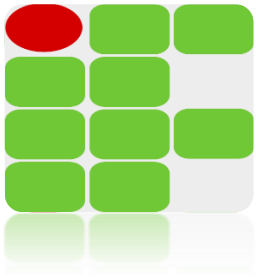
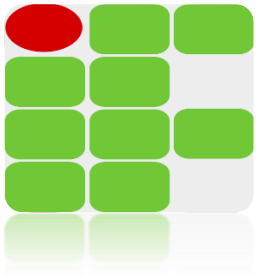


MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLOGIA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TOCANTINS
***CAMPUS* PORTO NACIONAL**
CURSO LICENCIATURA EM COMPUTAÇÃO

LUCIANO RAIMUNDO DOS SANTOS

UMA PROPOSTA DE SEGURANÇA DA INFORMAÇÃO PARA AS INSTITUIÇÕES DE ENSINO DE PORTO NACIONAL - TO

Porto Nacional – TO
2018



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLOGIA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TOCANTINS
***CAMPUS* PORTO NACIONAL**

LUCIANO RAIMUNDO DOS SANTOS

UMA PROPOSTA DE SEGURANÇA DA INFORMAÇÃO PARA AS INSTITUIÇÕES DE ENSINO DE PORTO NACIONAL - TO.

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Licenciatura em Computação do Instituto Federal de Educação Ciência e Tecnologia do Tocantins - *Campus* Porto Nacional, como exigência à obtenção do grau de Licenciado em Computação.

Orientador: Professor Me. Luciano Correia Franco.

Porto Nacional – TO
2018

LUCIANO RAIMUNDO DOS SANTOS

UMA PROPOSTA DE SEGURANÇA DA INFORMAÇÃO PARA AS INSTITUIÇÕES DE ENSINO DE PORTO NACIONAL - TO.

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Licenciatura em Computação do Instituto Federal de Educação Ciência e Tecnologia do Tocantins - *Campus* Porto Nacional, como exigência à obtenção do grau de Licenciado em Computação.

Orientador: Professor Me. Luciano Correia Franco.

Aprovado em: ___/____/_____

BANCA AVALIADORA

_____

Professor Me. Luciano Correia Franco

IFTO – *Campus* Porto Nacional – TO

_____

Professor Me. Elvis Nascimento da Silva

IFTO – *Campus* Porto Nacional – TO

_____

Professor Me. Teomar Manduca Aires

IFTO – *Campus* Porto Nacional – TO

Porto Nacional – TO

2018

Este trabalho é humildemente dedicado a Deus, e à minha família que sempre me apoio e me incentivou com os estudos: minha mãe guerreira, meus irmãos, é em especial minha esposa e minha filha.

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus, por me dar força e coragem para prosseguir em mais uma etapa da minha vida.

Agradeço a minha Mãe Iracema Raimundo dos Santos, meus Irmãos; Ana Lucilene dos Santos, Ana Lucia dos Santos, Edmilson dos Santos, Hesmildo R. dos Santos, Luciana R. dos Santos, Remilson R. dos Santos e Romildo R. dos Santos, que sempre me conduziram para continuar com os estudos, para que já mais desistisse dos meus sonhos.

Agradeço a minha querida esposa Raiele Florentino Ramos dos Santos e minha filha Layellen Florentino dos Santos pela paciência, sacrifícios, compreensão e apoio dedicados durante toda a minha vida acadêmica.

Agradeço ao meu mentor, conselheiro e orientador, professor e mestre Luciano Correia Franco, pela orientação, paciência e dedicação na elaboração deste trabalho.

Agradeço os demais professores que tive o prazer de conhecer ao longo do Curso de Licenciatura em Computação em especial, Albano Dias, Elias Vidal, Elvis Nascimento, Heleno Manduca, Jânio Carlos, Kênia Maria, Lillissanne Marcelly, Maria Madalena, Mayara Kayne, Paulo Patricio, Rafael Manduca, Rosinete Libânio e Teomar Manduca.

Agradeço a todos os meus amigos e colegas de curso em especial, José Maria, Gilmário, Pâmela, Karen e Willams, pelos momentos de convívio, apoio e incentivo nos trabalhos e estudos.

Agradeço também a todas aquelas pessoas que aqui não citei nome, como alguns professores, familiares, amigos e colegas que de alguma forma me ajudaram a vencer este desafio.

RESUMO

A tecnologia da informação vem passando por um processo de evolução muito rápida e transforma a vida de seus adeptos e usuários cada vez mais. Acesso à informação, interatividade, funcionalidades e possibilidades ilimitadas através das redes de computadores distribuídas por todo o mundo. A rede mundial de computadores, a Internet, reforça a necessidade de garantir a segurança da informação, com intuito de salvar, guardar e manter o sigilo e integridade de informações e proteger os recursos tecnológicos, de *Hardware* e *Software.* As políticas e protocolos de segurança são um conjunto de regras, normas e diretrizes que estabelecem padrões e constituem uma solução para o problema de segurança da informação em redes públicas e privadas, permitindo maior garantia de proteção, privacidade e controle de acesso nos ambiente das instituições, incluindo as de ensino da cidade de Porto Nacional – TO. Esse trabalho apresenta um levantamento que permite analisar a situação dessas instituições com relação aos investimentos internos em segurança de sistemas. E propõe a utilização de procedimentos e ferramentas que visem minimizar os problemas relacionados à segurança da informação.

Palavras Chave: Segurança da informação, segurança de redes, educação.

ABSTRACT

Information technology has been undergoing a very rapid evolution process and it transforms the lives of its fans and users more and more. Access to information, interactivity, functionality and unlimited possibilities through computer networks distributed all over the world. The worldwide computer network, the Internet, reinforces the need to ensure information security, in order to safe, guard and maintain the confidentiality and integrity of information and to protect the technological, hardware and software resources. Security policies and protocols are a set of rules, norms and guidelines that establish standards and provide a solution to the problem of information security in public and private networks, allowing greater guarantee of protection, privacy and access control in the institutions' environment , including those of teaching in the city of Porto Nacional - TO. This paper presents a survey that allows analyzing the situation of these institutions in relation to internal investments in systems security. It proposes the use of procedures and tools to minimize problems related to information security.

Keywords: *Information security, network security, education.*

LISTAS DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABRAVEATURAS E SIGRAS

ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
DoS	Denial of Service
ERP	Enterprise Resource Planning
FDDI	Fiber Distributed Data Interface
IEC	International Electrotechnical Commission
IGRP	InteriorGateway Routing Protocol
IP	*Internet Protocol*
ISO	International Organization for Standardization
LAN	*Local Area Network* – Rede de Área Local
MAC	*Media Access Control*
MANs	Metropolitan Area Networks
NBR	Norma Brasileira
QEdu	Qualidade da Educação
OSPF	Open Shortest Path First
PPP	Point – to Point Protocol
RIP	Routing Information Protocol
SCSI	Internet Small Computer System Interface
SNMP	*Simple Network Management Protocol*
TCP	*Transmition Control Protocol*
UDP	*User Datagram Protocol*
WANs	*Wide Area Network*

SUMÁRIO

1. INTRODUÇÃO

Podemos definir a segurança da informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acesso não autorizados, possuir políticas e ferramentas de baixo custo e de fácil configuração e administração pode ajudar na prevenção de falhas de segurança nas redes e obter maior controle das informações que trafegam nas mesmas, mesmo sem muitos recursos para se investir em infraestrutura (NBR ISSO/IEC 27002:2013, NBR ISSO/IEC 27000, NBR ISSO/IEC 27005:2011).

A segurança da informação, bem como a segurança das redes de computadores, têm se tornado um tema bastante comum. Nos dias atuais é difícil imaginar um computador “só”, ou seja, que esteja totalmente isolado de qualquer rede de computadores. Nem mesmo dispositivos móveis como telefones celulares digitais, *ipads, tablets* e *notebooks* estão isolados de qualquer rede que seja. Todos esses dispositivos, de maior ou menor complexidade, são conectados através de *roteadores* e *modens* a redes de menor ou maior abrangência, todas interconectadas, formando uma rede de alcance mundial, a Internet. Um mundo de computadores 100% interligados de alguma forma, cada um com seu endereço físico, conectados em algum lugar do mundo de forma unívoca (NBR ISSO/IEC 27002:2013, NBR ISSO/IEC 27000, NBR ISSO/IEC 27005:2011).

A Internet é conhecida como a Rede Mundial de Computadores, e dentro desse imenso escopo cresce a cada ano a preocupação com a segurança da informação. Os casos de danos causados por ação de programas maliciosos, ataques e outras ameaças vão da simples perda de privacidade a golpes e fraudes de grande prejuízo material e financeiro. As pessoas e empresas, bem como organizações de toda espécie, vêm travando uma verdadeira guerra no sentido de preservar seus dados dessas ameaças. Um tipo de organização que fica mais exposta aos riscos é a instituição educacional, devido o grande número de computadores, de uso administrativo e laboratorial. Porém, mesmo diante de tantos riscos aos quais as instituições de ensino públicas e privadas estão expostas na cidade de Porto Nacional – Tocantins, nota-se empiricamente que muitas vezes não existe uma estratégia eficaz para assegurar os dados e informações institucionais, como veremos no decorrer desta pesquisa (NBR ISSO/IEC 27002:2013, NBR ISSO/IEC 27000, NBR ISSO/IEC 27005:2011).

Este trabalho apresenta informações que foram coletadas através de questionário em uma pesquisa relacionada à segurança da informação, junto às Instituições de Ensino de Porto Nacional - TO. Procurou-se com essas informações construir indicadores de investimento em recursos de segurança da informação por parte dessas instituições, de forma a construir uma análise e propor soluções (NBR ISSO/IEC 27002:2013, NBR ISSO/IEC 27000, NBR ISSO/IEC 27005:2011).

1.1 Problema da pesquisa

O presente trabalho parte do pressuposto de que, de uma forma geral, as instituições de ensino da cidade de Porto Nacional não têm se preocupado devidamente com as questões de segurança da informação dentro de seus limites organizacionais. Um possível indício é a grande quantidade de relatos de incidentes de segurança por parte de alunos e colaboradores dessas instituições. Portanto, seria útil conhecer aspectos relacionados a essa realidade, buscar entendê-la e propor algumas soluções. Para isso foi preciso conhecer a realidade das escolas de Porto Nacional quanto ao investimento em segurança e o que poderia ser feito para mudar essa realidade.

1.2 Justificativa

Segundo Marconi e Lakatos (2011, p.69), a pesquisa de levantamento *survey* em campo é a mais apropriada para a construção de indicadores mais precisos; é preciso conhecer indicadores que se aproximem da realidade empírica das escolas quanto à preocupação com a segurança nos ambientes de rede. A proposta pode facilitar a gestão da segurança nas escolas, pois atualmente o assunto da segurança em rede está em pauta em grande parte dos ambientes. Mas pouco se fala em segurança da informação voltada para as instituições de ensino, em especial na cidade de Porto Nacional, TO.

> Problemas com segurança podem atrapalhar os professores no uso da Internet em seu ambiente de trabalho, alunos podem obtém informações que deveriam ser exclusivas de servidores ou da instituição e outras ocorrências podem surgir (Beal, 2005).

> Por mais que existam inúmeras tecnologias e ferramentas disponíveis no mercado para a segurança de redes, que poderiam ser usadas por estas instituições, elas ainda encontram dificuldades na implantação de uma política de

> segurança eficaz e de fácil gerenciamento. Parte por falta de profissionais de T.I dentro da unidade de ensino parte por falta de planejamento do setor financeiro ou dos gestores responsáveis por elas, e ainda pela falta de interesse em investimentos neste departamento (Sêmola, 2003).
>
> .

Existem hoje no mercado muitos tipos de soluções em segurança da informação e de redes, elas podem ser muito complexas, robustas e de alto custo, como também podem ser baratas, simples e ainda assim eficazes. O mais importante é dimensionar a solução de acordo com a situação, ou seja, adequar o investimento em segurança baseado na relação custo/benefício das mesmas. Desta forma torna-se mais fácil decidir qual seria a solução ideal (Sêmola, 2003).

