de fontes desconhecidas também podem prejudicar a segurança das informações.

Figura 26 - Permite o uso dos computadores para fins pessoais.



Fonte: Elaborado pelos autores (2019).

É importante que as escolas definam regras específicas e orientem seus funcionários quanto ao uso dos computadores e acesso à Internet, posto que várias ameaças provêm desse ambiente. E-mails pessoais são carregados mensagens indesejadas (*spam*) carregadas de códigos maliciosos que se escondem principalmente em arquivos de texto, além de golpes com intuito de extrair informações sigilosos. Outras sérias de ameaças podem vir acompanhadas de programas, músicas, jogos, vídeos e arquivos baixados na Internet de fontes principalmente desconhecidas e ilegais.

Para evitar que os funcionários acessem esses tipos de conteúdos, as escolas podem adotar alguns mecanismos de segurança, como por exemplo, fazer a filtragem dos conteúdos, definindo o que pode ou não ser acessado. Isso pode ser configurado através do firewall, porém é necessário ter alguém ou uma equipe técnica responsável para fazer as devidas configurações nos computadores da escola.

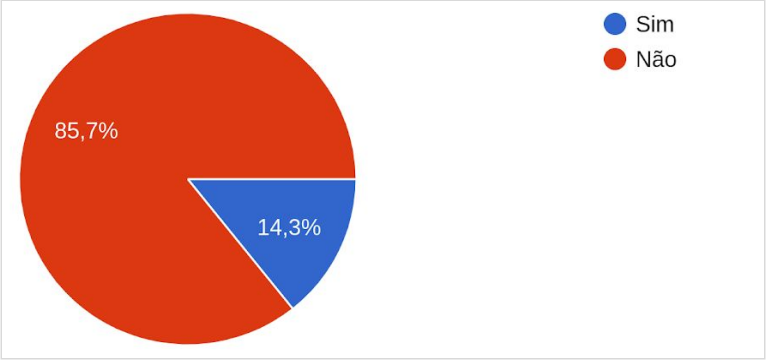
Como pode ser observado na Figura 27, as escolas além de não possuírem uma área de TI, 71,4% dessas disseram não receber o suporte necessário e constante da equipe disponibilizada pela Secretaria de Educação do município ou pessoa responsável pela área.

Figura 27 - Escolas possuem uma área de TI ou que recebem suporte.

Fonte: Elaborado pelos autores (2019).

Além dos fatos mencionados, outros fatores também são ameaçadores para a segurança das informações das escolas, como por exemplo, não realizar campanhas ou treinamentos para conscientizar os funcionários das consequências e riscos que o uso inadequado dos recursos de informática podem trazer, fato observado em 85,7% das escolas (Figura 28).

Figura 28 - Campanhas para uso adequado dos recursos de informática.

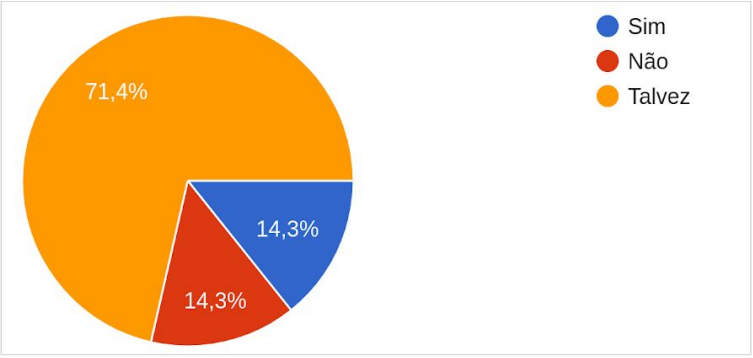


Fonte: Elaborado pelos autores (2019).

A conscientização dos funcionários de extrema importância para a segurança das informações institucionais. Essa lacuna pode ser suprida adotando como mecanismo o treinamento voltado para a capacitação constante dos funcionários sobre o assunto.

Com vistas a obter as opiniões dos entrevistado depois de realizadas todas as outras perguntas, questionamos se eles consideravam que as informações da escola estavam seguras, conforme representa a Figura 29, 71,4% responderam que talvez.

Figura 29 - Considera que as informações estão seguras.



Fonte: Elaborado pelos autores (2019).

Em fase a esse resultado obtido, percebe-se que os entrevistados demonstram insegurança quanto à segurança das informações. É preciso entender que a segurança nunca é 100%, porém é necessário que as informações tenham um nível adequado de segurança, adotando as medidas e mecanismos de segurança que visem assegurar esse nível.

4 CONSIDERAÇÕES FINAIS

Os resultados finais obtidos neste estudo mostraram que os ambientes educacionais estudados possuem vulnerabilidades que podem ser exploradas por diferentes ameaças e trazer sérios riscos e incidentes para suas informações, além disso, eles dispõem de poucos mecanismos de proteção e apoio técnico. Desse modo, os procedimentos, mecanismos, comportamentos e as atitudes adotadas para proteger as informações nos ambientes escolares pesquisados ainda não estão de acordo com as práticas recomendados para garantir um nível adequado de segurança.

Em resumo, consideramos que as principais incidências ameaçadoras para a segurança das informações nas escolas pesquisadas foram:

- Falta de uma Política de Segurança da Informação;
- Falta de um servidor de arquivos para organizar, manipular e armazenar os dados em um lugar principal;
- Computadores sem autenticação ou com autenticação única para todos os funcionários do setor;
- Perda de dados e informações manuais e digitais;
- Funcionários não fazerem uso de bloqueio de tela no computador quando se ausentam;
- Não alterar as senhas de autenticação nos computadores e contas de e-mails frequentemente;
- Armazenar as cópias de segurança nos computadores;
- Ataques à rede;
- Não atualizar os sistemas operacionais para as versões mais recentes;
- Não saber qual a procedência dos sistemas e programas instalados, se são licenciados;
- Utilizar apenas as versões gratuitas e limitadas dos antivírus;
- Já ter sido ou não saber se os computadores foram contaminados por códigos maliciosos, como também, não saber identificar a ocorrência deste incidente;
- Permitir que mídias, como pen drives pessoais, sejam inseridas nos computadores;
- Permitir o uso dos computadores e da Internet para fins pessoais;
- Não realizar campanhas de conscientização para o uso adequado dos recursos de informática.

Considerando que os aspectos mencionados podem deixar os ambientes estudados vulneráveis e propícios à ameaças, é importante que as escolas adotem medidas e mecanismos que visem contribuir para a segurança de suas informações, como as elencadas na Seção 2.3.

Dentre os mecanismos, ressaltamos a importância das escolas estabelecerem políticas de segurança, nas quais podem definir regras específicas para utilização dos computadores, Internet e e-mails. Além disso, sugerimos que seja realizado constantemente treinamentos voltado para a capacitação dos funcionários sobre o assunto. A falta desse mecanismo também deixa vulnerável as informações que estão sendo produzidas, manipuladas e armazenadas nestas instituições, tendo em vista os próprios funcionários serão fontes de ameaças para as informações se não estiverem bem treinados e conscientizados para identificar, evitar ou mesmo combater as principais ameaças que podem afetar o bem mais precioso de qualquer instituição, ou seja, as informações.

Diante deste estudo, é válido presumir que a situação atual das escolas no quesito segurança da informação e os problemas enfrentados retratam uma realidade muito presente em vários setores (públicos e privados) da sociedade e que, na falta de um departamento que gerencie a segurança da informação, os ativos de informação ficam à mercê de ameaças cada vez mais frequentes.

4.1 Dificuldades

A realização deste trabalho teve, naturalmente, algumas limitações. Dentre as dificuldades, encontramos diretores com receio de passar determinadas informações por medo expor a instituição. Desse modo, asseguramos que tanto os nomes deles quanto os das escolas não seriam divulgados. Também tiveram diretores que não souberam responder algumas perguntas. Para solucionar esse impasse, permitimos que eles fossem auxiliados por outros funcionários responsáveis que pudessem nos fornecer as informações necessárias.

4.2 Trabalhos Futuros

Em termos de investigações futuras, pensamos que seria interessante expandir a pesquisa para as demais escolas localizadas em áreas não urbanas do município para que, em

face e comparação dos resultados obtidos, possamos destacar ainda mais a importância do tema e a implementação das medidas que visem assegurar um nível de proteção maior para as informações geradas nesses ambientes. Pretendemos voltar as escolas pesquisadas com propostas de treinamentos e palestras educativas que visem conscientizar os funcionários e colaboradores da importância da segurança da informação, propondo melhorias e mecanismos, ou mesmo, elaborar uma política de segurança da informação em uma das escolas. Iremos também disponibilizar os resultados da pesquisa para o setor responsável na Secretaria de Educação do município. Com isso, esperamos que outros projetos possam ser desenvolvidos por parte da administração municipal.

4.3 Conclusão

A informação é imprescindível dentro das organizações. Essas produzem diariamente grandes quantidades de dados e informações com o auxílio da tecnologia, tarefas essas que antes eram realizadas manualmente. Devido essa evolução tecnológica, os ambientes organizacionais, além de ficarem dependentes da tecnologia, precisam proteger diariamente suas informações, visto que além delas se tornaram seu principal ativo, passaram a ser alvos de ameaças físicas, tecnológicas e humanas.

Neste contexto, o presente trabalho investigou inicialmente a realidade situacional das escolas municipais localizadas na área urbana de Girau do Ponciano- AL com relação a segurança de suas informações, observando se as práticas e procedimentos adotados nos ambientes estudados resguardavam adequadamente suas informações e qual era o conhecimento dos colaboradores sobre o assunto.

Primeiramente foi necessário realizar um estudo sobre os conceitos relacionados a segurança da informação, no qual foi possível descrever os principais incidentes, vulnerabilidades, ameaças, ataques e riscos que afetam os ativos informacionais das organizações e apresentar as principais medidas e mecanismos para o controle da segurança. Também foi possível compreender a importância de se estabelecer uma política de segurança da informação nos ambientes organizacionais. No decorrer do trabalho foi necessário aplicar um questionário junto aos diretores das escolas com intuito de levantar os dados necessários para dar suporte às análises dos resultados. Neste levantamento ficou visível que os

colaboradores das escolas, apesar de terem conhecimento sobre o assunto, demonstram uma certa insegurança.

Os objetivos foram traçados e alcançados no decorrer do seu desenvolvimento. Assim, fundamentando-se pela pesquisa bibliográfica e analisados os resultados obtidos neste estudo, conclui-se que o cenário atual das escolas em relação a segurança da informação ainda é crítico, porém com a adoção de alguns mecanismos de segurança já citados (Seção 2.3), assim como, a implantação de políticas de segurança da informação e a realização de capacitações para conscientizar os funcionários podem minimizar as falhas na segurança e preservar as informações contra futuras eventualidades.

O estudo também nos permitiu compreender a importância dada às informações e as tecnologias existentes nos ambientes organizacionais de modo geral e precisamente nos ambientes estudados através da identificação das prática e dos procedimentos adotados, assim como, do entendimento dos gargalos identificados e dos mecanismos que podem ser implementados para diminuir os problemas encontrados. Desse modo, destacamos que a proteção dos ativos informacionais é responsabilidade de todos e uma necessidade constante para garantir a segurança das informações e das tecnologias não só das escolas estudadas, mas de qualquer organização.

Por fim, além de servir para compreender a importância de se estabelecer uma política de segurança da informação eficaz, observou-se que alguns locais não há a estrutura necessária para manter a segurança dos dados, assim, é sugerido que seja realizada a contratação de pessoal com o conhecimento técnico comprovado para que possa elaborar uma metodologia de segurança e principalmente resolver os obstáculos que envolvem a informática na instituição. As dicas de segurança citadas se encaixam de maneira pertinente em relação às pessoas que acessam a Internet e aos cuidados básicos e essenciais na usabilidade cotidiana do computador e na utilização de seus recursos.

REFERÊNCIAS

ALBUQUERQUE JÚNIOR, A. E.; SANTOS, E. M. Adoção de medidas de segurança da informação: um modelo de análise para institutos de pesquisa públicos. **Revista Brasileira de Administração Científica,** Aquidabã, v.5, n.2, p.46-59, 2014. Disponível em: https://repositorio.ufba.br/ri/bitstream/ri/25123/1/document.pdf. Acesso em: 23 mar. 2019.