1.3 Objetivos da Pesquisa

1.3.1 Objetivo Geral

Este trabalho tem como objetivo principal propor soluções seguras de administração de redes para pequenas e médias organizações com segurança da informação para as instituições de ensino públicas e particulares, de ensino básico e superior, na cidade de Porto Nacional – TO, com base na análise de informações levantadas.

1.3.2 Objetivos Específicos

- Discorrer sobre os conceitos de segurança da informação, com foco na gestão dos sistemas e nas questões sociais que envolvem o tema;
- Apresentar indicadores do investimento em segurança da informação nas instituições de ensino de Porto Nacional;
- Analisar os indicadores levantados sob a ótica da gestão de recursos, com foco na resolução de problemas;

2. SEGURANÇA DA INFORMAÇÃO

Segundo a norma ABNT NBR ISO/IEC – 17799 (2005), o conceito geral sobre segurança da informação está diretamente relacionado à segurança de um conjunto de dados, a fim de preservar seu valor de informação. O termo segurança é usado com o significado de minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos. Vulnerabilidade é qualquer fraqueza que pode ser explorada para se violar um sistema ou as informações que ele contém.

A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados, e a utilização não autorizada do computador ou de seus dispositivos periféricos. A necessidade de proteção deve ser definida em termos das possíveis ameaças e riscos e dos objetivos de uma organização, formalizados nos termos de uma política de segurança. (SOARES; LEMOS e COLCHER, 1995, p.448):

A segurança em redes de computadores foi se tornando uma preocupação gradativa, à medida que as organizações necessitavam “esconder” seus dados importantes, medidas de segurança começaram a ser pensadas para a proteção destes dados. Nesta esfera pode-se entender que a partir do momento que se necessita proteger algo, tem-se este algo como um objeto ou informação de valor, e aí crescem cada vez mais as motivações para roubar estes dados das empresas (ABNT, 2006; NBR ISO/IEC 27001; ISO, 2005).

Segundo Kane (1989), após o surgimento e popularização dos microcomputadores e a criação da Internet, e seu crescente uso, inimagináveis formas de roubar dados vem sendo utilizadas por “piratas da Internet”, atualmente conhecidos como *Hackers (*indivíduos que elaboram e modificam softwares e hardwares de computadores*)*, *Crackers (*usado para designar quem pratica a quebra de um sistema de segurança*)* e outros. Estes são “bandidos” virtuais, que se utilizam de recursos computacionais para infringir a segurança das redes. Diante disso empresas começam a investir cada vez mais em segurança da informação, a fim de manter seus dados protegidos, bem como manter sua rede em perfeito funcionamento, visto que hoje a grande maioria das empresas depende das redes de computadores para sua sobrevivência. Enviar *E-mails*, acessar *sites*, pesquisar, trocar informações, acessar o sistema *ERP (Enterprise Resource Planning)*, concretizar negócios ou vender seus produtos *on-line*. Tudo isso não seria possível

sem o uso das redes de computadores, então se julga extremamente necessária sua segurança.

Uma rede de computadores é uma infraestrutura que permite interligar dois ou mais computadores (chamados *hosts*) para que possa haver troca de informações (mensagens) entre estes. Isso é possível devido a um conjunto de regras pré-estabelecidas para a comunicação, chamadas de protocolos. Os protocolos devem obrigatoriamente ser respeitados e seguidos por todos os *hosts* da rede de forma uniforme. A necessidade de um protocolo dá-se ao fato de que os *hosts* precisam comunicar-se de uma forma padrão ou, “falar a mesma língua”. Para isso necessitam-se não apenas de um protocolo, mas sim de uma pilha de protocolos separados em camadas, cada qual com suas características e funcionalidades (KUROSE; ROSS, 2006).

Os tópicos a seguir servirão de apoio para o entendimento dos conceitos de segurança da informação, camadas de protocolos de rede, protocolos de roteamento, topologias de rede entre outros. Pretende-se contemplar algumas dessas características na proposta de segurança para as escolas de Porto Nacional, apresentada neste trabalho.

2.1 Políticas de Segurança

A norma ABNT NBR. ISO/IEC – 17799 (2005) foi usada como referência nesse trabalho, pois constitui uma espécie de código nacional de prática para a gestão da segurança da informação. A política de segurança refere-se a um conjunto de regras, normas e diretrizes que estabelecem padrões desejáveis e aceitáveis de uso dos sistemas, bem como definem as limitações aferidas aos usuários da rede.

Com o crescente uso da Internet, das operações realizadas através dela e dos riscos que ela oferece, deve-se pensar em política de segurança, não apenas das redes de computadores, mas sim de todo um conjunto de diretrizes que administrem os pontos cruciais para a segurança, desde os direitos e deveres do uso de computadores pelos colaboradores, até uma política de acesso restrito à área de servidores. Também são necessárias políticas funcionais para o conjunto de dados que necessitam ser gravados em *backups*. Tudo deve ser pensado para a proteção de qualquer dado ou bem, seja intelectual ou físico.

A necessidade de uma política clara e usual é definitiva quando o assunto é segurança, cada empresa possui características e necessidades distintas, desta forma cada política deve conter diretrizes conforme as necessidades da empresa. Segundo alguns autores, mesmo com as diferentes necessidades das organizações, existem algumas premissas que devem ser levadas em conta na elaboração de uma política de segurança, mais precisamente três principais pontos devem ser levados em consideração.

Segundo Mello (2003), as políticas de segurança de sistemas se diferem em três ramos principais: segurança física, segurança gerencial e segurança lógica.

- **Segurança física –** trata-se da segurança física do sistema, o meio físico em que o sistema se sustenta. Que define as medidas de segurança contra desastres como: alagamentos, terremotos, incêndios, ou qualquer evento natural que venha prejudicar ou interromper o funcionamento dos sistemas. Bem como as restrições e delimitações de acesso aos equipamentos e etc;
- **Segurança gerencial –** trata-se do ponto de vista estratégico organizacional, definindo os processos, normatizando e gerenciando as tomadas de decisão;
- **Segurança lógica –** trata-se das definições de segurança no nível da aplicação, como permissões de usuários, direitos e monitoramentos das atividades.

2.1.1 Uso de *Firewall* e *Proxies* de rede

Para Mello (2003), o *Firewall* é uma ferramenta extremamente importante na proteção das redes corporativas, visto que ele é o responsável por filtrar os pacotes de dados que entram e saem da rede, bem como ajuda no bloqueio das portas de uso comum nos ataques de intrusos.

Os *Proxies* também são ferramentas de grande ajuda na proteção da rede, seu intuito é limitar o acesso dos usuários da rede para o mundo externo, ou seja, *proxies* bloqueiam o acesso dos usuários da rede interna para a Internet, impróprios, *downloads*, execução de complementos, programas de *downloads* como: P2P, Torrents (Rede de computadores onde os usuários conectados podem realizar funções de servidor e cliente ao mesmo tempo, P2P você baixa o arquivo completo de uma vez o Torrent você baixa o arquivo fragmentando), entre outros. O uso de

Proxies é muito recomendado visto que grande parte das vulnerabilidades da rede ocorre devido ao mau uso da Internet por parte dos usuários, (MELLO, 2003).

2.1.2 Senhas e configurações dos equipamentos

Segundo Bonifácio (1998), que fala sobre uma característica imprescindível quando se trata de segurança em rede, todos os equipamentos utilizados como: *modems,* roteadores*, switchs, firewalls, proxies,* servidores*, access points*, entre outros, devem ter suas senhas atualizadas periodicamente, seguindo um padrão aceitável de segurança, com uma quantidade mínima de caracteres aceitável. Por exemplo, a senha de um *modem* normalmente vem configurada por padrão com usuário=Admin e a sua senha=Admin. O recomendável é que se possível altere-se os dois campos, tanto usuário quando senha, se não for possível alterar o usuário, cria-se um novo usuário *master* e inativa-se o usuário Admin. A senha deve ter um mínimo de 8 caracteres em qualquer situação, e sempre utilizar senhas alfanuméricas combinadas com caracteres especiais, intercalando letras minúsculas e maiúsculas.

2.1.3 Utilização de equipamentos de proteção à rede física

Segundo BATES (1999), eis o motivo de propor-se uma análise da segurança da informação organizacional pela visão da teoria das ciências sociais: a informação é gerada, armazenada, tratada e transmitida com o fim de ser comunicada, e a comunicação é eminentemente um processo grupal, seja ela interna ou externa às fronteiras da organização. Uma rede se sustenta através do meio físico e todos os componentes que o compõe, Servidores, Computadores, *Switchs*, roteadores entre outros.

Para BATES (1999) a proteção física destes equipamentos previne desastres e perda de dados e informações. Ou seja, uma rede não sofre apenas problemas de ataques de intrusos, a segurança da rede envolve a perda, roubo ou destruição de dados e informações importantes. E neste contexto a falha de proteção com os equipamentos físicos da rede pode trazer prejuízos aos dados da empresa. Pode-se exemplificar tal situação com a hipótese de um raio queimar os servidores da empresa por falta de protetores anti-surtos*,* ou até mesmo uma oscilação de tensão na energia danificar o *software* ERP por falta de *no-breaks*.

Segundo BATES (1999) todo e qualquer problema que atrapalhe ou impeça o perfeito funcionamento da rede é considerado como falha de segurança da informação, mais precisamente no contexto de segurança de redes de computação. Desta forma o uso de *no-breaks*, anti-surtos elétricos, estabilizadores e outras formas de proteção são imprescindíveis para a segurança da rede.

2.1.4 Local para os equipamentos físicos

É comum deparar-se com empresas que alocam os equipamentos que compõem as redes em locais inadequados, sem ventilação, sujos, muitas vezes onde qualquer colaborador tem acesso, totalmente vulneráveis e sem nenhuma condição física adequada. É muito importante a conscientização de que os equipamentos da rede precisam estar em um local adequado, arejado, alocados em um *rack*, de preferência em local onde se possa controlar a temperatura com o uso de ar-condicionado. Recomenda-se que pelo menos algumas dessas providências sejam tomadas. Muitas vezes a empresa não possui um espaço adequado, como uma sala só para os equipamentos, e nestes casos recomenda-se que exista ao menos uma estrutura de divisórias impedindo o acesso livre aos equipamentos. (MELLO 2003).

A segurança física é feita nas imediações da empresa levando em consideração a prevenção de dados que podem sofrer danos. Por isso, investigar a ocorrência de eventos climáticos passados é importante ao se planejar os métodos de segurança física para proteção de funcionários, equipamento e dados do local. Além disso, a segurança física trata de métodos para evitar o acesso de pessoas não autorizadas a áreas em que se encontram dados e informações críticas da empresa. Outro tipo de reforço para a segurança do local é usar mecanismos como fechaduras eletrônicas, câmeras e alarmes, para controlarem o acesso aos ambientes que guardam *backups* e computadores com dados confidenciais. Para desenvolver uma boa segurança física é preciso analisar o perfil da empresa, o tipo de proteção necessária, os investimentos possíveis e definir uma política de controle de acesso físico que se encaixe ao modelo de negócio, (BONIFÁCIO, 1998).

A segurança lógica controla o acesso a aplicativos, dados, sistemas operacionais, previne contra *hackers* e possíveis invasões às fontes internas da empresa. A segurança lógica permite que o acesso seja baseado nas necessidades específicas de cada usuário para realizar suas tarefas, assim, nenhum

funcionário poderá executar funções que não sejam de seu cargo. Para aprimorar esses mecanismos, é importante sempre manter sistemas e protocolos operacionais atualizados. Os riscos que uma empresa corre por não ter uma boa estrutura de segurança lógica são muitos, como acesso de terceiro a informações sigilosas, perdas de dados, falhas na rede causada por fraudes, entre outros, (BONIFÁCIO, 1998).