ALVES, C. B. **Segurança da informação vs. Engenharia Social:** Como se proteger para não ser mais uma vítima. Brasília, 2010. Disponível em:https://adm-portal.appspot.com.storage.googleapis.com/_assets/modules/academicos/academico_3641.pdf. Acesso em: 2 maio 2019.

AMORIM, M. R. L.; TELES, B. A. W. Superando Dificuldades na Implantação dos Sistemas de Informação nas Organizações. **Revista Foco**, [*S.l.*], v. 6, n. 1, p. 31-45, nov. 2013. ISSN 1981-223X. Disponível em: http://revistafocoadm.org/index.php/foco/article/view/52/47. Acesso em: 13 mar. 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBR ISO/IEC 27000. **Tecnologia da informação** - Técnicas de segurança - Sistemas de gestão da segurança da informação - Visão geral e vocabulário. Rio de Janeiro, 2014.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBR ISO/IEC 27001. **Sistemas de gestão da segurança da informação** - Requisitos. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBR ISO/IEC 27002. **Tecnologia da Informação** – Técnicas de segurança – Código de prática para a gestão da Segurança da Informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBR ISO/IEC 27002**.** **Tecnologia da Informação** – Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBR ISO/IEC 27005. **Tecnologia da Informação** – Técnicas de Segurança – Gestão de riscos de segurança de informação. Rio de Janeiro, 2011.

BAARS, H. et al. **Fundamentos de Segurança da Informação:** com base na ISO 27001 e na ISO 27002. Rio de Janeiro; Editora Brasport, 2018.

BALDISSERA, T. A.; NUNES, R. C. Impacto na Implementação da Norma NBR ISO/IEC 17799 para a Gestão da Segurança da Informação em Colégios: um estudo de caso. *In*: ENCONTRO NACIONAL DE ENGENHARIA DA PRODUÇÃO, 27., 2006, Foz do Iguaçu. **Anais** [...]. Foz do Iguaçu: Associação Brasileira de Engenharia da Produção, 2007. Disponível em: http://www.abepro.org.br/biblioteca/enegep2007_tr640475_9300.pdf. Acesso em: 2 maio 2019.

BATISTA, E. O. **Sistema de Informação:** o uso consciente da tecnologia para o gerenciamento. 2. ed. São Paulo. Saraiva, 2004. Disponível em: https://pt.scribd.com/document/342525179/Sistemas-de-Informacao-o-Uso-Consciente-da-Tecnologia-Para-o-Gerenciamento-2%C2%AA-Ed-2012-pdf. Acesso em: 19 abr. 2019.

CARDOSO, D. B. **Política De Segurança Da Informação Para O Departamento De Segurança Da Faculdade Do Conhecimento,** 2013. 87f. TCC (Graduação em Tecnólogo em Segurança da Informação) - Faculdades Integradas Promove de Brasília, Brasília, 2013. Dispoível em: http://nippromove.hospedagemdesites.ws/anais_simposio/arquivos_up/documentos/artigos/aa7ca5af64a0241839da284feae87f2f.pdf. Acesso em: 14 abr. 2019.

CARVALHO, E. A.; REIS, T.; ALVES, F. J. Ensino de Noções Básicas de Segurança da Informação nas Escolas Brasileiras. **Anais do Workshop de Informática na Escola,** [*S.l.*], p. 765, out. 2017. ISSN 2316-6541. Disponível em: https://www.br-ie.org/pub/index.php/wie/article/view/7295. Acesso em: 26 mar. 2019.

CERT.br. (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). **Estatísticas dos Incidentes Reportados ao CERT.br.** 2019. Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 19 mar. 2019.

CERT.br.(Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). **Incidentes Reportados ao CERT.br. Janeiro a Dezembro 2018**. 2019. Disponível em: https://www.cert.br/stats/incidentes/2018-jan-dec/tipos-ataque.html. Acesso em: 19 mar. 2019.

CERT.br. (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). **Cartilha de Segurança para Internet.** 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 2 maio 2019.

CERT.br. (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). **Cartilha de Segurança para Internet. Fascículo Backup.** 2017. Disponível em: https://cartilha.cert.br/fasciculos/backup/fasciculo-backup.pdf. Acesso em: 2 maio 2019.

CGI.br/NIC.br. **Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nas Escolas Brasileiras**.2018. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/tic_edu_2017_livro_eletronico.pdf. Acesso em: 19 mar. 2019.

DANTAS, M.L. **Segurança da Informação:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

DEITOS, M. L. M. S. **A Gestão da Tecnologia em Pequenas e Médias Empresas:** fatores limitantes e formas de superação. Cascavél: Edunioeste, 2002. Disponível em: www.unioeste.br/editora/pdf/livro_gestao_tecnologia_maria_lucia_deitos_protegido.pdf. Acesso em: 15 abr. 2019.

DHILLON, G. Violation of Safeguards by Trusted Personnel and Understanding Related

Information Security Concerns. **Computers & Security**, v. 2, p. 65-172. 2001. Disponível em: https://doi.org/10.1016/S0167-4048(01)00209-7. Acesso em: 12 abr. 2019.

FONTES, E. **Segurança da Informação:** O usuário faz a diferença. São Paulo: Saraiva, 2006.

FURNELL, S.; THOMSON, K.-L.From Culture to disobedience: recognising the varying user acceptance of IT security. **Computer Fraud & Security,** v. 2, p. 5-10, 2009. Disponível em: https://www.sciencedirect.com/science/article/pii/S1361372309700193. Acesso em: 13 fev. 2019.

GUIMARÃES, R. Modelo de governança de segurança da informação para a Administração Pública Federal. 2018. **Perspectivas em Gestão & Conhecimento,** João Pessoa, v. 8, n. 3, p. 90-109, set./dez. 2018. Disponivel em: http://www.periodicos.ufpb.br/ojs2/index.php/pgc/article/view/34717/21768. Acesso em: 2 abr. 2019.

KNAPP, K. J.; MORRIS, R. F.; MARSHALL, T. E.; BYRD, T. A.Information security policy: An organizational-level process model. **Computers & Security**, v. 28, n. 7, p. 493-508, 2009. Disponível em: https://www.researchgate.net/publication/222706081_Information_security_policy_An_organizational-level_process_model. Acesso em: 13 fev. 2019.

KONZEN, M. P. **Gestão de Riscos de Segurança da Informação Baseada na Norma NBR ISO/IEC 27005 Usando Padrões de Segurança**. 2013. Disponível em: https://www.researchgate.net/publication/222706081_Information_security_policy_An_organizational-level_process_model. Acesso em: 13 fev. 2019.

KRUGER, H. A.; KEARNEY, W. D.Consensus Ranking - An ICT security awareness case study. **Computers & Security.** v. 27, n. 7, p. 493-508, 2008. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404808000448. Acesso em: 13 fev. 2019.

Kurose, J. F. **Redes de Computadores e a Internet**: uma abordagem top-down. 5. ed. São Paulo: Pearson, 2010.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de Informações Gerenciais**. Editora: Pearson Prentice Hall. 9. ed.. São Paulo, 2010.

LAUREANO, M. A. P. **Gestão de Segurança da Informação**, 2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. Acesso em: 19 ago. 2019.

LENNERT, L. S.; OLIVEIRA, M. A. O que é engenharia social?. **Gestão de Riscos**, São Paulo, ed. 64, mar. 2011. Disponível em: https://docs.wixstatic.com/ugd/fbc826_264fa5ab81504c55964ccf9618934d8a.pdf. Acesso em: 3 maio 2019.

LUNARDI, G. L. & DOLCI, P. C. Adoção de Tecnologia da Informação e seu Impacto no Desempenho Organizacional: um estudo realizado com micro e pequenas empresas. *In*: ENCONTRO DA ANPAD, 30., 2006. Salvador. **Anais** [...]. Salvador: ENANPAD, 2006.

LYRA, M. R. **Governança da Segurança da Informação**. Edição do Autor – Brasília, 2015. Disponível em: http://mauriciolyra.pro.br/site/wpcontent/uploads/2016/02/Livro-Completo-v4-para-impress%C3%A3o-com-ISBN.pdf. Acesso em: 1 mar. 2019.

MAIOR, A. O. B.; SANTOS, F. A.; DAL LACQUA, S. C.**Gestão da segurança da Informação**. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação)-Faculdade Gennari & Peartree, Pedreiras, 2006. Disponível em: http://www.abepro.org.br/biblioteca/enegep2007_tr640475_9300.pdf.Acesso em:12 abr. 2019.

MARCIANO, J. L. P. **Segurança da Informação** - uma abordagem social. 2006. Tese (Doutorado em Ciência da Informação) - Universidade de Brasília, Brasília, 2006. Disponível em: http://www.enancib.ppgci.ufba.br/premio/UnB_Marciano.pdf. Acesso em: 29 mar. 2019.

MENDONÇA, M. G.. et al. Segurança em sistemas de informação: Um estudo comparativo sobre os programas de antivírus e sistemas de firewall. 2010. 4 f. **X Encontro latino Americano de Pós-Graduação**. Universidade de Taubaté – UNITAU, Programa de Pós-graduação em Gestão e Desenvolvimento Regional. Taubaté, 2010. Disponível em: http://www.inicepg.univap.br/cd/INIC_2010/anais/arquivos/0220_0496_01.pdf. Acesso em: 12 abr. 2019.

MITNICK, K. My First RSA Conference**. Security Focus**, April 30, 2001. Disponível em:https://www.securityfocus.com/news/199. Acesso em: 10 abr. 2019.

MITNICK, K.D.; SIMON, W. L. **A Arte de Enganar. Ataques de hackers:** Controlando o fator humano na Segurança da Informação. [S.l]: Pearson Education do Brasil Ltda, 2003.

MOREIRA, N. S. **Segurança mínima:** uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books., 2001

OLIVEIRA, A. M. R. de; NOGUEIRA, R. C. S.; LEMES, E. G. Segurança da informação nas empresas: enfocando a engenharia social**.** *In*: SEMINÁRIO DE PRODUÇÃO ACADÊMICA DA ANHANGUERA, 2011, Anhanguera. **Anais** […]. Anhanguera, 2011.

PIMENTA, A. M. S.; Quaresma, R.F.C. A segurança dos sistemas de informação e o comportamento dos usuários. **JISTEM J.Inf.Syst. Technol. Manag.**, São Paulo , v. 13, n. 3, p. 533-552, Dec. 2016 . Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752016000300533&lng=en&nrm=iso. Acesso em: 15 mar. 2019.

PONTES, M. V. F. **Política de Segurança da Informação:** uma contribuição para o Campus IV. Rio Tinto - PB, 2014.

POPPER, M. A.; BRIGNOLI, J. T. **Engenharia Social**: Um Perigo Eminente. 2002. 11 f. **Instituto Catarinense de Pós-Graduação** – ICPG. Blumenau, 2002. Disponível em: https://docplayer.com.br/3991308-Engenharia-social-um-perigo-eminente.html. Acesso em: 5 maio 2019.

PROMON, Business & Tecnology review. **Segurança da Informação** – Um diferencial determinante na competitividade das corporações. Rio de Janeiro, 2005. Disponível em: https://www.teleco.com.br/promon/pbtr/Seguranca_4WEB.pdf. Acesso em: 12 mar. 2019.

PWC.(PricewaterhouseCoopers). **The Global State of Information Security Survey 2018**. Disponível em: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html#insight2. Acesso em: 2 mar. 2019.

RHEE, H.-S., KIM, C., RYU, Y. U., (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. **Computers & Security**, v. 28, n. 8, p. 816-826. Disponível em: https://www.sciencedirect.com/science/article/pii/S016740480900056X. Acesso em: 15 fev. 2019.

SÊMOLA, M. **Gestão da Segurança da Informação, uma visão Executiva**. Rio de Janeiro: Elsevier, 2003.