2.1.5 Uso de Redundâncias

O uso de redundâncias também é uma prevenção à indisponibilidade de sistemas, tanto para o *software* quanto para o *hardware*. A rede sempre deve ter uma segunda ou terceira alternativa, assim como um roteador precisa de rotas alternativas, uma rede precisa opções para um funcionamento alternativo. Todo o tráfego de uma rede pode parar simplesmente porque um roteador parou de funcionar, deve haver um equipamento configurado sobressalente, ou uma rota alternativa para não comprometer o funcionamento da rede. Assim também como *links* de redundância de Internet. Uma rede que necessita do uso da Internet para o funcionamento de suas aplicações não pode depender de um único *link* de Internet, ou de um único provedor de serviços de Internet (ISP). Deve haver sempre ao menos dois *links* distintos de operadoras distintas, e ainda se possível que haja balanceamento de carga destes *links*, ou seja, se um *link* cair por algum motivo, outro *link* é acionado automaticamente sem que haja queda da Internet. O balanceamento de carga também é útil na divisão do fluxo da rede em *links* diferentes, não permitindo que ocorra excesso de carga em um único *link*, ou uma única rota na rede, (MOREIRA, 2001, p.50).

2.1.6 Monitoramento, Controle e Gerência de redes

Segundo Westphalen (2014, pág.54), existem ferramentas no mercado que possibilitam o monitoramento e controle da rede através de protocolos específicos para estas finalidades, como por exemplo, o protocolo SNMP (*Simple Network Management Protocol*). O SNMP tem por objetivo principal coletar informações da rede e fornecê-las para possibilitar seu gerenciamento, controle, resolver eventuais problemas e fornecer informações para planejar expansões. Uma rede de computadores precisa ser monitorada, controlada e gerenciada por alguém, o uso de

equipamentos e ferramentas de rede não tem valor algum se estes não forem gerenciados por um departamento ou um profissional da empresa. O próprio protocolo SNMP que possui uma utilidade enorme torna-se obsoleto se não for gerenciado por alguém, pois nenhuma aplicação, *software* ou *hardware* poderá ser tomado de decisões gerenciais da empresa, estas podem apenas fornecer as informações necessárias para as tomadas de decisão. Embora, do ponto de vista tecnológico, a necessidade de uma segurança da informação efetiva e os requisitos que almejam satisfazê-la estejam muito bem definidos e sejam amplamente conhecidos.

2.2 Segurança de rede

Partindo de um princípio lógico sobre segurança em rede de computadores, pode-se afirmar que a segurança está na preservação dos dados mantidos nos elementos que integram esta rede, como por exemplo, um banco de dados do sistema que a empresa possui, ou a troca de informações de entrada e saída da rede corporativa de forma segura e confidencial, (KUROSE, 2006).

Segundo Kurose (2006), para que possamos estabelecer uma conexão de rede de forma segura, é desejável que se atentem às seguintes propriedades: “Confidencialidade: Somente o remetente e o destinatário pretendido devem poder entender o conteúdo da mensagem transmitida.” Sendo para isso necessário o uso de alguma forma de criptografia de dados, fazendo com que a mensagem não possa ser decifrada por algum intruso. “Autenticação: O remetente e o destinatário precisam confirmar a identidade da outra parte envolvida na comunicação – confirmar que a outra parte realmente é quem alega ser.” Um dos pontos mais difíceis de tratar quando o assunto é comunicação segura, é que hoje em dia existem inúmeras formas de se passar por outra pessoa na Internet, como por exemplo, a camuflagem de endereço IP (endereço do protocolo de *internet*). Com um programa é possível disfarçar um endereço de IP por outro. “Integridade e não repúdio de mensagem: Mesmo que o remetente e o destinatário consigam se autenticar reciprocamente, eles também querem assegurar que o conteúdo de sua comunicação não seja alterado, por acidente ou por má intenção, durante a transmissão.” Ou seja, a mensagem tem que chegar ao destinatário exatamente como saiu do remetente, utilizando técnicas de criptografia e comparação de dados.

Disponibilidade e controle de acesso: um dos maiores fatores que levaram ao uso de políticas de segurança de rede surgiu após a popularização da Internet, devido aos ataques de negação de serviço *DoS* (*Denial of Service*), que indisponibilizam os serviços da rede para os usuários legítimos, de forma que nenhum usuário consegue acessar um servidor ou um *host* da rede.

Confidencialidade, autenticação, integridade e não-repúdio de mensagem vêm sendo considerados componentes fundamentais da comunicação segura há bastante tempo (McCUMBER, 1991). Disponibilidade e controle de acesso são extensões mais recentes da noção de comunicações seguras (BISHOP, 2003).

2.3 Falhas que comprometem a segurança da rede

Para SÊMOLA (2003), diante de todo o exposto sobre as características das redes de computação, dos conceitos e políticas da segurança em redes de computadores e das motivações para ataques a redes corporativas por *crakers* e outros piratas da Internet, é preciso entender quais são as principais formas de ataques, e discutir as principais vulnerabilidades das redes corporativas, bem como utilizar sempre um *case* de redes de pequenas e médias empresas, visto que esse tamanho de rede é o objeto de estudo deste *TCC.*

2.3.1 Ausência de Políticas de Segurança da Informação

Para Sêmola (2003), a gestão de segurança da informação pode ser classificada em três aspectos: tecnológicos, físicos e humanos. Esta é sem dúvidas uma das principais falhas na segurança de uma organização ou instituição. Como em qualquer sociedade que não possui leis que orientem como deve ser o comportamento dos cidadãos - esta sociedade não terá limites e estará completamente vulnerável a qualquer situação de risco - assim também é uma rede que não possui suas diretrizes e normas de uso. Sem estas é impossível controlar o que está sendo feito dentro da rede, assim como também não será possível tomar medidas reativas, uma vez que essas não foram definidas em uma política de uso da rede.

Para Schneier (2001), “as ameaças do mundo digital espelham no mundo físico. Se o desfalque é uma ameaça, então o desfalque digital também é uma ameaça. Se os bancos físicos são roubados, então os bancos digitais serão

roubados.” Infelizmente uma das principais causas de invasões e problemas de proliferação de vírus e *key-logers* em redes de computadores corporativas é o mau uso da Internet*, e-mail* e mensageiros eletrônicos por parte dos usuários destas redes. Atualmente existem milhares de correspondências e *links* falsos que disseminam programas maliciosos, sendo espalhadas nos últimos anos principalmente através das redes sociais.

2.3.2 Ausência de controle de acesso à rede

Para Moreira (2001, p.50), poucas são as organizações de pequeno e médio porte que possuem um controle adequado de acesso à rede por meio de autenticação de segurança, bem como dificilmente possuem uma gerência destes acessos, ou seja, não se sabe ao certo quem está usando a rede, se este usuário é um colaborador ou um intruso, se algum usuário está realizando acessos a locais indevidos e o quê o usuário está acessando na Internet.

2.3.3 *E-mails* e *links* falsos

O roubo de informações, conforme MOREIRA (2001, p. 49), ocorre não somente quando os computadores e *notebooks* são roubados fisicamente, mas também quando são subtraídas as informações que eles contêm. Pode acontecer todos os dias, sendo necessário por parte da empresa trabalhar com a conscientização dos funcionários, no intuito de evitar a conivência com ações como estas. Uma das formas muito comuns de invasão a redes corporativas são *links* e *e-mails* falsos que encaminham os usuários a páginas que possuem o intuito de instalar programas maliciosos na rede, como *key-logers, sniffers* entre outros. Estes programas, por sua vez, tem o intuito de roubar dados e/ou danificar os arquivos dos computadores.

Conforme Moreira (2001, p.50), existem vários riscos relacionados ao *e-mail* falso*,* desde golpes até contaminação por vírus. Apesar de ser um meio eficiente de se trocar informações, ultimamente têm surgido diversas formas de burlá-lo e torná-lo um meio de propagar vírus pela Internet. O *e-mail* em uma organização deve ser utilizado para propósitos comerciais, mas comumentemente é utilizado para propósitos particulares, para fazerem *spam,* e outros fins que não o de negócios.

2.3.4 Ausência de *firewalls* e *proxies*

Segundo Soares (1995), um *firewall* poder ser uma solução de *software* ou *hardware*. Esta informação não está incorreta, mas é necessário um complemento: o *hardware firewall* nesse caso nada mais é do que um equipamento com um *software* de *firewall* instalado, destinado exclusivamente a essa tarefa.

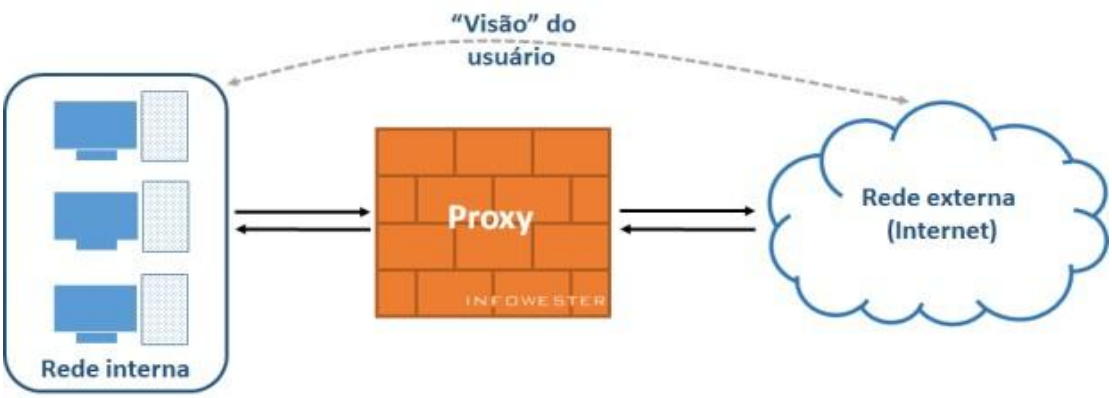
É possível encontrar, por exemplo, roteadores, *modens* ou equipamentos semelhantes que exercem a função de *firewall*. Neste caso, o objetivo normalmente é o de proteger uma rede com tráfego considerável ou com dados muito importantes.

Sem o controle do que entra e sai da rede, e sem o controle do que pode ser acessado pelos usuários, fica ainda mais fácil invadir uma rede com técnicas de varredura de portas, vírus, *ip spoofing*, roteamento dirigido, *trojan horse* entre outros (SOARES, 1995).

O *firewall* de aplicação**,** também conhecido como *Proxy* de Serviços (*Proxy Services*) é uma solução de segurança que atua como intermediário entre um computador ou uma rede interna e outra rede, externa - normalmente, a Internet. Geralmente instalados em servidores potentes por precisarem lidar com um grande número de solicitações, *firewalls* deste tipo são opções interessantes de segurança porque não permitem a comunicação direta entre origem e destino (SOARES, 1995).

A imagem a seguir ajuda na compreensão do conceito. Perceba que em vez de a rede interna se comunicar diretamente com a Internet, há um equipamento entre ambos que cria duas conexões: entre a rede e o *proxy*, e entre o *proxy* e a Internet.

Figura 1: Diagrama uso do *Firewall*



Fonte: Infowester (2018).

2.3.5 Ausência de Gerenciamento da Rede

Por fim a ABNT NBR ISO/IEC 17799 (2005), aponta que um dos motivos que levam empresas a sofrerem ataques de todos os tipos é o não gerenciamento de suas redes de computadores, bem como o não gerenciamento da segurança da informação como um todo. Definitivamente uma rede sem gerenciamento está muito mais suscetível a falhas de segurança. Vêm crescendo o nível de preocupação das empresas com a Gerência da Segurança da Informação, mas ainda assim o número de empresas de pequeno e médio porte que crescem sem nenhum profissional gerenciando a segurança da informação ainda é preocupante. Esta é uma área da tecnologia que já é indispensável, porém quando se trata de investir em tecnologias e em profissionais para gerenciá-las, o pensamento em pelo menos um terço das empresas é de que não há ainda necessidade de tais investimentos. Entretanto uma concepção que deve ser levada em conta é a de que quanto antes forem os investimentos em segurança da informação, menor serão os gastos para reparar os estragos que um invasor pode causar no futuro.