SILVA, N. B. X.; Araújo W. J. de; Azevedo P. M. de. Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação.2013. **Revista Ibero-Americana de Ciência da Informação,** v. 6, n. 2, p. 37-55, 11. Disponível em: https://periodicos.unb.br/index.php/RICI/article/view/1782. Acesso em: 29 abr. 2019.

SONICWALL. **2018 Sonicwall Cyber Threat Report.** Disponível em: https://drive.google.com/file/d/1jYA_xoc5YKnfH4Y8do6bdCSlYcUMTEQe/view?usp=sharing. Acesso em: 16 dez. 2018.

SONICWALL. **Relatório de Ameaças Cibernéticas da Sonicwall 2019**. Disponível em: https://www.sonicwall.com/pt-br/lp/2019-cyber-threat-report-lp/. Acesso em: 2 maio 2019.

SPANCESKI, F. R. **Política de Segurança da Informação** - Desenvolvimento de um modelo de segurança da informação voltado para instituições de ensino. 2004. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) - Instituto Superior Tupy, Joinville, 2004. Disponível em: http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_francini_politicas.pdf. Acesso em: 13 jan. 2019.

STAIR, R. M; REYNOLDS, G. W. **Princípios de Sistemas de Informação.** Tradução da 9ª Edição Norte-Americana. São Paulo: Editora Cengage Learning, 2011.

SYMANTEC CORP. **Ransom.Wannacry 2017**. Disponível em:

https://www.symantec.com/security-center/writeup/2017-051310-3522-99#. Acesso em: 31 jul. 2019.
TANENBAUM, A. S. **Redes de Computadores.** 4. ed. Rio de Janeiro, Brasil: Ed. Campus, 2003.

ULLMANN, P. E. **Políticas de Segurança da Informação:** um estudo de caso baseado nas normas ABNT NRT ISO/IEC 27014: 2013 e ABNT NRT ISO/IEC 27005:2011. Santa Rosa, 2015. Diponível em: http://bibliodigital.unijui.edu.br:8080/xmlui/handle/123456789/318.Acesso em: 20 mar. 2019.

VIANNA, C. T. **Sistemas de Informação no Contexto da Inovação, dos Sistemas, da Informação e dos Processos Gerenciais**. Florianópolis: Publicações do Ifsc, 2015. Disponível em: https://www.ifsc.edu.br/documents/30701/523474/sistemas_Informa%C3%A7%C3%A3o_contexto_inovacao_producao_WEB.pdf/12c17647-b399-5426-3380-b40cd4709c93. Acesso em: 31 mar. 2019.

YAMAJI, E. K. **Tecnologia da informação:** políticas de segurança da informação. 2013. Disponível em: http://dspace.mackenzie.br/handle/10899/139. Acesso em: 22 maio 2019.

ZANELLA, Tatieli. **Estudo Sobre A Quebra De Confidencialidade Da Informação E Mecanismos De Segurança**. 2017. 79 f. TCC (Graduação em Sistemas de Informação) - Universidade de Caxias do Sul, Caxias do Sul, 2018. Disponível em: https://repositorio.ucs.br/xmlui/handle/11338/3807?show=full. Acesso em: 15 maio 2019.

APÊNDICE A - INSTRUMENTO DE COLETA DE DADOS

Este questionário será aplicado no início do estudo de caso com o objetivo de realizar o levantamento dos dados necessários para investigar a situação atual das escolas em relação a segurança da informação e analisar se estes ambientes estão protegendo adequadamente suas informações e qual o conhecimento dos colaboradores sobre o assunto.

1. A escola atende quais anos da educação básica? Marque as opções.

- ❑ Educação Infantil
- ❑ 1º ano
- ❑ 2º ano
- ❑ 3º ano
- ❑ 4º ano
- ❑ 5º ano
- ❑ 6º ano
- ❑ 7º ano
- ❑ 8º ano
- ❑ 9º ano
- ❑ Educação de Jovens e Adultos (EJA)

2. A escola funciona em quais horários?

- ❑ Manhã
- ❑ Tarde
- ❑ Noite
- ❑ Integral

3. Qual o total de alunos da escola? _____

4. Qual o total de funcionários da escola?

- ❑ < 10
- ❑ De 30 a 50
- ❑ De 50 a 100
- ❑ > 100
- ❑ Não sei

5. Qual área é produzida, manipulada e guardada as informações mais importantes da escola? _____

6. Quantos funcionários trabalham nessa área? _____

7. Como são produzidas e manipuladas as informações da escola?

- ❑ Somente Manual
- ❑ Somente Digital
- ❑ Manualmente e Digitalmente
- ❑ Outros _____

8. Onde são armazenadas as informações da escola?

- ❑ armários, arquivos (Aço, madeira)
- ❑ CDs e DVDs
- ❑ Pen drives
- ❑ Computadores
- ❑ Armazenamento em nuvem
- ❑ Em um servidor
- ❑ Outros _____

9. A escola possui um servidor de arquivos principal para compartilhar dados com outros computadores ligados à rede? _____

10. A escola faz uso de algum sistema de gerenciamento de banco de dados (Access,Oracle,MySQL)? Se sim, Qual? _____

11. Quando chega um novo funcionário lhe é passado as responsabilidades referente à segurança da informação utilizada na escola? _____

12. Quantos computadores a escola possui? (Incluindo notebooks e os computadores que não estão funcionando - se não tiver nenhum coloque 0)**. _____**

13. Todos os computadores estão em funcionamento?

- ❑ Sim. Todos.
- ❑ Apenas alguns.
- ❑ Não. Nenhum funciona.
- ❑ Não possui computadores.

14. Quantos exatamente funcionam? _____

15. A escola possui laboratório de informática? Está ativo?

- ❑ Sim. Está ativo.
- ❑ Não possui.
- ❑ Sim. Não Ativo.
- ❑ Outro _____

16. A escola tem um funcionário responsável pelo Laboratório? (**Não se aplica** se a escola não tiver laboratório). _____

17. Se tem laboratório, quem tem acesso aos computadores? (**Não se aplica** se a escola não tiver laboratório).

- ❑ Todos (Alunos, professores e demais funcionários).
- ❑ Apenas alguns funcionários (rede administrativa e direção).
- ❑ Apenas professores e demais funcionários.
- ❑ Não se aplica.

18. Os alunos têm aula prática de informática? Se sim, têm acesso à Internet? (Não se aplica se a escola não tiver laboratório).

- ❑ Sim. Com acesso à Internet.
- ❑ Não tem.
- ❑ Sim. Sem acesso à Internet.
- ❑ Não se aplica.

19. É abordado nas aulas práticas o uso seguro da Internet? (Não se aplica se a escola não tiver laboratório). _____

20. Há professores de informática na escola?_____

21. Há alguém responsável pelo controle de acesso aos recursos de informática?_____

22. A escola tem uma área de TI ou recebe suporte de uma equipe responsável pela área disponibilizada pela secretaria de educação do município?

- ❑ Sim. Tem uma área de TI.
- ❑ Não. Recebemos apenas o suporte da equipe disponibilizada.
- ❑ Não temos uma área de TI e não recebemos o suporte constante da equipe disponibilizada.

23. Como é dividida a estrutura de informática? Quantos computadores em cada rede? (Coloque 0 para as salas que não possuir computadores).

Rede administrativa (secretaria): _____ Sala dos Professores: _____

Rede de ensino (laboratório): _____ Sala da direção:_____

24. A escola possui Internet Banda Larga? _____

25. Se sim para pergunta anterior. A Internet é fornecida por algum programa do governo federal, prefeitura ou recursos próprios da escola?

- ❑ Sim. Fornecida pelo programa do governo.
- ❑ Sim. Fornecida pela prefeitura.
- ❑ Sim. Fornecida com recursos próprios da escola.
- ❑ Não tem.

26. Se tem Internet, é distribuída/compartilhada a conexão por rede Wi-Fi? _____

27. A rede Wi-Fi possui senha de segurança para ser acessada? _____

28. Quem tem acesso a rede Wi-i?

- ❑ Todos (Alunos, professores e demais funcionários).
- ❑ Apenas professores e demais funcionários.
- ❑ Apenas alguns funcionários (rede administrativa e direção escolar).
- ❑ Não se aplica.

29. Todos os computadores e dispositivos ficam conectados na mesma rede? _____

30. Já aconteceu da rede Wi-Fi ser invadida por alunos ou mesmo por outra pessoa e, devido isso, ter que ser reconfigurada novamente para restabelecer o acesso?

- ❑ Sim. Já aconteceu algumas vezes e tivemos que reconfigurar a rede para restabelecer o acesso.
- ❑ Não sei informar se isso já aconteceu, porém já tivemos que reconfigurar a rede para restabelecer o acesso.
- ❑ Não. Nunca tivemos a rede invadida.
- ❑ Não sei informar.
- ❑ Não se aplica.

31. É permitido que outros funcionários tenham acesso aos computadores principais onde e manipulada e armazenada a maior parte da informações da escola?

- ❑ Sim. Todos, sem autorização.
- ❑ Sim. Todos, com autorização.
- ❑ Sim. Apenas alguns e com autorização.
- ❑ Não. Só é permitido o acesso do responsável pelo setor.
- ❑ Não se aplica.

32. Para acessar os computadores da escola é necessário que seja feita uma autenticação (login) para utilizar o mesmo?

❑ Sim. Em todos. ❑ Sim. Em quase todos. ❑ Não.

33. Cada funcionário que manuseia as informações nos computadores possuem usuário e senha de acesso restrito?

- ❑ Sim. Cada funcionário tem sua autenticação.
- ❑ Não. Os computadores possuem autenticação única para todos os funcionários.
- ❑ Não. Os computadores não possuem autenticação.
- ❑ Não se aplica.

34. O funcionário quando se ausenta por algum momento do computador faz uso de bloqueio e proteção de tela? _____

35.Quando um funcionário deixa de trabalhar na escola, as senhas do local de trabalho, e-mails e outros utilizado por ele são trocadas? _____

36. A escola possui algum sistema de restrição de pessoas a determinadas informações?

- ❑ Sim. Não é permitido que algumas pessoas tenham acesso a algumas informações.
- ❑ Não. Todos podem ter acesso às informações quando solicitadas.

37. A escola possui restrição/controle de acesso físico em determinadas salas/departamentos?

❑ Sim. Em todos. ❑ Sim. Em quase todos. ❑ Não possui restrições de acesso.

38. Os funcionários obedecem às restrições?_____

39. Qual sistema operacional dos computadores da escola e qual a versão?

❑ Windows 7 ❑ Linux ❑ Não sei

❑ Windows 8 ❑ MacOS ❑ Outro _____

❑ Windows 10 ❑ Não se aplica

40. É pago a licença do Sistema Operacional e dos programas instalados? _____

41. O Sistema Operacional e programas dos computadores são atualizados com frequência?_____

42. Os computadores tem antivírus instalado? Se sim, qual?_____

43. É pago a licença dos antivírus? _____

44. Os computadores da escola já foram infectados por algum tipo de código malicioso? (vírus, cavalo de troia entre outros). _____

45. Você saberia identificar se um computador estaria infectado por algum código malicioso? _____

46. Os funcionários recebem orientações sobre o que é e como funciona um software malicioso? _____

47. É feito cópias de segurança dos dados com regularidade? _____

48. Se é feito cópias de segurança, onde são guardadas?_____

49. Sabe informar se os professores abordam conteúdos sobre uso seguro da Internet com os alunos? _____

50. Considera importante uma capacitação para docentes, funcionários e alunos sobre o tema segurança da informação? _____

51. É permitido que docentes,funcionários e alunos insiram mídias (Pen Drives, celulares, etc), mesmo para fins didáticos, nos computadores da escola?_____

52. É permitido o uso de computadores da escola para fins pessoais? (exemplo: acessar/enviar e-mais pessoais, acessar páginas desconhecidas, youtube, redes sociais, etc..). _____

53. Vocês realizam alguma campanha para conscientização do uso adequado dos recursos de informática? _____

54. Qual firewall a escola utiliza? _____

55. É permitido que docentes, funcionários ou alunos instalar programas ou baixar conteúdos (músicas, filmes, jogos)? _____

56. Os funcionários costumam deixar papéis com informações importantes sobre a mesa?_____

57. A escola já procurou algum dado ou informação importante e não encontrou?

❑ Sim.Informações manuais. ❑ Sim. Informações digitais. ❑ Não.