2.4 Como evitar falhas na segurança da rede

Para Beal (2005), devido à alta complexidade e ao alto custo de manter os ativos da informação salvos de ameaças à sua confidencialidade, integridade e disponibilidade são importantes à empresa adotar um enfoque de gestão baseado nos riscos específicos para o negócio. Sêmola (2003) define risco como: “a probabilidade de que agentes, que são ameaças, explorem vulnerabilidades, expondo os ativos a perdas de confidencialidade, integridade e disponibilidade e causando impacto nos negócios”. Os impactos são limitados por medidas de segurança, que ajudam a diminuir o risco. Assim, a gestão do risco é o conjunto de processos que permitem às organizações identificarem e programarem as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos. (BEAL, 2005).

Para SÊMOLA (2003), as ameaças somadas às vulnerabilidades quando mal gerenciadas facilitam o ataque a um ativo da informação. Um ataque concluído gera o incidente de segurança que culmina em um impacto para os negócios da

organização. As seguintes medidas podem ser implementadas para melhor gerenciar os riscos:

Medidas Preventivas: reduzem a probabilidade de uma ameaça se concretizar ou diminuem o grau de vulnerabilidade do ambiente, ativo ou sistema; reduzindo assim a probabilidade de um ataque e/ou sua capacidade de gerar efeitos adversos na organização. Exemplos de medidas preventivas:

Política de segurança;

Controles de acesso físicos e lógicos;

Programas de conscientização e treinamento; etc.

Métodos Detectivos: expõem ataques ou incidentes e disparam medidas reativas, tentando evitar a concretização do dano, reduzi-lo ou impedir que se repita. Exemplos de métodos detectivos:

Monitoração da rede;

Sistemas de detecção de intrusos;

Auditorias; etc.

Medidas Reativas: reduzem o impacto de um ataque ou incidente. São medidas tomadas durante ou após a ocorrência do evento. Exemplos de medidas reativas:

Ação legal;

Restauração do serviço;

Procedimentos de resposta a incidentes; etc.

2.5 Redes de computadores

2.5.1 Redes Locais (LANs)

Para Soares (1995), uma rede LAN (*Local Area Network* – Rede de Área Local) é uma rede de computadores concentrada em uma área geográfica, como por exemplo, um prédio, uma empresa, um escritório ou um campus universitário. Atualmente a grande maioria das redes empresariais e domésticas é qualificada como LAN, o acesso a Internet também é realizado através destas redes LANs. Por meio das redes LAN pode-se compartilhar o uso dos dispositivos da rede, ou até mesmo o uso de dispositivos dos *hosts* que compõem a rede, como unidades de CD/DVD, impressoras, discos rígidos entre outros.

2.5.2 Redes MANs e WANs

Segundo Soares (1995), além das redes LANs, existem outras formas de redes que se pode citar, apenas para efeito de comparação, pois não falaremos de características mais profundas de redes que não as LANs.

Redes *MANs*: (*Metropolitan Area Networks*), são redes de médio porte, redes MANs interligam redes LANs, normalmente são redes de abrangência estadual.

Redes *WANs:* *(Wide Area Network*), são redes utilizadas para interligar outras redes geograficamente distantes, as redes WAN utilizam a infraestrutura de transmissão de empresas de telecomunicações, como Copel, Embratel entre outras.

2.6 Topologia Básica da Rede

Segundo SOARES (1995) topologia é a forma como os pontos de rede se interligam, a infraestrutura utilizada para a comunicação entre dois ou mais computadores da rede.

As topologias de redes em geral têm dois tipos de comunicação, ponto a ponto e redes do tipo multiponto ou de difusão.

2.6.1 Ponto a ponto

É uma forma de comunicação exclusiva entre dois pontos (*hosts*), ou seja, se um *host* A deseja comunicar com um *host* B deve haver uma linha exclusiva entre um e outro, não possibilitando a comunicação com um terceiro *host* através desta mesma comunicação. Em redes *LANs* atuais, utilizando-se de cabos de rede do tipo par trançado dá-se o nome ao cabo que interliga dois *hosts* ponto a ponto de *crossover,* (SOARES, 1995).

2.6.2 Multiponto

Em uma rede multiponto, uma única linha de comunicação servirá na comunicação de vários *hosts* ao mesmo tempo. Obviamente o controle para isto é mais complexo, mas um *host* A poderá se comunicar com outros *hosts* (B, C, D) sem que haja a necessidade de uma linha exclusiva entre cada um deles, (SOARES, 1995).

2.7 Protocolo TCP/IP e pilhas de protocolos

Segundo a ABNT NBR ISO/IEC 17799 (2005), o TCP/IP *(Transmition Control Protocol / Internet Protocol)* é o conjunto de protocolos de comunicação ou pilha de protocolos. Desenvolvido essencialmente para resolver problemas de compatibilidade de diferentes tecnologias e plataformas no âmbito das redes Intranets e também na Internet.

Os protocolos TCP/IP podem ser utilizados sobre qualquer estrutura de rede, seja ela simples como uma ligação ponto-a-ponto ou uma rede de pacotes complexa. Como exemplo, podem-se empregar estruturas de rede como *Ethernet*, *Token-Ring,* FDDI*,* PPP*,* ATM*,* X. 25, *Frame-Relay*, barramentos SCSI, enlaces de satélite, ligações telefônicas discadas e várias outras como meio de comunicação do protocolo TCP/IP.

Para ABNT NBR ISO/IEC 17799 (2005), a arquitetura TCP/IP, assim como OSI realiza a divisão de funções do sistema de comunicação em estruturas de camadas. Em TCP/IP as camadas são: Uma arquitetura de camadas que foi desenvolvida para que as funções fossem divididas dentro de uma estrutura de comunicação em rede.

Segundo Kurose (2006), “O sistema de camadas de protocolos tem vantagens conceituais e estruturais.” segundo ele “a divisão em camadas proporciona um modo estruturado de discutir componentes de sistema”.

Camada de Rede – A camada de rede fica responsável pelo envio de datagramas construídos na camada de Inter-redes, esta camada possui um mapeamento de endereço de identificação no nível físico da rede. No caso de redes *Ethernet* cada estação possui um endereço único chamado de endereço MAC (*Media Access Control*). Pode-se citar que na camada de redes e na camada de Inter-redes do modelo TCP/IP, um protocolo muito comum utilizado é o protocolo ARP (Address Resolution Protocol), que é um protocolo de mapeamento de endereços físicos e lógicos.

Camada Inter-Rede – Esta camada é responsável pela comunicação entre máquinas vizinhas através do protocolo IP. O protocolo IP realiza a função de roteamento que consiste no transporte da mensagem entre redes e nas decisões de qual rota cada mensagem deverá seguir até seu destino.

Camada de Transporte – A camada de Transporte possui os protocolos UDP *(User Datagram Protocol*) e TCP *(Transmission Control Protocol*). Esta camada reúne os protocolos que realizam as funções de transporte de dados fim-a-fim, considerando apenas a origem e destino da comunicação, sem se preocupar com os elementos intermediários.

Camada de Aplicação – A camada de aplicação reúne os protocolos que fornecem serviços de comunicação ao sistema ou ao usuário. Esta camada possui a comunicação direta entre a aplicação propriamente dita, como exemplo o sistema operacional, e as camadas mais baixas.

Modelo OSI - A arquitetura TCP/IP difere e muito do modelo OSI, devido fato de que a arquitetura TCP/IP agrupa como subcamadas, as camadas utilizadas no modelo OSI.

Para a ABNT NBR ISO/IEC 17799, (2005), as principais diferenças são: O Modelo OSI que trata todas as camadas, enquanto TCP/IP apenas a partir do nível de rede do modelo OSI*;* TCP/IP é largamente compatível com diversos modelos de arquiteturas, enquanto OSI não; OSI oferece serviços orientados à conexão no nível de rede, o que demanda um trabalho e uma inteligência muito maior, já o TCP/IP tem uma função muito simples de roteamento.

Segundo ABNT NBR ISO/IEC 17799 (2005), os protocolos TCP/IP tratam os níveis superiores de forma monolítica, desta forma OSI é mais eficiente, pois oferece reaproveitamento de funções comuns a diversos tipos de aplicação, o TCP/IP necessita montar uma estrutura completa para cada tipo de aplicação.

2.8 Roteamento de rede e Protocolos de Roteamento

Para Kurose (2006), uma das funções principais da camada de rede é prover o roteamento dos pacotes que transitam em rede. “A camada de rede deve determinar a rota ou o caminho tomado pelos pacotes ao fluírem de um remetente a um destinatário”.

O papel de um roteador é definir qual será a rota que aquele pacote deverá seguir, utilizando o conceito de repasse, ou seja, o pacote de dados chegará através de uma das portas do roteador, e o mesmo se encarregará em repassar este pacote para outra porta, usando uma tabela de rotas que pode ser estática (definida

manualmente), ou dinâmica (utilizando um protocolo que crie esta tabela dinamicamente) (KUROSE, 2006).

Segundo Kurose (2006), para que o rota seja definida, os roteadores realizam os cálculos das métricas através de um algoritmo de roteamento, que irá definir o melhor caminho para enviar aquele pacote. A métrica é o padrão de medida que é usado pelo algoritmo de roteamento, que utilizará um ou vários parâmetros para definir a rota, entre os parâmetros mais comuns encontram-se:

- Tamanho do caminho;
- Confiabilidade;
- Atraso;
- Largura de Banda;
- Carga;
- Custo da comunicação.

Roteamento Estático: No roteamento estático as tabelas de rotas são construídas manualmente, atribuído a redes pequenas com um número limitado de roteadores. As rotas podem ou não serem divulgadas para outros dispositivos, sendo que a não divulgação é uma das características positivas deste tipo de roteamento devido ao aumento da segurança. Outro ponto positivo é que as tabelas estáticas diminuem o *overhead* introduzido pela troca de mensagens de roteamento na rede, (SOARES, 1995).

Roteamento Dinâmico: O roteamento dinâmico ocorre quando há mais de uma rota possível para o mesmo ponto, desta forma uma tabela de rotas é construída automaticamente a partir da troca de informações dos protocolos de roteamento. Os protocolos de roteamento mais comuns são RIP e seu sucessor OSPF, o IGRP, BGP entre outros, (SOARES, 1995).

3. PROCEDIMENTOS METODOLÓGICOS

Observando os critérios para classificação de pesquisas propostos por Marconi e Lakatos (2011, p.69), quanto à área de conhecimento, esta pesquisa tem como finalidade demonstrar o cenário de segurança da informação das instituições de ensino que ofertam o nível fundamental II, médio ou superior da rede pública estadual, federais e privadas da cidade de Porto Nacional – TO.

Quanto à metodologia utilizada, a pesquisa é de levantamento (*survey*), método exploratório-descritivo, com pesquisa bibliográfica e de campo, conforme definições de Marconi e Lakatos (2011, p.69). Bervian e Silva (2007, p.53), no que diz respeito a questionários, afirmam que “é a forma mais usada para coletar dados, pois possibilita medir com mais exatidão o que se deseja [...] meio de obter respostas às questões por uma fórmula que o próprio informante preenche”.

3.1 Plano de Coleta de Dados

Segundo o site QEdu (2016), existem na cidade de Porto Nacional – TO, 17 escolas públicas estaduais de ensino médio básico, 2 escolas privadas de ensino médio básico, 2 de ensino superior privadas e 2 de ensino superior públicas federais, num total de 23 instituições educacionais. Sendo assim foi aplicado um questionário entre os meses de junho a dezembro de 2017, em 20 instituições de ensino desta cidade. A confiabilidade da amostra é de 90%, com margem de erro de 6,81%.