❑ Sim. Informações manuais e digitais. ❑ Prefiro não informar. ❑ Não sei informar.

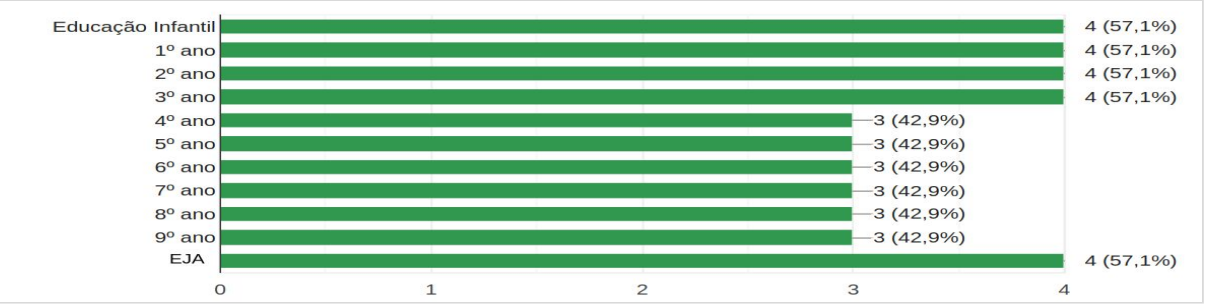
58. A escola possui uma política de segurança da informação? _____

59. Você sabe o que é segurança da informação? Se sim, pode nos explicar se ela é aplicada na escola e como. _____

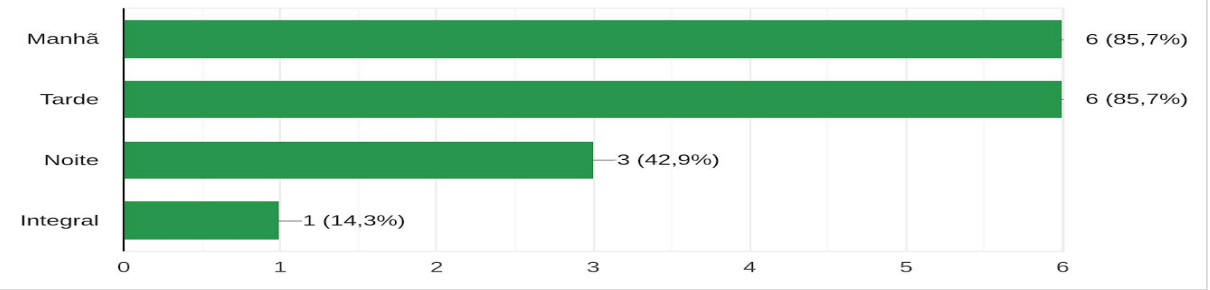
60. Considera que as informações da escola estão seguras? _____

APÊNDICE B - RESULTADO COMPLETO DA COLETA DE DADOS

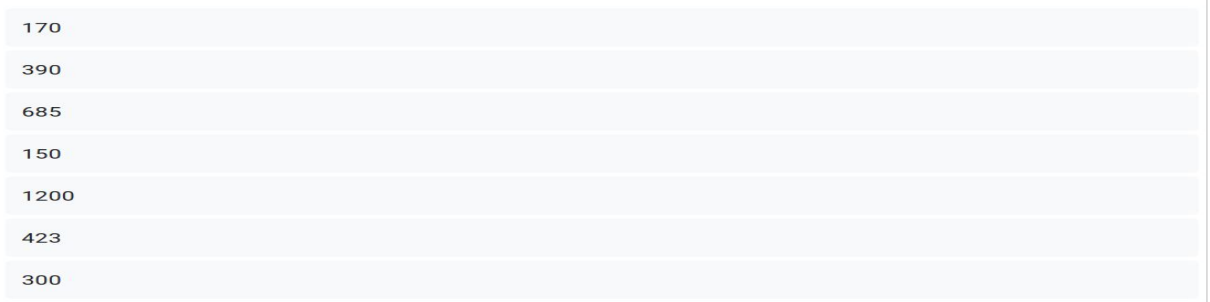
1.A escola atende quais anos da educação básica? Marque as opções.



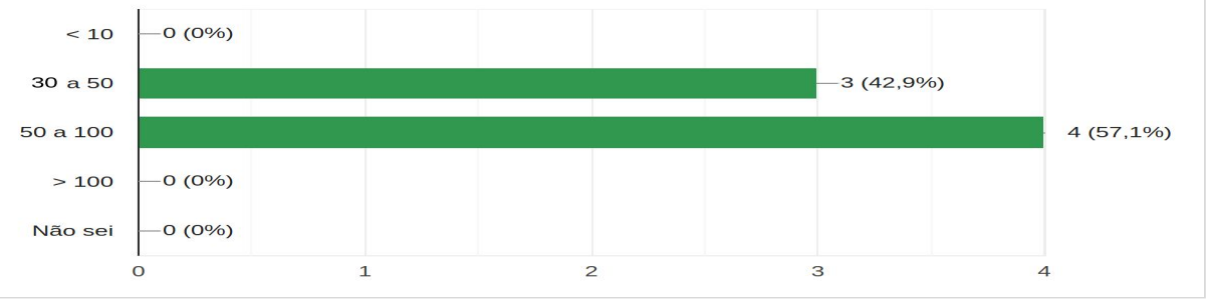
2.A escola funciona em quais horários?



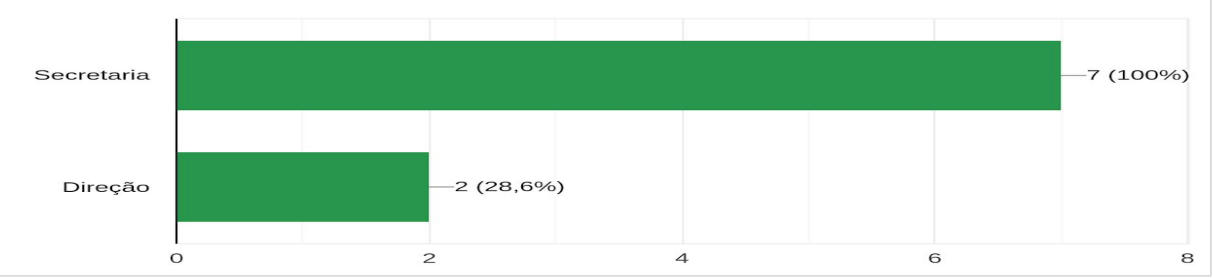
3.Qual o total de alunos da escola?



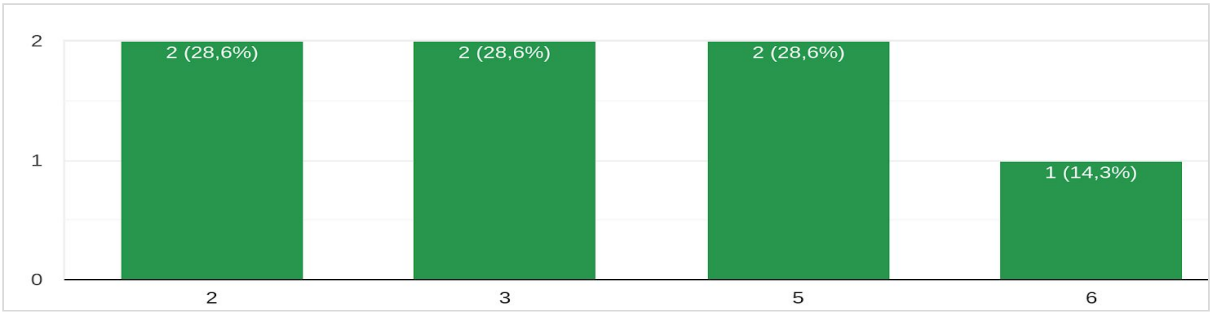
4.Qual o total de funcionários da escola?



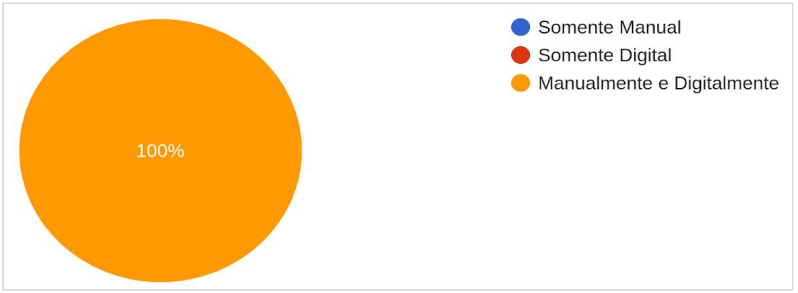
5.Qual área é produzida, manipulada e guardada as informações mais importantes da escola?



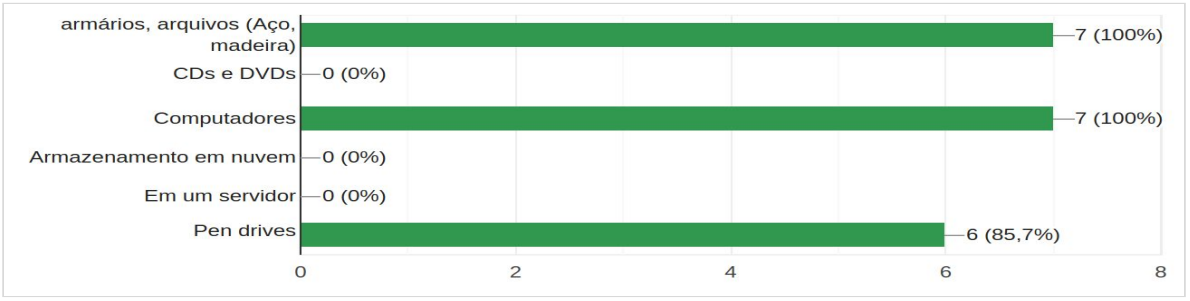
6.Quantos funcionários trabalham nessa área?



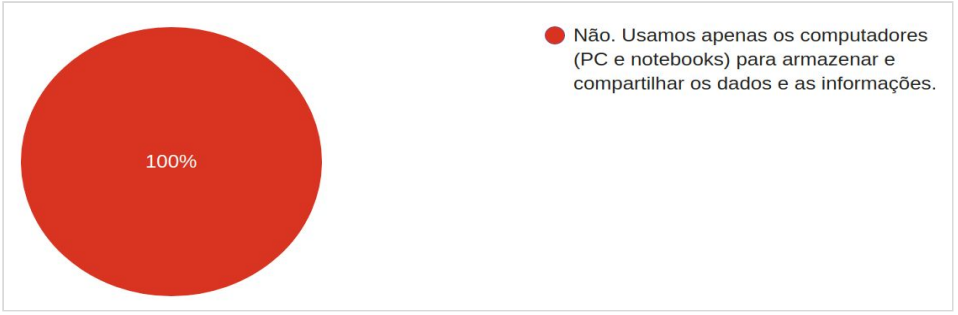
7.Como são produzidas e manipuladas as informações da escola?



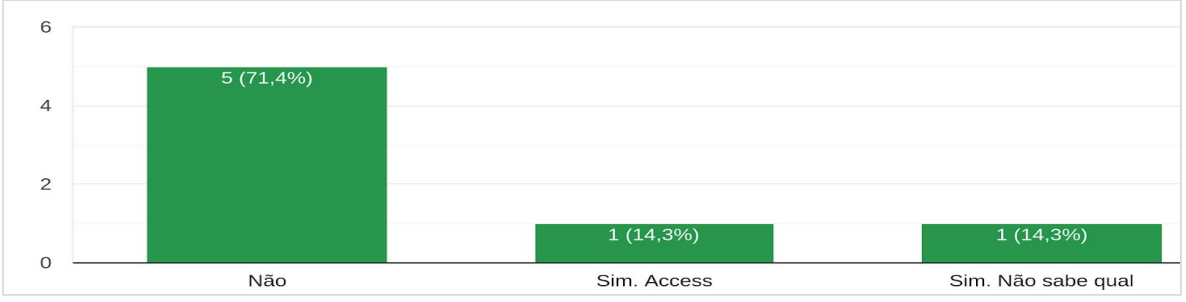
8.Onde são armazenadas as informações da escola?



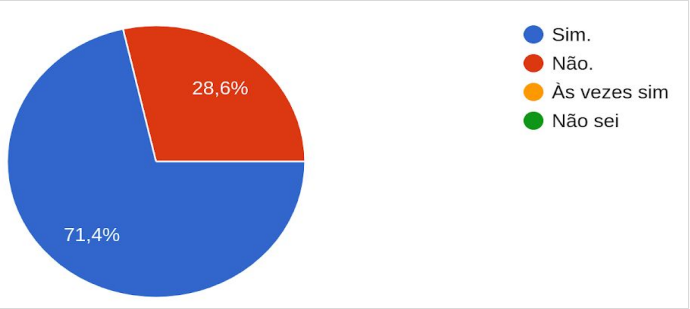
9.A escola possui um servidor de arquivos principal para compartilhar dados com outros computadores ligados à rede?



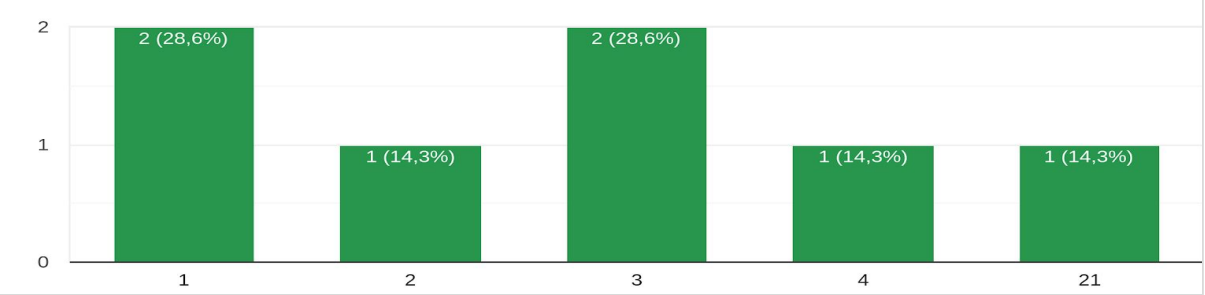
10.A escola faz uso de algum Sistema de Gerenciamento de Banco de Dados (Access,Oracle,MySQL)? Se sim, Qual?



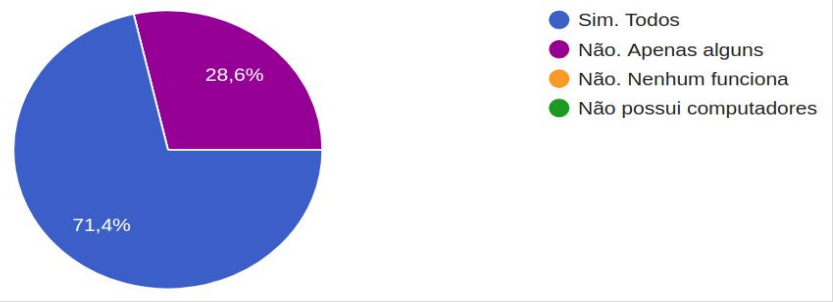
11. Quando chega um novo funcionário lhe é passado as responsabilidades referente à segurança da informação utilizada na escola?



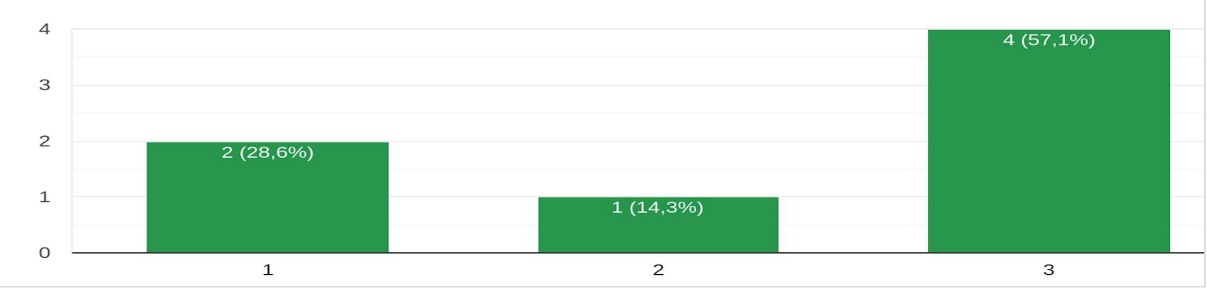
12. Quantos computadores a escola possui? (Incluindo notebooks e os computadores que não estão funcionando - se não tiver nenhum coloque 0).



13. Todos os computadores estão em funcionamento?

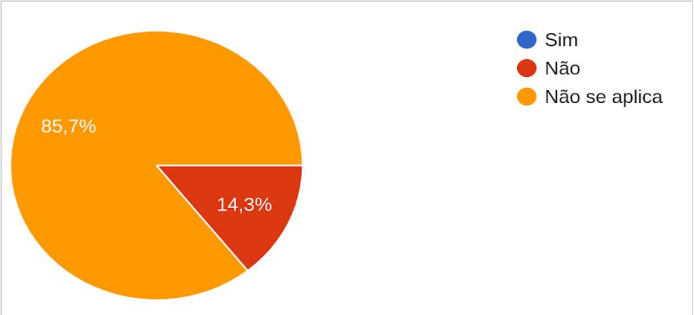


14. Quantos exatamente funcionam? (Quantidade exata de computadores que funciona e que são utilizados).

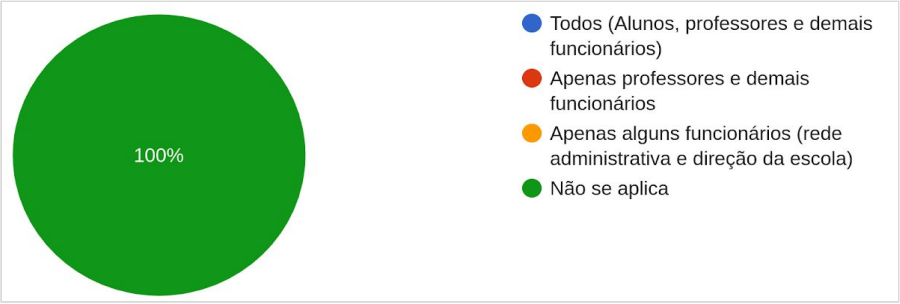


15. A escola possui laboratório de informática? Está ativo?

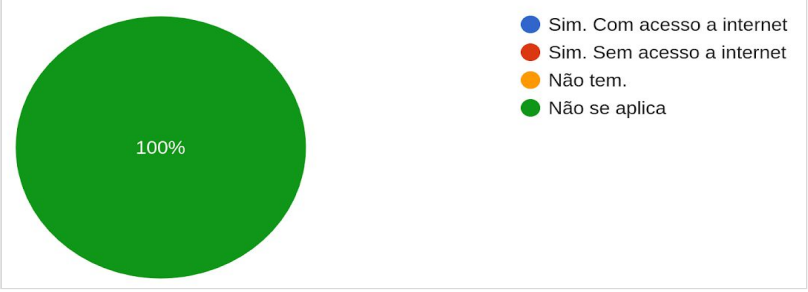
16. A escola tem um funcionário responsável pelo Laboratório? (Não se aplica se a escola não tiver laboratório).



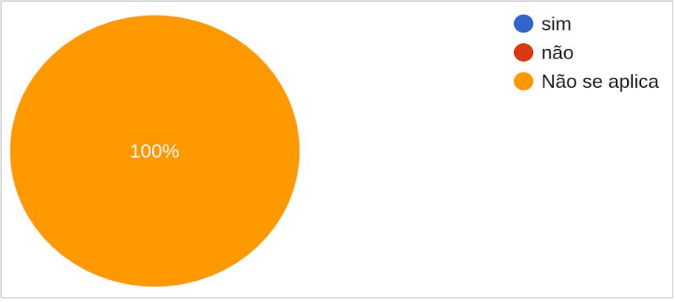
17. Se tem laboratório, quem tem acesso aos computadores? (Não se aplica se a escola não tiver laboratório).



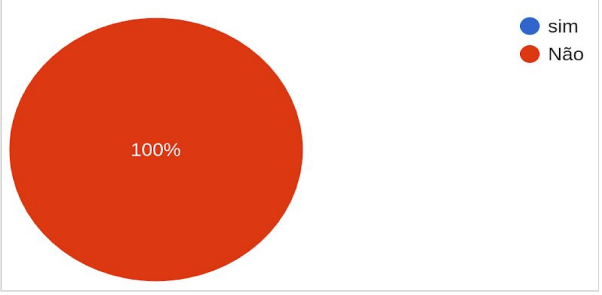
18. Os alunos têm aula prática de informática? Se sim, têm acesso à Internet? (Não se aplica se a escola não tiver laboratório).



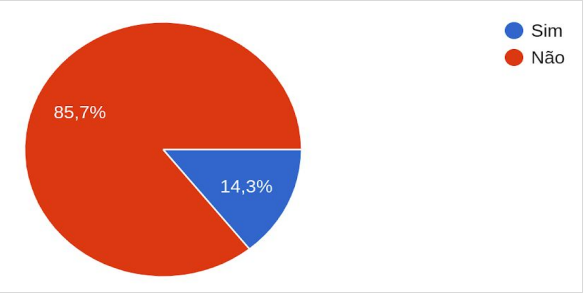
19. É abordado nas aulas práticas o uso seguro da Internet? (Não se aplica se a escola não tiver laboratório).



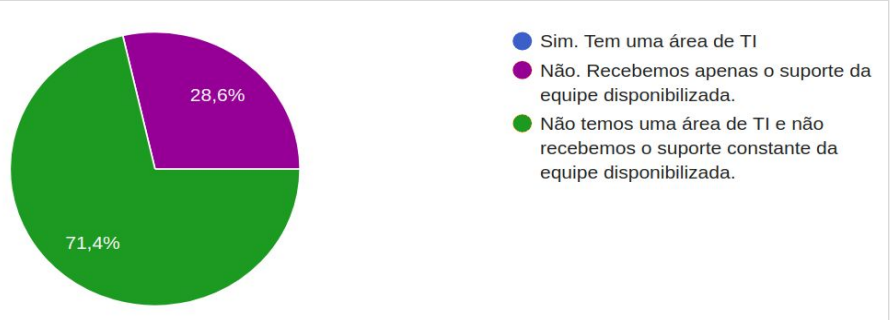
20. Há professores de informática na escola? (Não se aplica se a escola não tiver laboratório).