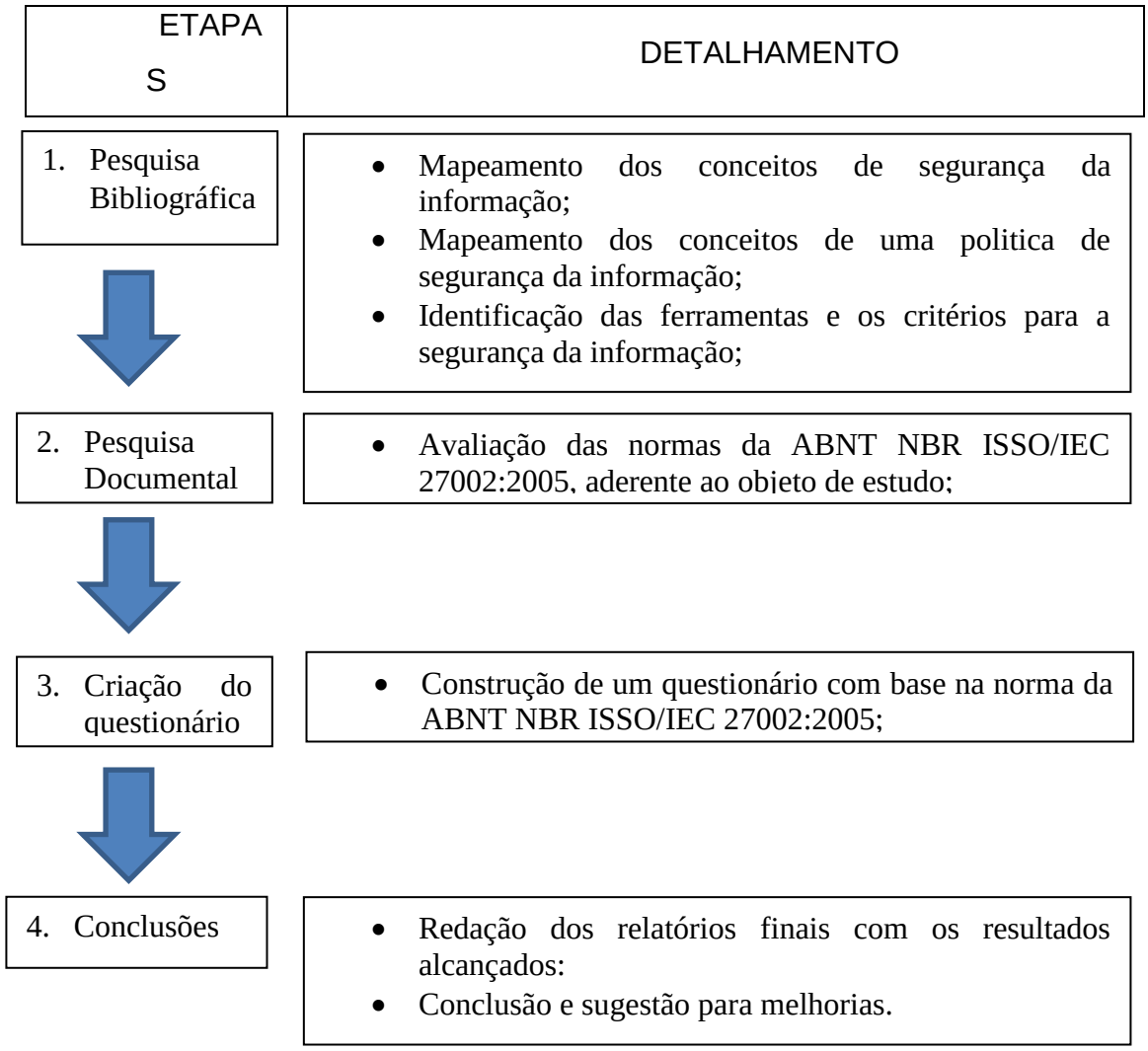
Tabela 01 – Instituições pesquisadas

NOME DA INSTITUIÇÃO	PÚB.	PRIV.	FUND.II	MÉDIO	SUPER.
COL. EST. ALFREDO NASSER	X	-	X	X	-
COL. EST. PEDRO L. TEIXEIRA	X	-	X	X	-
COL. EST. M. ANGÊLICA ARANHA	X	-	X	X	-
COL. EST. CEM FLORÊNCIO AIRES	X	-	X	X	-
COL. EST. CEM FELÌZ CAMOA	X	-	X	X	-
COL. EST. M. ARTUR COSTA E SILVA	X	-	X	X	-
ESC. EST. CARMENIA MATOS MAIA	X	-	X	X	-
ESC. EST. ALC. RODRIGUES AIRES	X	-	X	-	-
ESC. EST. FREI ALDRIN	X	-	X	-	-
ESC. EST. IRMA ASPÁSIA	X	-	X	-	-
ESC. EST. DOM PEDRO II	X	-	X	-	-
ESC. EST. DOM DOMI. CARRERONT	X	-	X	-	-
ESC. EST. ANA MACEDO MAIA	X	-	X	-	-
ESC. EST. CUST. DA SILVA PEDREIRA	X	-	X	-	-
IFTO – *CAMPUS* PORTO NACIONAL	X	-	-	X	X
UFT – *CAMPUS* PORTO NACIONAL	X	-	-	-	X
COL. SAGRADO C. DE JESUS	-	X	X	X	-
ESCOLA PRISMA E FAC. UNOPAR	-	X	X	-	X
FACULDADE FASAMAR	-	X	-	-	X
ITPAC – PORTO NACIONAL	-	X	-	-	X

Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

Gil (2002) considera que o levantamento é o procedimento técnico mais adequado a ser utilizado em pesquisas descritivas, visto que “procede-se à solicitação de informações a um grupo significativo de pessoas acerca do problema estudado para, em seguida, mediante análise quantitativa, obterem-se as conclusões correspondentes aos dados coletados”. Para Appolinário (2006), o levantamento “tem por finalidade investigar as características de determinada realidade ou mesmo descobrir as variáveis componentes dessa realidade”. GIL (2002) acrescenta que os levantamentos trazem as seguintes vantagens: conhecimento direto da realidade (evita subjetivismo dos pesquisadores), economia e rapidez (dados obtidos por questionários têm custos relativamente baixos), quantificação (possibilidade de análise estatística, com o uso de correlações e outros procedimentos). A aplicação do questionário seguiu as etapas da pesquisa, conforme demonstrado no diagrama a seguir.

Figura 2: Diagrama das etapas da pesquisa



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

Conforme Gil (2010, p.113) esclarece, “o processo de análise de dados envolve diversos procedimentos; codificação das respostas, tabulação dos dados e cálculos estatísticos”. Mais ainda, Gil (2010, p.113) afirma que “após, ou juntamente com a análise, pode ocorrer também à interpretação dos dados, que consiste, fundamentalmente, em estabelecer a ligação entre resultados obtidos com os já conhecidos”.

Foram entrevistados funcionários das instituições de ensino responsáveis por cuidar dos assuntos relacionados à área de T.I, sendo eles profissionais de T.I ou apenas pessoas com algum conhecimento sobre o assunto.

O questionário de pesquisa foi aplicado com um total de 20 questões relativas à segurança da informação, sendo 10 questões sobre informações gerais

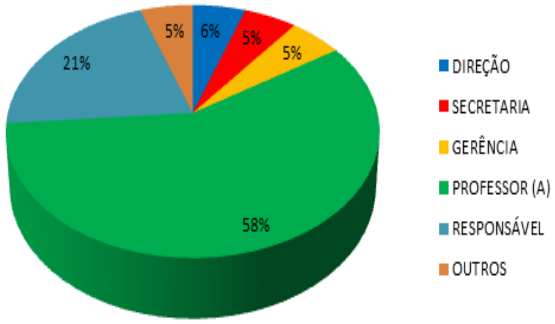
da instituição e 10 sobre informações técnicas específicas de grande relevância no contexto deste trabalho.

Para análise dos resultados foram realizados procedimentos de estatística descritiva para verificação de significância dos dados através de procedimentos de amostragem, coleta e validação dos dados, utilizando *software* apropriado. O questionário aplicado na amostra é apresentado no Apêndice A.

4. APRESENTAÇÃO E ANÁLISE DOS DADOS

Entre as pessoas que responderam o questionário, 21% são profissionais da área de T.I, 58% são professores que ocupam cargos de gerenciamento ou responsabilidade pelo setor. Em 6% dos casos a direção é a responsável pelo departamento de T.I. Secretarias, gerências e outros são responsáveis pela T.I. em 5% cada, somando 15% dos casos.

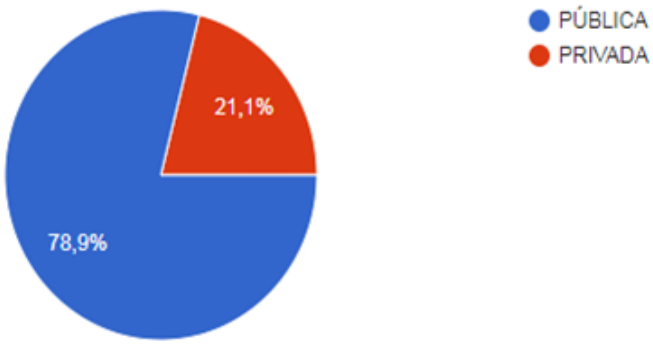
Gráfico 01 – Qual sua função na instituição de ensino?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

O gráfico 02 apresenta os resultados quanto à categoria administrativa das escolas pesquisadas. 78,9% são instituições de ensino públicas e 21,1% pertencem ao setor privado. Para essa amostra foram pesquisadas apenas as que ofertam ensino fundamental II, médio ou superior.

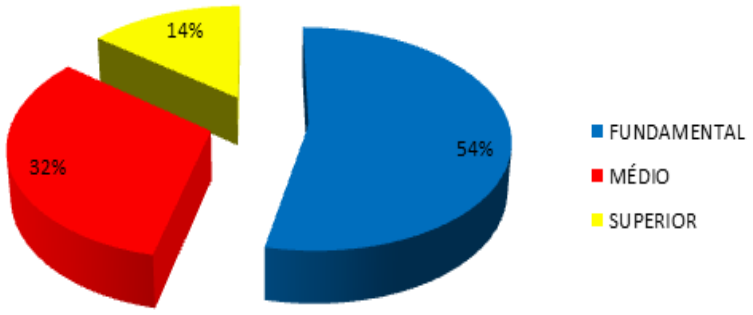
Gráfico 02 – A instituição de ensino é pública ou privada?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

O gráfico a seguir apresenta quais modalidades de ensino são ofertadas por estas instituições.

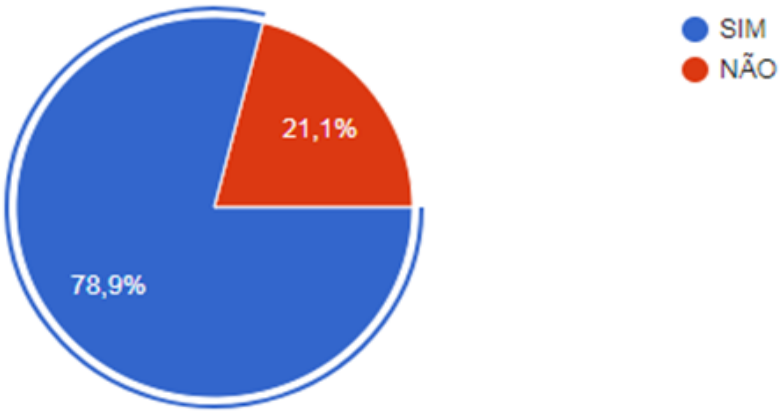
Gráfico 03 – A instituição oferece ensino fundamental, médio ou superior?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

O próximo gráfico mostra que a maioria das instituições possui laboratório de informática.