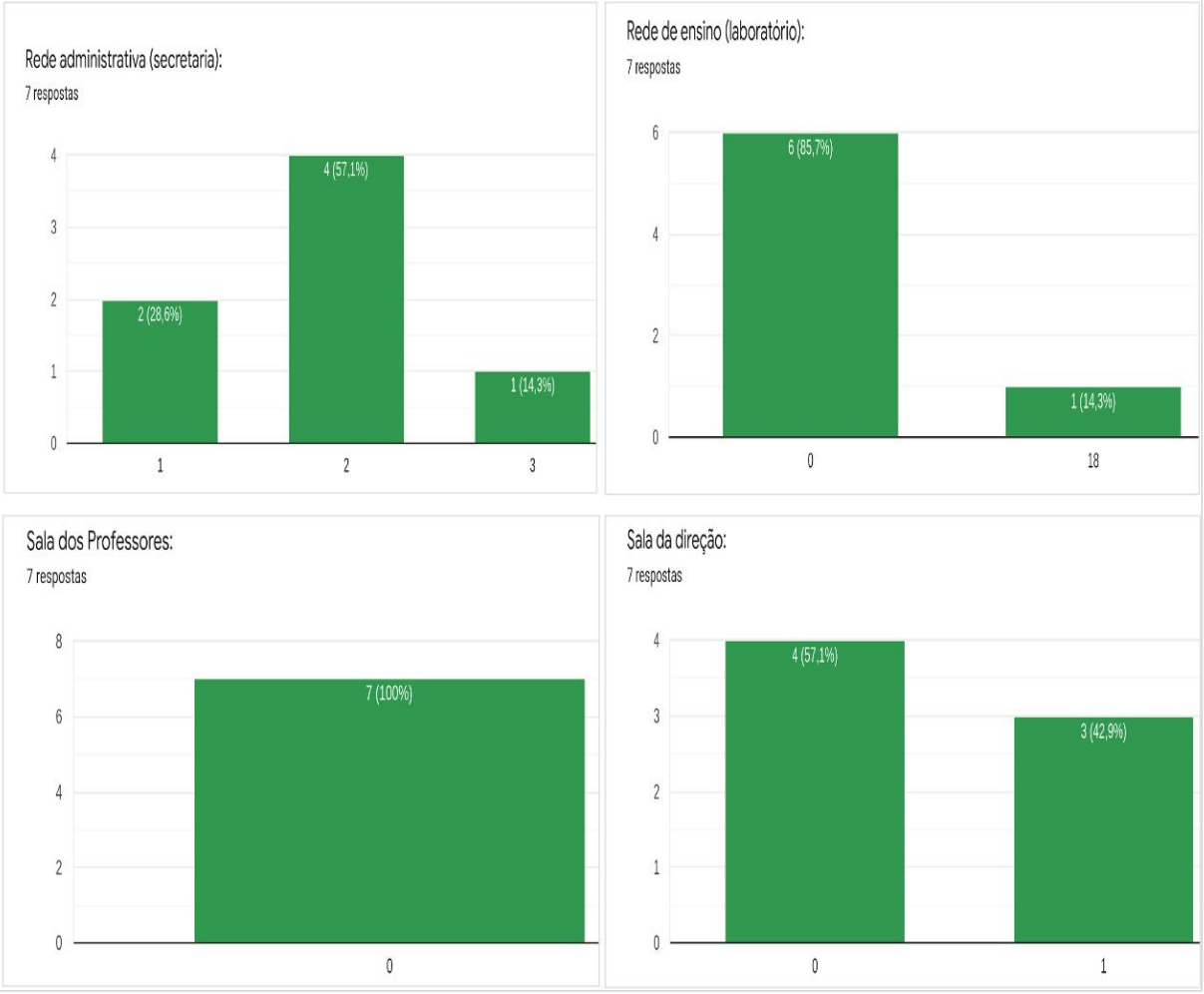
21. Há alguém responsável pelo controle de acesso aos recursos de informática?



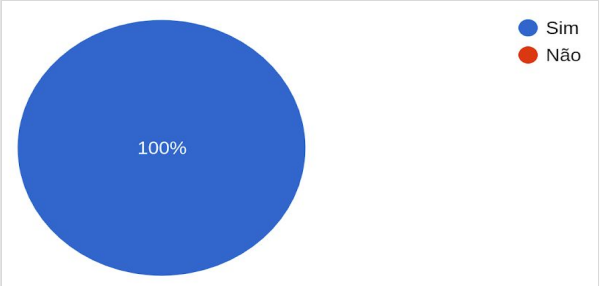
22. A escola tem uma área de TI ou recebe suporte de uma equipe responsável pela área disponibilizada pela secretaria de educação do município?



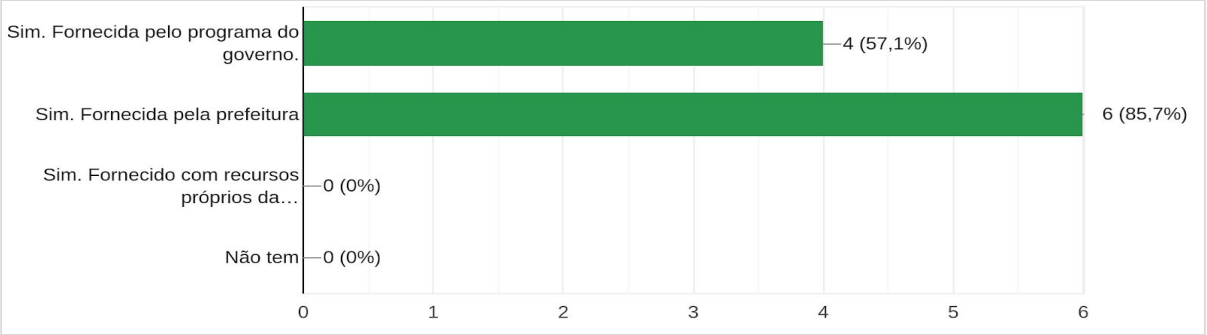
23. Como é dividida a estrutura de informática? Quantos computadores em cada rede? (Coloque 0 para as salas que não possuir computadores).



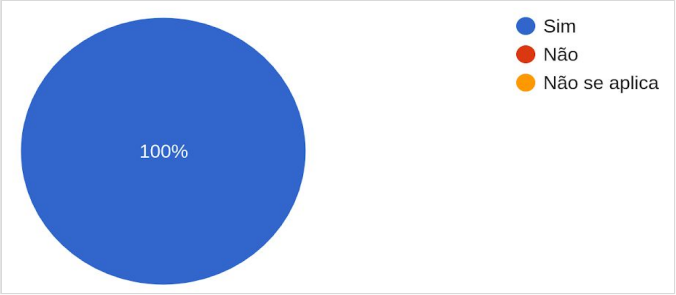
24.A escola possui Internet Banda Larga?



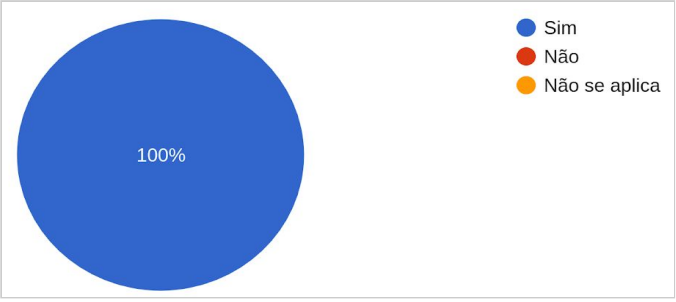
25.Se sim para pergunta anterior. A Internet é fornecida por algum programa do governo federal, prefeitura ou recursos próprios da escola?



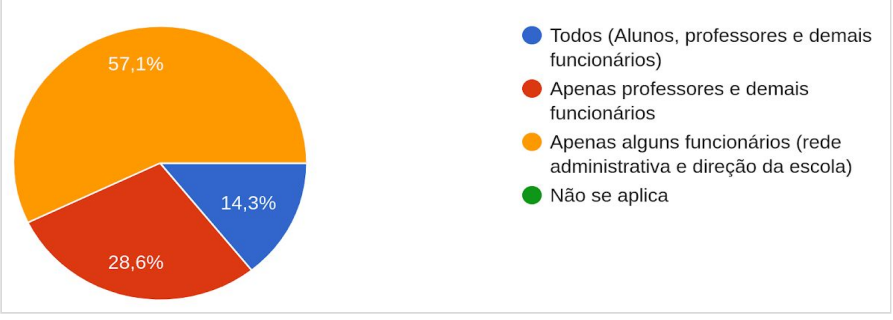
26.Se tem Internet, é distribuída/compartilhada a conexão por rede Wi-Fi?



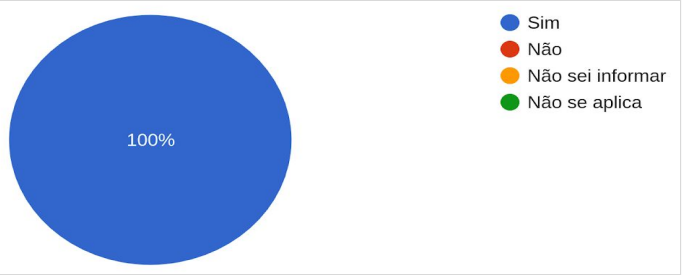
27.A rede Wi-Fi possui senha de segurança para ser acessada?



28.Quem tem acesso a rede Wi-Fi?



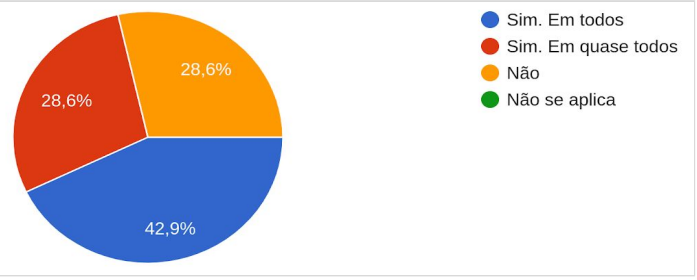
29. Todos os computadores e dispositivos ficam conectados na mesma rede?



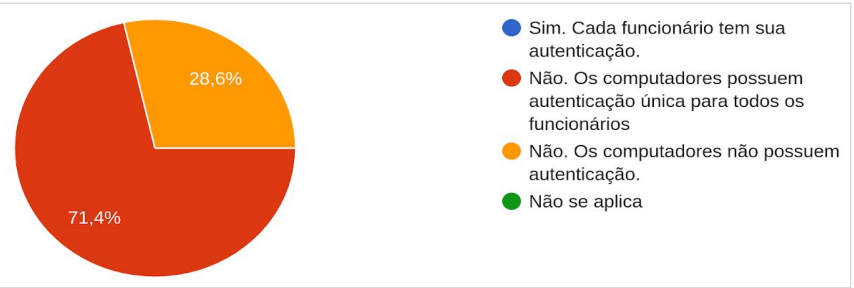
30. Já aconteceu da rede Wi-Fi ser invadida por alunos ou mesmo por outra pessoa e, devido isso, ter que ser reconfigurada novamente para restabelecer o acesso?

31. É permitido que outros funcionários tenham acesso aos computadores principais onde e manipulada e armazenada a maior parte da informações da escola?

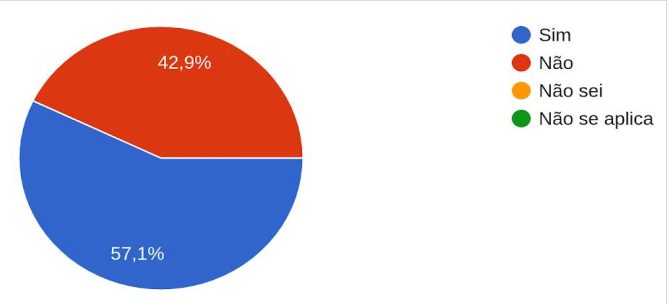
32. Para acessar os computadores da escola é necessário que seja feita uma autenticação (login) para utilizar o mesmo?



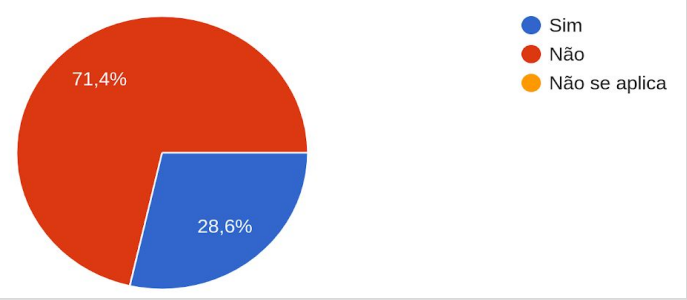
33. Cada funcionário que manuseia as informações nos computadores possuem usuário e senha de acesso restrito?



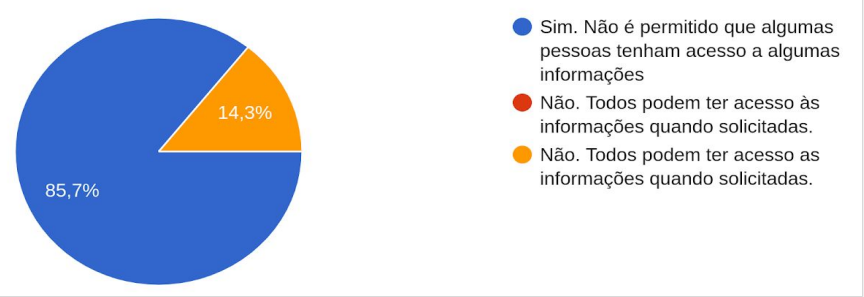
34. O funcionário quando se ausenta por algum momento do computador faz uso de bloqueio e proteção de tela?