Gráfico 04 – A instituição possui laboratórios de informática?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

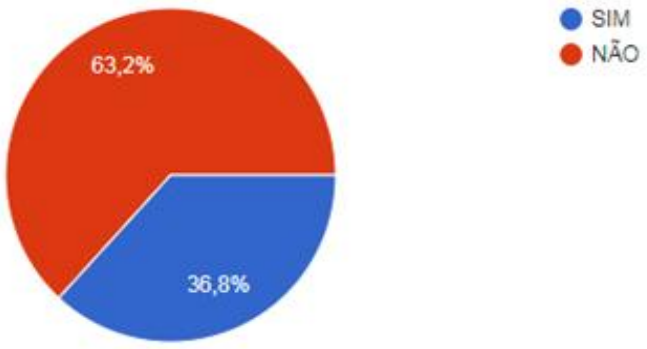
O gráfico 05 apresenta a informação de que as instituições possuem um lugar específico para guardar ou armazenar com segurança seus equipamentos de redes.

Gráfico 05 – A Instituição possui armários ou *racks* para abrigar os equipamentos de informática e de transmissão de dados de Intranet ou Internet?

Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

O gráfico 06 demonstra que a maioria das instituições pesquisadas não possui profissionais preparados ou capacitados a cuidar dos serviços de manutenção dos serviços relacionados à área de T.I.

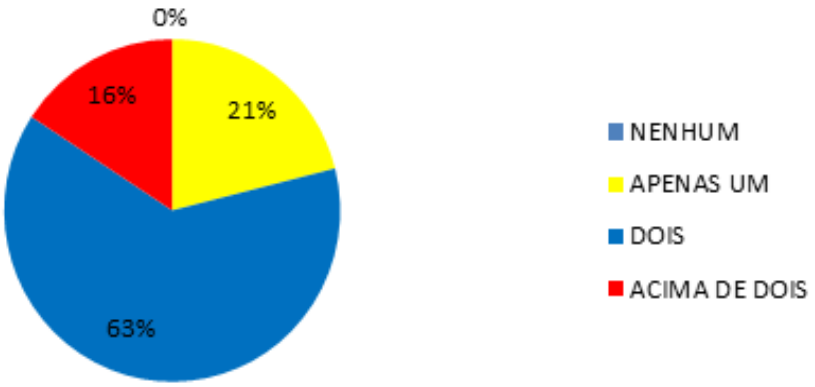
Gráfico 06 – A instituição possui funcionários capacitados para cuidar da manutenção dos serviços de T.I?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

O gráfico 07 mostra que mais da metade das instituições possui mais de um *link* de acesso a Internet.

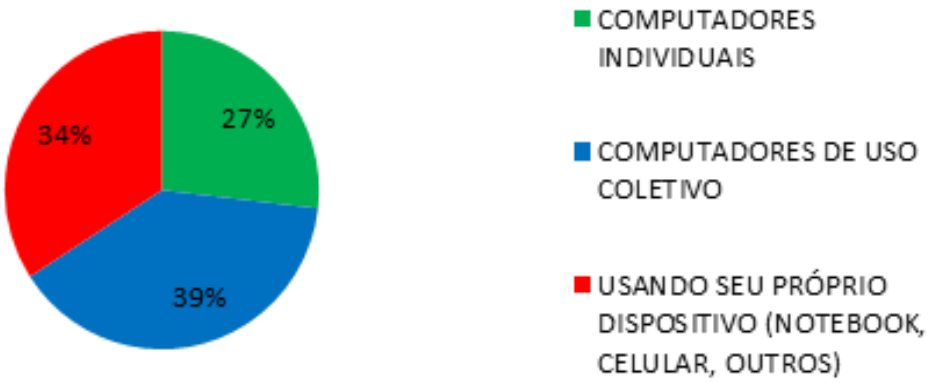
Gráfico 07 – A instituição oferece acesso à Internet? Marque o número de *links* (provedores) de acesso.



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

O gráfico 08 apresenta a forma de acesso à informação dentro das instituições para seus funcionários e colaboradores. A maioria tem que usar computadores de uso coletivo.

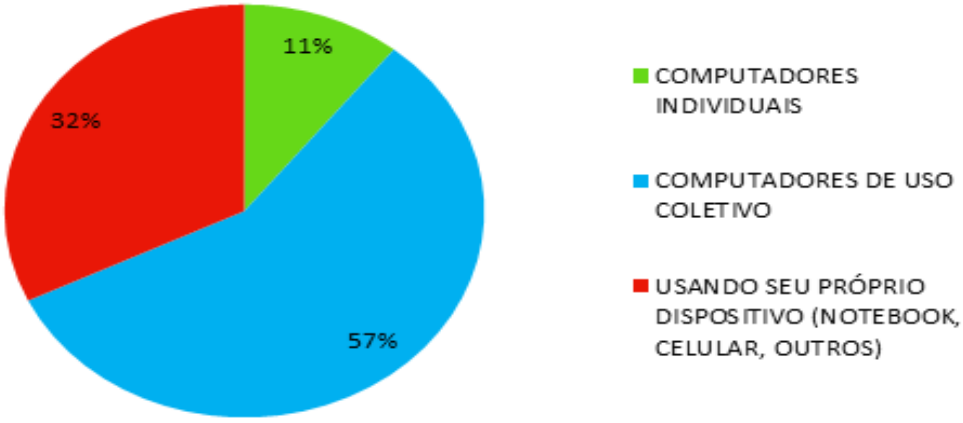
Gráfico 08 – Quais formas de acesso à informação e Internet a instituição oferece aos funcionários e colaboradores?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

O gráfico a seguir mostra que o acesso à informação dentro das instituições, para os estudantes, não é muito diferente dos colaboradores e professores. A maioria usa computadores de uso coletivo, com poucas opções de usar um computador individual.

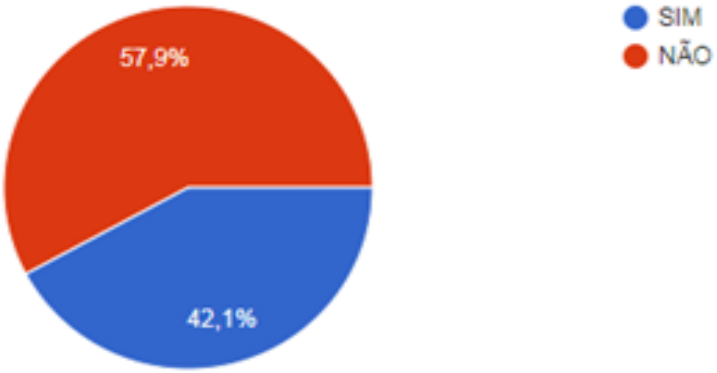
Gráfico 09 – Quais formas de acesso à Internet a instituição oferece aos estudantes?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

O gráfico a seguir demonstra que as pessoas entrevistadas consideram que o valor investido no espaço e infraestrutura não é satisfatório para suprir as necessidades da instituição oferecendo qualidade e segurança das informações.

Gráfico 10 – Você considera o grau de investimento da instituição em *HARDWARE e SOFTWARE* suficiente para suprir as necessidades organizacionais com segurança?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

De acordo com a norma ABNT NBR ISO/IEC 17799 (2005), uma política de segurança não estará completa se não houver controle dos acessos às informações armazenadas em meios computacionais e dispositivos que permitam a comunicação ou transmissão de informação digital, visto que é dentro dos computadores e dispositivos móveis que as pessoas estão sempre conectadas. Da mesma forma

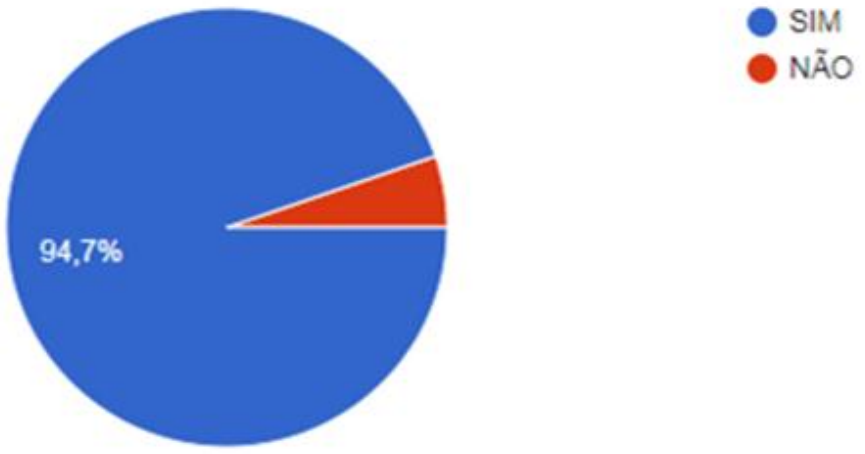
como os procedimentos de segurança refletem as linhas da política de segurança, o *software* de segurança escolhido para monitorar e controlar os acessos ao ambiente de informações residentes nas redes de computadores segue os procedimentos que foram desenvolvidos com base na política de segurança.

> A segurança de uma rede pode ser comparada à segurança de uma casa. Não importa que grau de segurança exista, não importa que sistemas ou trancas sejam usados. Quando alguém decide com suficiente empenho, invadir provavelmente terá êxito. De modo análogo, todas as medidas no sentido de se aumentar a segurança de uma rede tem como objetivo torna-la tão segura quanto possível já que nenhum sistema conhecido garante o estado – da – arte em termos de proteção. Geralmente, um atacante irá analisar a relação custo/benefício, ou seja, o quão custoso e complicado será invadir um determinado sistema ponderado aos lucros que ele alcançará com tal invasão. Uma vez que esta proporção se torne inviável, pode-se dizer que foi atingido um bom grau de segurança (BONIFÁCIO, 1998).

Segundo Soares (1995), uma política de segurança é um conjunto de leis, regras e práticas que regulam como uma organização gerencia protege e distribui suas informações e recursos. A seguir apresentar-se-ão os resultados referentes à segunda parte do questionário aplicado, que corresponde às perguntas técnicas sobre segurança da informação.

Conforme apresenta o gráfico abaixo, 94,7% dos entrevistados disseram conhecer ou já ter ouvido falar em normas de segurança da informação, provando estar ciente dos riscos relacionados a não aplicação de políticas de segurança dentro da instituição de ensino.

Gráfico 11 – Você tem conhecimento ou já ouviu falar sobre normas de segurança da informação ou segurança de sistemas?

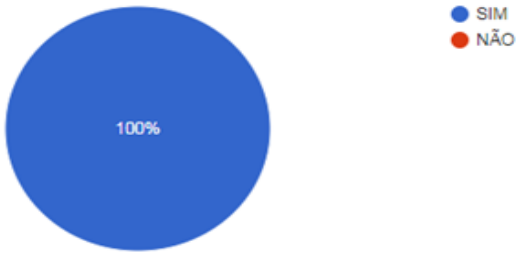


Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

O gráfico abaixo mostra que os usuários dão uma garantia de 100% em conhecimento dos riscos relativos ao acesso indevido, pois os recursos a serem protegidos pelos controles de acesso físicos são os equipamentos, a documentação e suprimentos.

A proteção física desses recursos constitui-se em uma barreira adicional e anterior às medidas de segurança de acesso lógico. Pode se dizer que os controles de acesso físico protegem os lógicos (ABNT NBR ISO/IEC 17799, 2005).

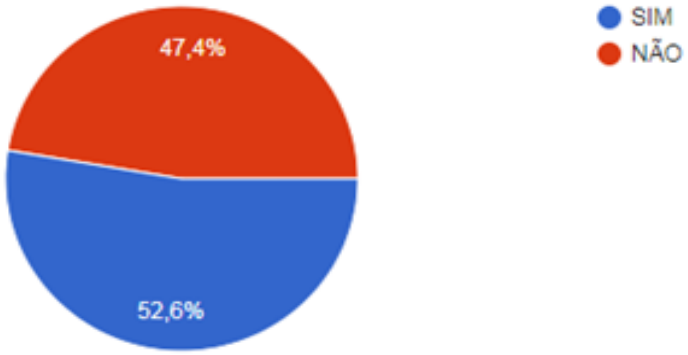
Gráfico 12 – Você conhece os riscos relativos à segurança, tais como perda de informações importantes, ataques e acessos indevidos?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

O gráfico abaixo mostra que apenas um pouco mais da metade das instituições entrevistadas tem uma regra ou controle que se aplique aos sistemas informatizados.