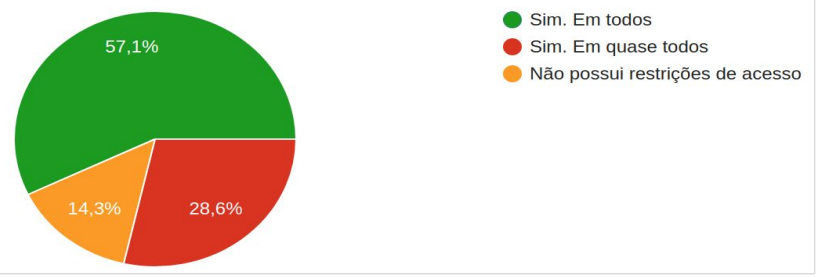
35. Quando um funcionário deixa de trabalhar na escola, as senhas do local de trabalho, e-mails e outros utilizado por ele são trocadas?



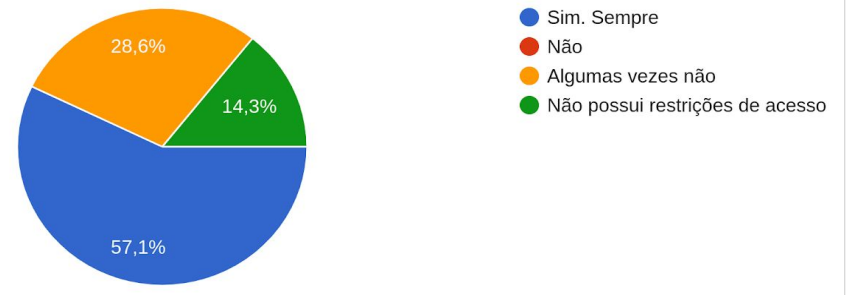
36. A escola possui algum sistema de restrição de pessoas a determinadas informações?



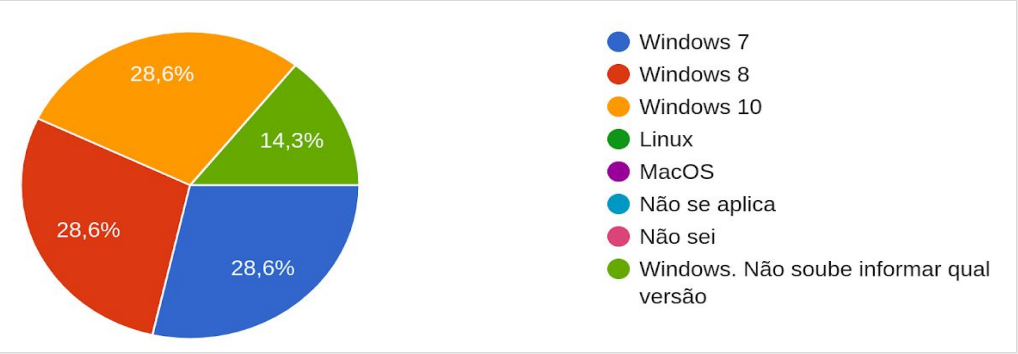
37. A escola possui restrição/controle de acesso físico em determinadas salas/departamentos?



38. Os funcionários obedecem às restrições?

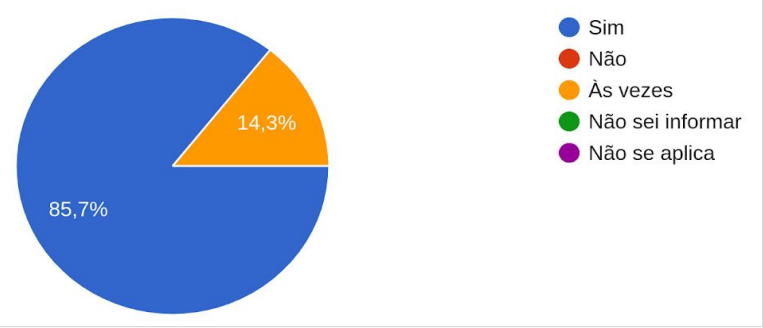


39.Qual sistema operacional dos computadores da escola e qual a versão?

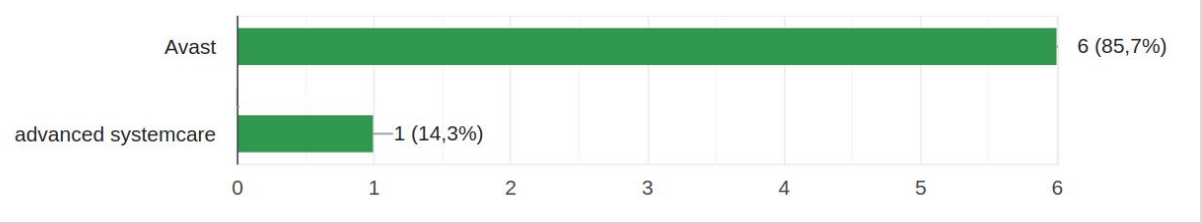


40.É pago a licença do Sistema Operacional e dos programas instalados?

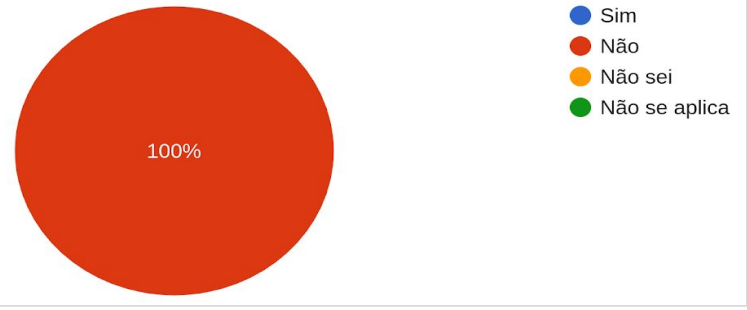
41.Sistema Operacional e programas dos computadores são atualizados com frequência?



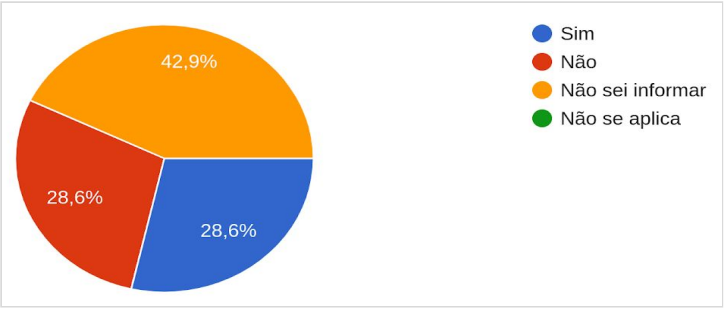
42.Os computadores tem antivírus instalado? Se sim, qual?



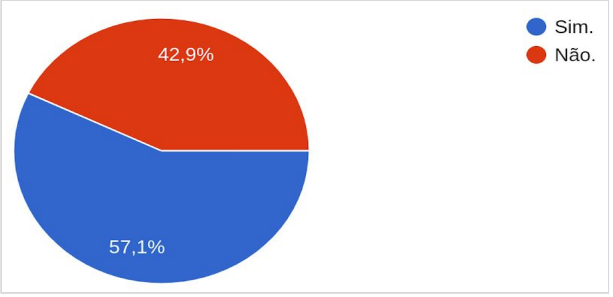
43.É pago a licença dos antivírus?



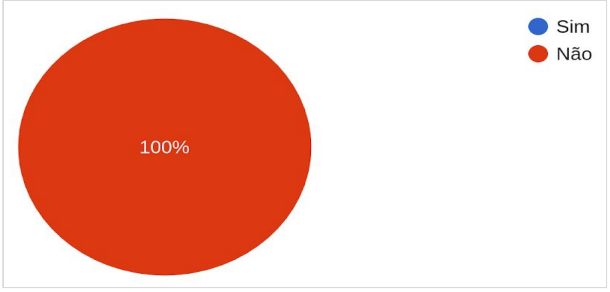
44. Os computadores da escola já foram infectados por algum tipo de código malicioso? (vírus, cavalo de troia entre outros).



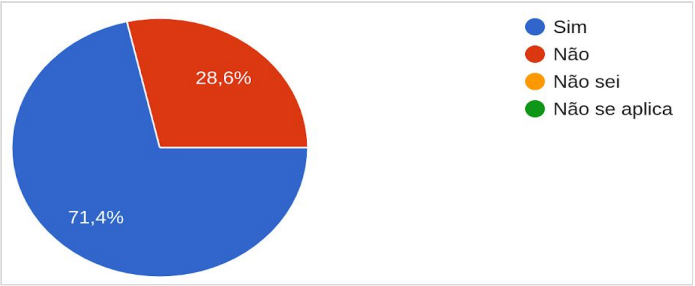
45. Você saberia identificar se um computador estaria infectado por algum código malicioso?



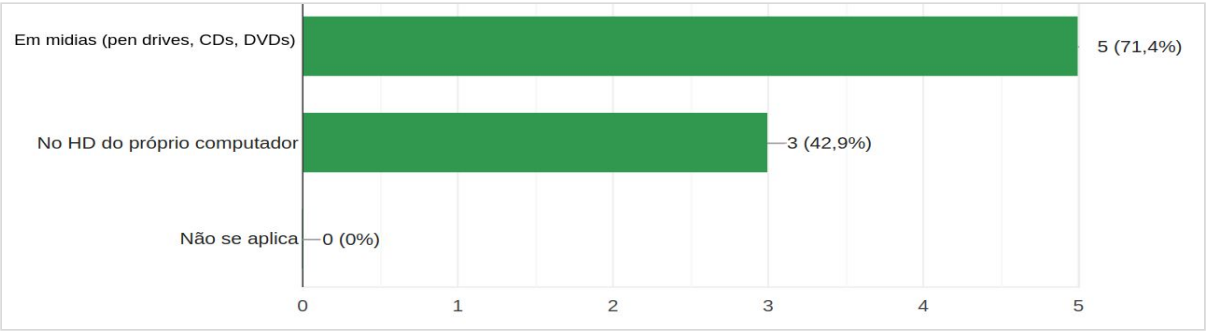
46. Os funcionários recebem orientações sobre o que é e como funciona um software malicioso?



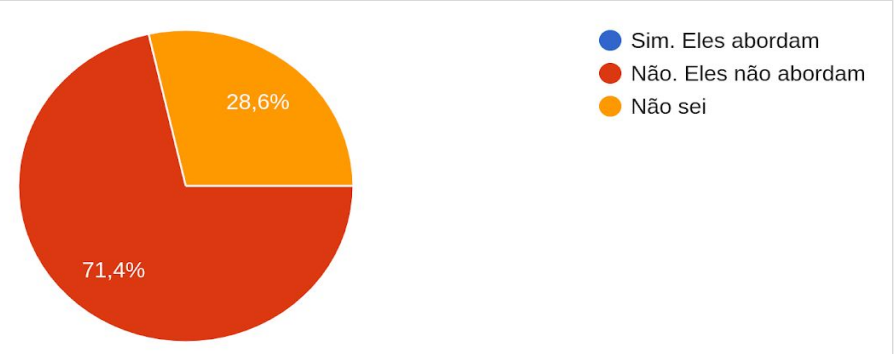
47. É feito cópias de segurança dos dados com regularidade?



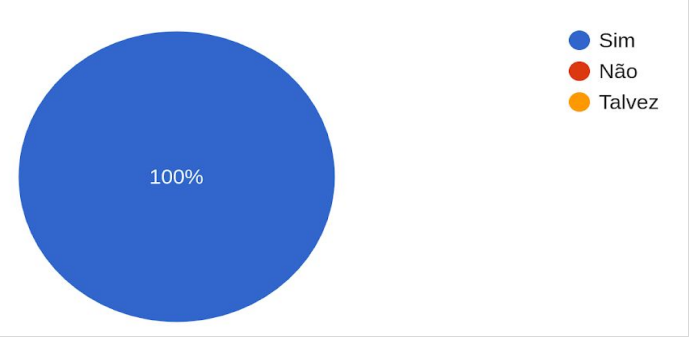
48. Se é feito cópias de segurança, onde são guardadas?