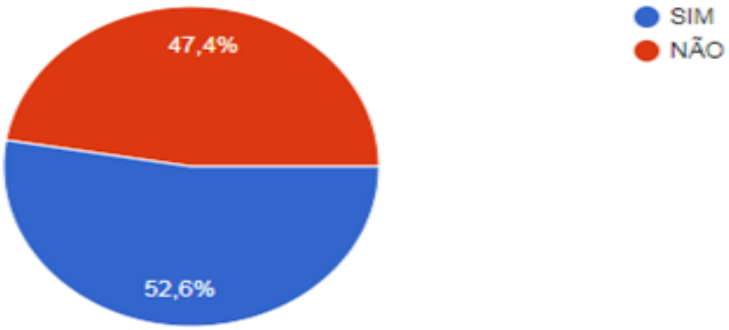
Gráfico 13 – A instituição possui alguma regra, norma ou política de segurança que se aplique aos sistemas de informação?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

O gráfico mais abaixo mostra tamanha necessidade de quase a metade das instituições pesquisadas precisar entender que os controles de acesso físico têm como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos. Apenas pessoas autorizadas pelo responsável por aquele departamento podem ter acesso físico aos sistemas de computadores (ABNT NBR ISO/IEC 17799, 2005).

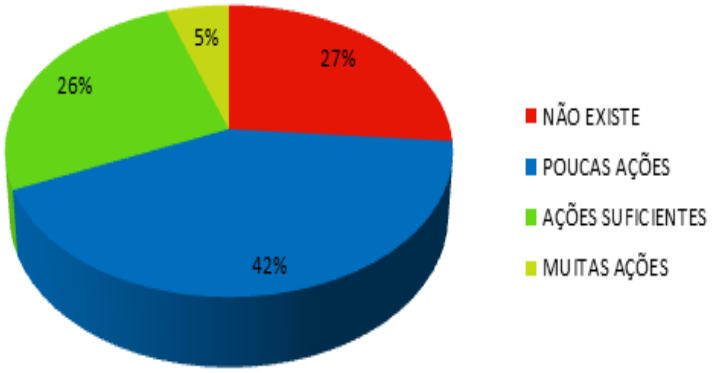
Gráfico 14 – Existe(m) pessoas(s) responsável(eis) pela segurança física (*HARDWARE*) e lógica (*INFORMAÇÃO*) dos sistemas da instituição?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

Segundo Kurose (2006), para que possamos estabelecer uma conexão de forma segura é desejável que exista sempre ações que venham a manter e preservar a qualidade de uso dos equipamentos. Conforme mostra o gráfico abaixo não é isso que vem acontecendo na maioria das instituições de ensino de Porto Nacional.

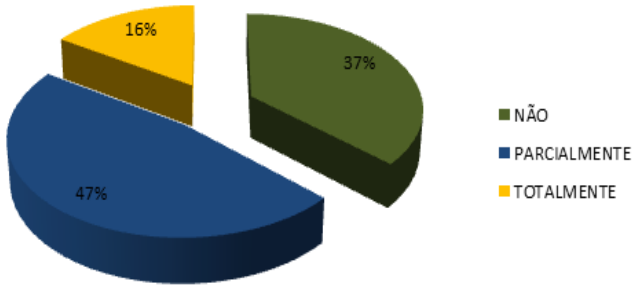
Gráfico 15 – Existem ações da instituição no sentido de conscientizar, educar e treinar os colaboradores e estudantes para uma utilização e manutenção segura dos sistemas de informação?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

Partindo de um princípio lógico sobre segurança em rede de computadores, pode-se afirmar que a segurança está na preservação dos dados mantidos nos elementos que integram esta rede (KUROSE, 2006). Conforme apresenta o gráfico abaixo, não existe um bom controle por parte da maioria das instituições no sentido de monitoramento do uso da rede para, assim preservar a integridade dos dados.

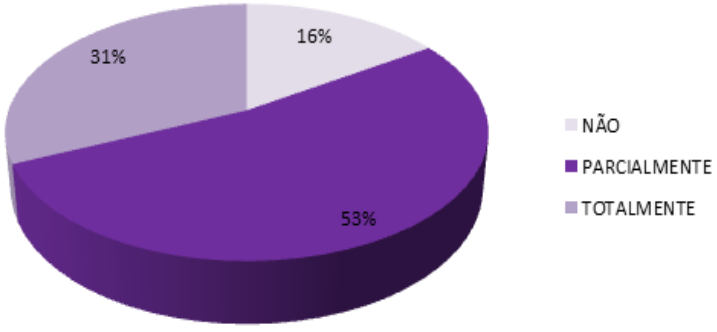
Gráfico 16 – A instituição monitora o uso dos serviços de rede (*web, e-mails, downloads*, redes sociais, outros aplicativos) pelos usuários?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

O gráfico abaixo apresenta que poucas são as instituições de ensino que possuem um controle adequado de acesso à rede por meio de autenticação de segurança, bem como dificilmente possuem uma gerência destes acessos, ou seja, não se sabe ao certo quem esta usando a rede, se este usuário é um colaborador ou um intruso, se algum usuário esta realizando acessos a locais indevidos, ou o que o usuário esta acessando na Internet.

Gráfico 17 – Existe algum tipo de monitoramento e/ou controle de acesso aos recursos físicos (*Hardware*) e lógicos (*Softwares*) dos sistemas de informação?



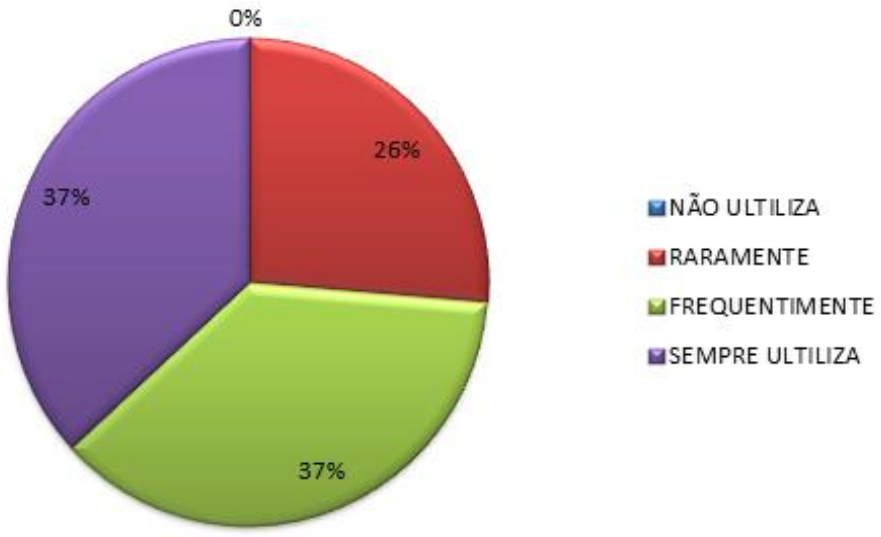
Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

Segundo Melo (2003), as políticas de segurança de sistemas se diferem em três ramos principais: segurança física, segurança gerencial e segurança lógica.

- **Segurança física –** trata-se da segurança física do sistema, o meio físico em que o sistema se sustenta. Que define as medidas de segurança contra desastres como: alagamentos, terremotos, incêndios, ou qualquer evento natural que venha prejudicar ou interromper o funcionamento dos sistemas. Bem como as restrições e delimitações de acesso aos equipamentos e etc.
- **Segurança gerencial –** trata-se do ponto de vista estratégico organizacional, definindo os processos, normatizando e gerenciando as tomadas de decisão.
- **Segurança lógica –** trata-se das definições de segurança no nível da aplicação, como permissões de usuários, direitos e monitoramentos das atividades.

Quando questionados sobre a utilização de algum meio de proteção e se ele era usado com frequência, uma boa parte dos entrevistados respondeu não utilizar sempre esses recursos.

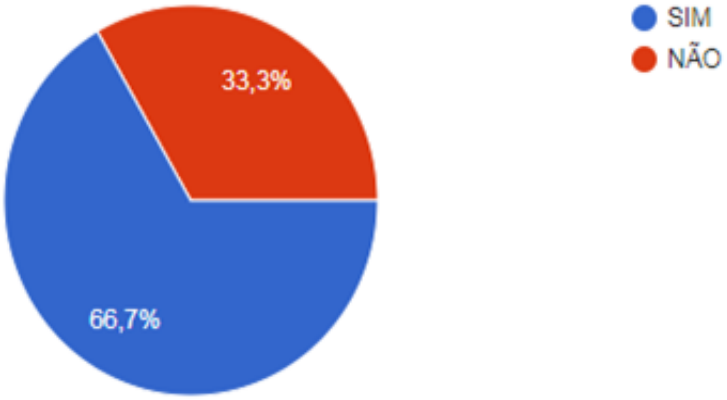
Gráfico 18 – A instituição utiliza ferramentas de segurança da informação, tais como antivírus, *ANTI-SPAM, FIREWALL, PROXY* e outras?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

Conforme o gráfico abaixo a maioria das instituições pesquisadas tem seu próprio *site,* que significa ter mais uma ferramenta de divulgação de seu trabalho, mais uma ferramenta para se proteger a integridade dos dados.

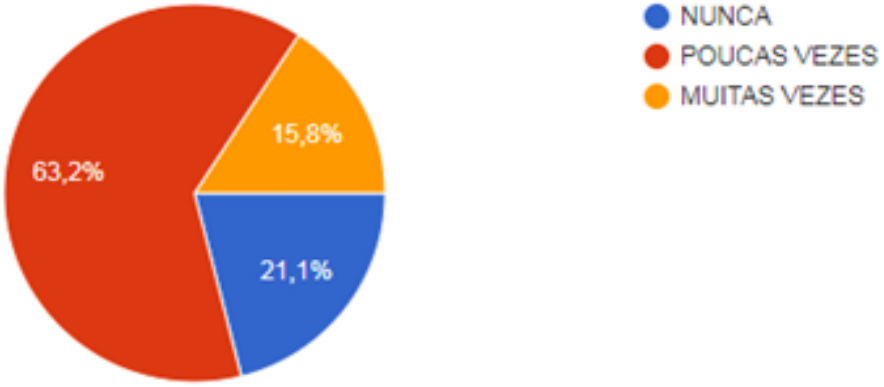
Gráfico 19 – A instituição possui *website* próprio?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

No gráfico abaixo, percebe-se que as instituições em sua maioria já sofreram alguns tipos de incidentes, como os ataques de vírus.

Gráfico 20 – A instituição já registrou a ocorrência de incidentes de segurança da informação, tais como vírus, ataques, acesso indevidos, golpes, fraudes, furtos de informações ou equipamentos?



Fonte: Elaborada pelo autor, com base nos dados do questionário aplicado (2017).

4.1 Uma proposta para melhoria da segurança de redes

Segurança da informação é uma pauta que não deve estar fora das reuniões das organizações. A principal tarefa deste trabalho foi criar uma ferramenta simples, em forma de questionário (ver Apêndice A), para que qualquer organização possa verificar sua aderência com a segurança da informação de acordo com as normas brasileiras (ABNT NBR ISO/IEC 27002, 2005).

A pesquisa aponta claramente que as instituições de ensino tanto públicas quanto privadas da cidade de Porto Nacional – TO são deficientes quanto a possuírem uma política de segurança ou regras de acesso à rede, bem como em possuir departamento específico para monitorar ou gerenciar os recursos de T.I. Existe então a necessidade imediata de desenvolver nessas instituições políticas de segurança com normas simples, que contemplem as necessidades primordiais da organização. Essa política pode ser orientada por algumas características básicas, a seguir:

- Criação de uma implementação de fácil administração. Desenvolver e publicar as diretrizes de uso aceitável dos recursos de T.I., com a ciência de todos.
- Criar e reforçar o uso de ferramentas de segurança apropriadas, sendo configuradas e orientadas pelas necessidades apontadas pela análise de um profissional capacitado na área de Tecnologia da Informação.
- Deve definir claramente as áreas de responsabilidade para os usuários, administradores, gerência ou responsável pelo departamento/segmento.