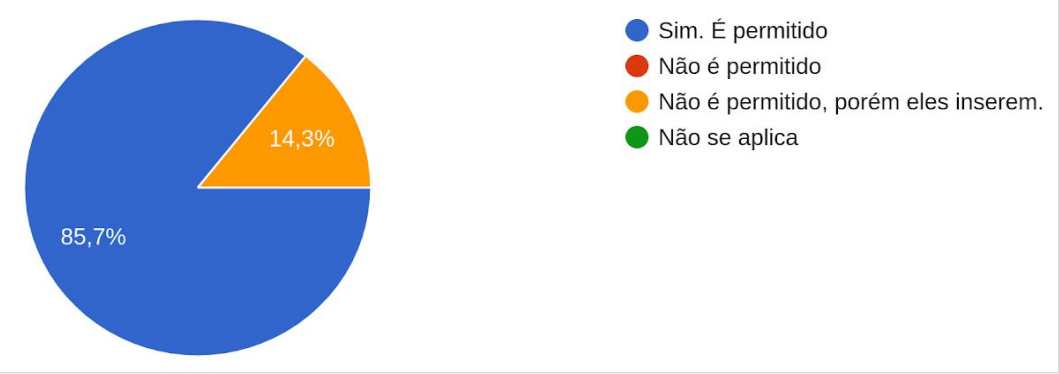
49. Sabe informar se os professores abordam conteúdos sobre uso seguro da Internet com os alunos?



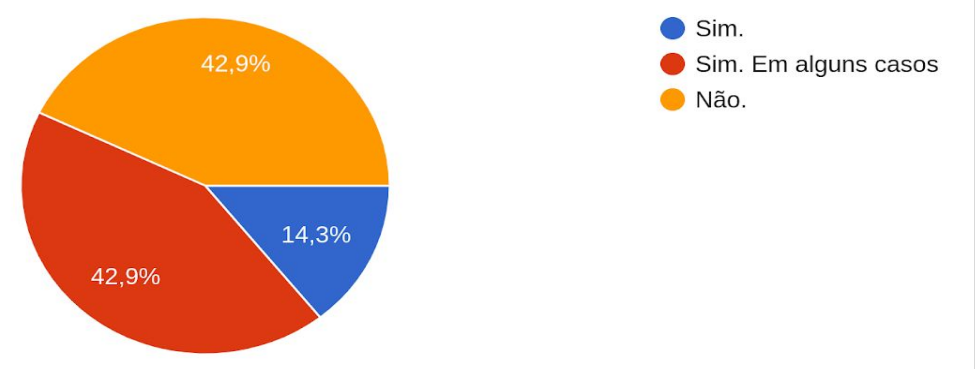
50. Considera importante uma capacitação para docentes, funcionários e alunos sobre o tema segurança da informação?



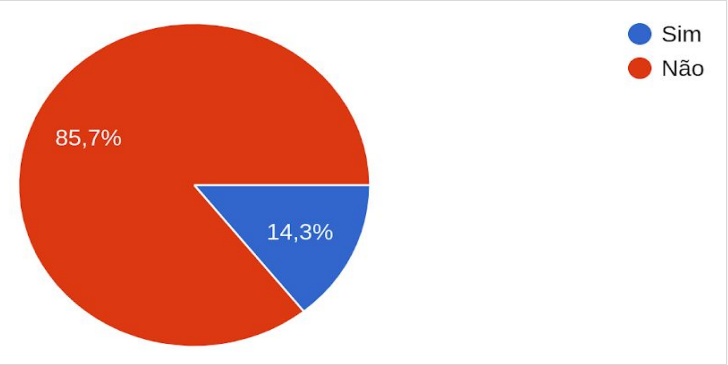
51. É permitido que docentes, funcionários e alunos insiram mídias (Pen Drives, celulares, etc), mesmo para fins didáticos, nos computadores da escola?



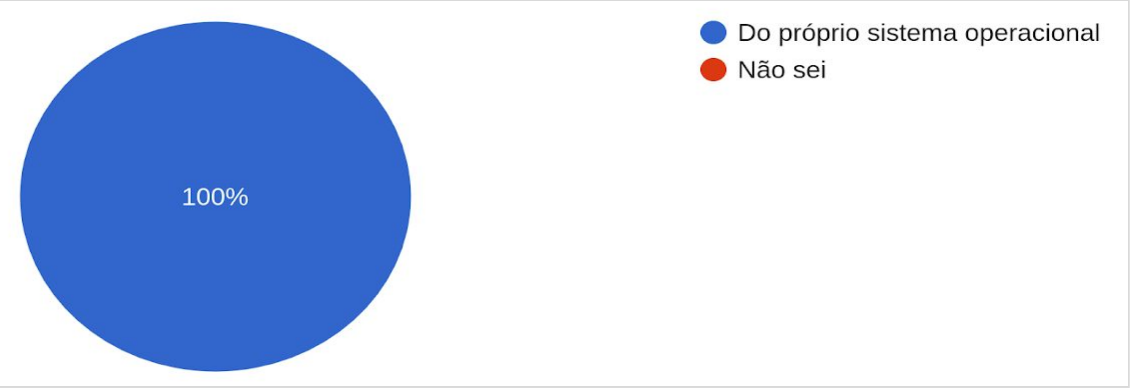
52. É permitido o uso de computadores da escola para fins pessoais? (exemplo: acessar/enviar e-mais pessoais, acessar páginas desconhecidas, youtube, redes sociais, etc.).



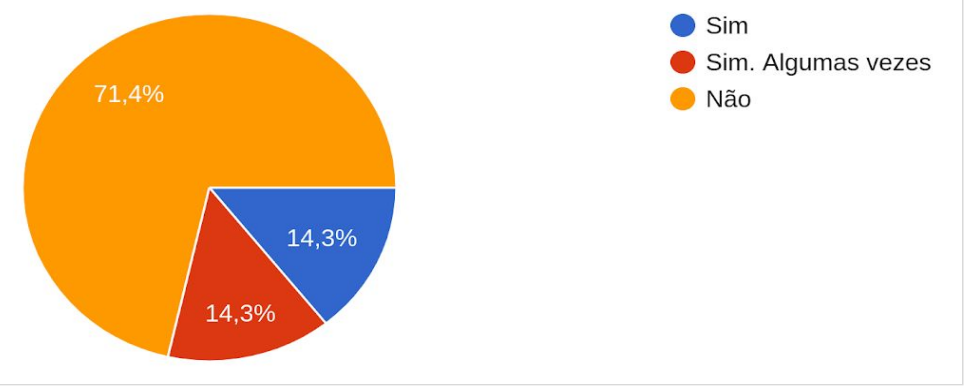
53. Vocês realizam alguma campanha para conscientização do uso adequado dos recursos de informática?



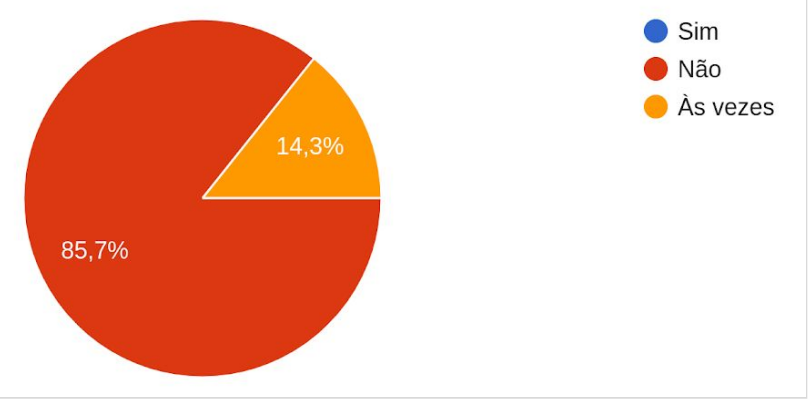
54. Qual firewall a escola utiliza?



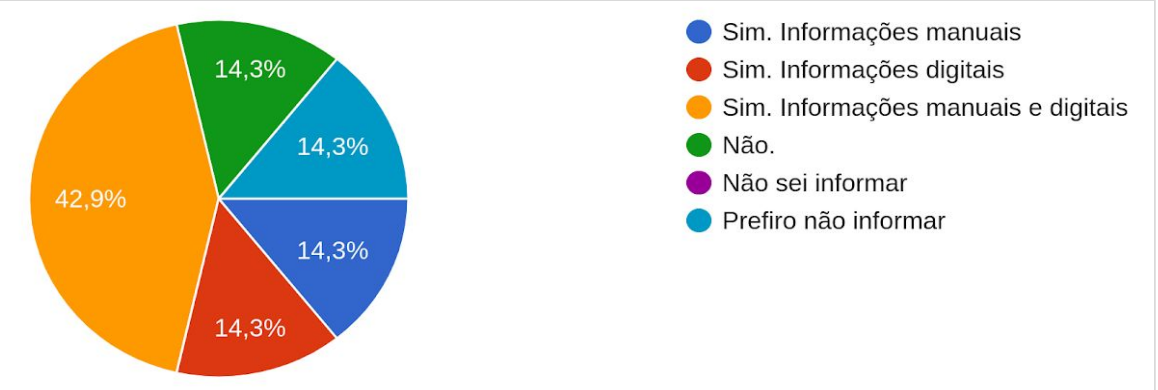
55. É permitido que docentes, funcionários ou alunos instalar programas ou baixar conteúdos (músicas, filmes, jogos)?



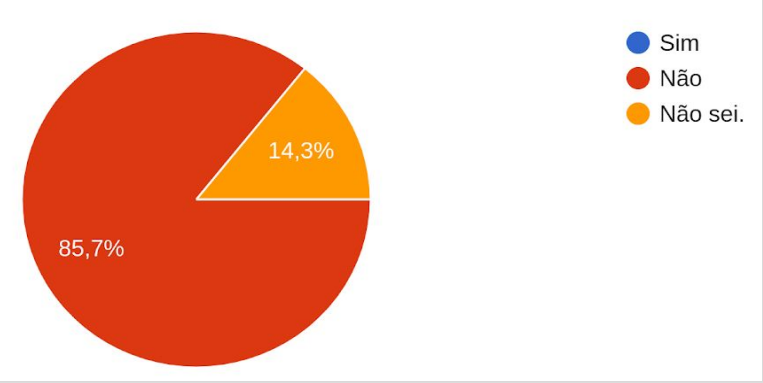
56. Os funcionários costumam deixar papéis com informações importantes sobre a mesa?



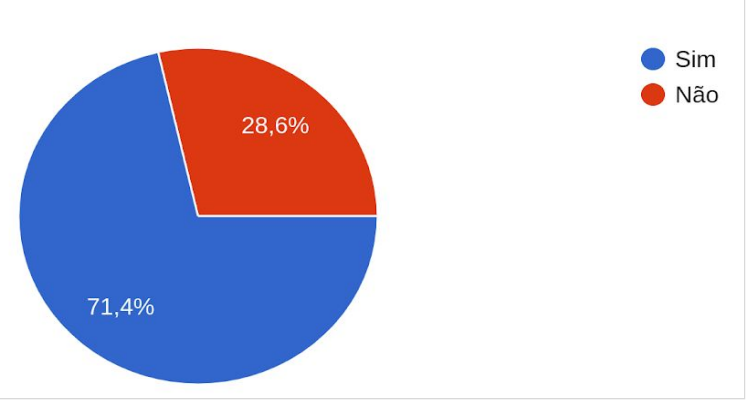
57. A escola já procurou algum dado ou informação importante e não encontrou?



58. A escola possui uma política de segurança da informação?



59. Você sabe o que é segurança da informação? Se sim, pode nos explicar se ela é aplicada na escola e como.



60. Considera que as informações da escola estão seguras?