Os componentes básicos de uma boa política de segurança incluem:

- Uma política de acesso que define direitos de acesso e privilégios necessários para proteger os recursos da rede, bem como o acesso a dispositivos da rede, dispositivos móveis pessoais, mídias em ROM, horários de uso dos equipamentos, instalação de aplicativos, adição de atualizações ou aplicativos de uso pessoal, busca de diretórios compartilhados não pertinentes ao uso especificamente profissional ou educacional;
- Uma política que defina as responsabilidades dos usuários, bem como a capacidade de auditoria caso seja constatada uma falha na segurança;
- Uma política de autenticação de usuários, bem como as diretrizes sobre o uso individual das senhas utilizadas na rede ou aplicações que a instituição possua. Também a especificação das características mínimas exigidas para a criação de senhas e o tempo de expiração das mesmas;
- Uma política de definição de disponibilidade da rede, bem como suas redundâncias e as capacidades de *backup* que a rede possui;
- Uma declaração de horários de manutenção, previsões para solução de problemas pertinentes a rede ou aos usuários especificamente. Muito importante

é a informação das manutenções realizadas de forma remota, onde o administrador ou técnico terá acesso e controle total ao equipamento;

- Informações claras e objetivas do que está sendo monitorada na rede, uma política de controle e monitoramento de informações que trafegam pela rede através de *e-mail*, mensageiros instantâneos, acessos a sites, *downloads* realizado, tempo de acesso e permanência em *sites*.

E obviamente uma política descrevendo os direitos de usuários e da instituição, bem como procedimentos reativos da instituição, caso sejam encontradas violações das normas pelos usuários da rede, bem como a eleição de um foro judicial caso seja constatado crime cibernético ou espionagem por parte de colaboradores, alunos da própria instituição de ensino ou usuário externo que venha a usar o equipamento.

5. CONSIDERAÇÕES FINAIS

Redes de computadores têm a finalidade de possibilitar o relacionamento e interação de pessoas através do compartilhamento dos recursos disponíveis em cada componente da própria rede. Facilitam o acesso à informação privada ou pública e o seu compartilhamento. Atualmente o uso da Internet permite o acesso a um ilimitado conteúdo e a realização de ações que vão do simples entretenimento aos mais complexos procedimentos operacionais de forma remota. Esse meio de comunicação inovador, virtual, que tende a cada vez mais se tornar acessível, interativo, funcional e ilimitado, reproduz todos os riscos e ameaças do mundo real.

Segurança é um assunto que deveria preocupar a todos, seja no setor público ou no privado. Nas instituições de ensino de Porto Nacional – TO o ambiente virtual não é diferente. Faz- se então necessário tomar precauções para garantir a integridade das informações e preservar os recursos e a privacidade de usuários e instituição. As falhas de segurança podem incluir riscos como, por exemplo, possibilitar a usuários mal intencionados ou atacantes vantagens ilícitas; possibilidade de alterar dados estudantis, financeiros e administrativos; causar danos ao sistema e a terceiros; e outros.

Na era digital a informação pode ser muito valiosa, e em mãos erradas pode ser utilizada de forma inconsequente ou maliciosa, causando grandes prejuízos a instituições e pessoas. Por isso, é essencial utilizar a tecnologia a nosso favor, a fim de tornar o ambiente virtual protegido e um lugar mais seguro, no qual as partes possam utilizá-la para desempenhar suas atividades e processos sem o temor de que ocorram perdas e prejuízos sejam eles psicológicos, financeiros, tecnológicos, morais entre outros.

As políticas de segurança, tendo como propósito minimizar a vulnerabilidade de bens e recursos, atualmente são os principais instrumentos utilizados para tentar garantir a segurança a um conjunto de dados e a infraestrutura que os suportam, a fim de preservar seu valor de informação. Por isso, essa é a ferramenta mais adequada para obter-se confidencialidade, autenticidade, integridade, disponibilidade e controle de acesso nas redes de computadores por todo o mundo.

As políticas de segurança evitam a proliferação de códigos maliciosos; diminuem acessos não permitidos; definem mecanismos de criptografia,

monitoramento de tráfego, análises de ameaças e vulnerabilidades; selecionam ferramentas de segurança tais como *firewalls*, antivírus e *proxies* e muito mais.

Em Porto Nacional - TO, as instituições de ensino, embora comprovadamente não muito engajadas nas questões de segurança interna da informação, caminham para uma melhora significativa das ações relacionadas ao tema. Seja devido a grande ocorrência de incidentes de segurança, que impulsionam as instituições reativamente, seja pela conscientização promovida pela própria mídia, inclusive a Internet, através de organismos como o Centro de Tratamento e Resposta a Incidentes de Segurança, CERT.br.

Entretanto, presume-se relevante considerar também que as próprias instituições de ensino são responsáveis por essa conscientização, por motivos óbvios. Sendo assim elas deveriam tomar a dianteira dessas ações. Para isso a sociedade necessita de políticas públicas que contemplem com mais seriedade as questões relacionadas à segurança da informação nas instituições. Isso requer mobilização e vontade política, mas necessita também de embasamento teórico. Um dos objetivos específicos dessa pesquisa é exatamente apresentar dados que possam colaborar com essas iniciativas.

Para trabalhos futuros, sugere-se estender geograficamente essa pesquisa, determinando indicadores microrregionais ou estaduais. Ou buscar explicações mais detalhadas para a ausência de maiores investimentos em segurança da informação e redes, por parte de tais instituições de ensino.

REFERÊNCIAS

ABNT NBR ISO/IEC 17799. NBR ISO/IEC 17799–**Tecnologia da informação—Técnicas de segurança—Código de prática para a gestão da segurança da informação**, 2001.

ABNT NBR ISO/IEC 17799. NBR ISO/IEC 17799–**Tecnologia da informação—Técnicas de segurança—Código de prática para a gestão da segurança da informação,** 2005.

ABNT NBR ISO/IEC 27001. NBR ISO/IEC 27001 - **Sistema de Gestão de Segurança da Informação – Requisitos,** 2013.

ABNT NBR ISO/IEC 27002. NBR ISO/IEC 27002 - **Tecnologia da informação - técnicas de segurança - código de prática para a gestão da segurança da informação,** 2015.

ABNT NBR ISO/IEC 27002. NBR ISO/IEC 27002 - **Tecnologia da informação - técnicas de segurança - código de prática para a gestão da segurança da informação,** 2013.

APPOLINÁRIO, Fabio. **Metodologia da Ciência: filosofia e prática da pesquisa** – São Paulo: Pioneira Thomson Learning, 2006.

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

BONIFÁCIO Jr. J. M.; CASIAN. A.M.; CARVALHO. A.C.P.L.; MOREIRA , E.S. **Um Ambiente de Segurança Distribuição para a Integração de *Firewalls* com Sistemas de Detecção de Intrusão. In; XVI Brazilian Symposium on Computer Network,** SBRC'98, Rio de Janeiro, 1998.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa** – São Paulo: Atlas, 2002.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

INFOWESTER, **Segurança na Internet,** 2018. Disponível em https://www.infowester.com/firewall.php,> Acessado em: 13 de jan. 2018.

KANE, P.V.I.R.U.S protection: **Vital Information Resources Under Sieger**. New York: Bantam Book, 1989.

KUROSE, James; ROSS, Keith. **Rede de computadores e a internet: Uma abordagem top-down**. 3.ed. São Paulo: Pearson Addison Wesley, 2006.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Técnicas de pesquisa: planejamento e execução de pesquisas, amostragens e técnicas de**

pesquisas, elaboração, análise e interpretação de dados. 7 ed. São Paulo: Atlas, 2008

MELLO, Ivo Soares. **Administração de Sistemas de Informação**. 3 ed. São Paulo: Pioneira Thomson Learning, 2006.

MOREIRA, Stringasci Nilton. **Segurança mínima; uma visão coorporaiva da segurança de informações**. Rio de Janeiro: Axcel Books, 2001.

QEdu, **Use dados, Transforme a educação**, 2016; Disponível em <http://www.qedu.org.br/cidade/2558-porto-nacional/ideb>, Acessado em: 21 jan. 2018.

SCHNEIER, Bruce. **Segurança.com: segredos e mentiras sobre a proteção na vida digital** – Rio de Janeiro: campus, 2001.

SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva – Rio de Janeiro: Campus, 2003.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores das LANs, MANs e WANs às Redes ATM.** 2.ed. Rio de Janeiro: Campus, 1995.

WESTPHALEN, Frederico. et. **Redes de computadores,** Al.Franciscatto, Roberto. / Roberto Franciscatto, Fernando de Cristo, Tiago Perlin. – Frederico Westphalen: Universidade Federal de Santa Maria, Colégio Agrícola de Frederico Westphalen, 2014.116 p.: il.; 28 cm. ISBN: 978-85-63573-46-9, 2014.

APÊNDICE

UMA PROPOSTA DE SEGURANÇA DA INFORMAÇÃO PARA AS INSTITUIÇÕES DE ENSINO DE PORTO NACIONAL - TO.

QUESTIONÁRIO

Informações Gerais

Favor marcar com um X somente em uma única resposta que melhor se apresente para você.

1 – Qual sua função na instituição de ensino?

( ) Direção ( ) Secretaria ( ) Gerência ( ) Professor(a)

( ) Responsável pela TI ( ) Outros.

2 – A instituição de ensino é pública ou privada?

( ) Pública ( ) Privada

3 – A instituição oferece ensino fundamental, médio ou superior? (permitido marcar mais de uma opção).

( ) Fundamental ( ) Médio ( ) Superior

4 – A instituição possui laboratórios de informática?

( ) Sim ( ) Não

5 – A Instituição possui armários ou racks para abrigar os equipamentos de informática e de transmissão de dados de Intranet ou Internet?

( ) Sim ( ) Não

6 – A instituição possui funcionários capacitados para cuidar da manutenção dos serviços de TI?

( ) Sim *( ) Não*

7 – A instituição oferece acesso à internet? Marque o número de links (provedores) de acesso.

( ) 0 *( ) 1* *( ) 2* *( ) mais de 2*

8 – Quais formas de acesso à informação e Internet a instituição oferece aos funcionários e colaboradores? (permitido marcar mais de uma opção).

( ) Computadores individuais

( ) Computadores de uso coletivo

( ) Usando os próprios computadores (notebooks, celulares, outros)

9 – Quais formas de acesso à Internet a instituição oferece aos estudantes? (permitido marcar mais de uma opção).

( ) Computadores individuais

( ) Computadores de uso coletivo

( ) Usando os próprios computadores (notebooks, celulares, outros)

10 – Você considera o grau de Investimento da instituição em hardware e software suficiente para suprir as necessidades organizacionais com segurança?

( ) Sim *( ) Não*

Informações Técnicas

Favor marcar com um X somente em uma única resposta o que a instituição tem a oferecer para os usuários da rede local.

1 – Você tem conhecimento ou já ouviu falar sobre normas de segurança da informação ou segurança de sistemas?

( ) Sim ( ) Não

2 – Você conhece os riscos relativos à segurança, tais como perda de informações importantes, ataques e acessos indevidos?

( ) Sim ( ) Não

3 – A instituição possui alguma regra, norma ou política de segurança que se aplique aos sistemas de informação?

( ) Sim ( ) Não

4 – Existe(m) pessoa(s) responsável (eis) pela segurança física (hardware) e lógica (informação) dos sistemas da instituição?

( ) Sim ( ) Não

5 – Existem ações da instituição no sentido de conscientizar, educar e treinar os colaboradores e estudantes para uma utilização e manutenção segura dos sistemas de informação?

( ) não existe ( ) poucas ações ( ) ações suficientes ( ) muitas ações

6 – A instituição monitora o uso dos serviços de rede (web, e-mails, downloads, redes sociais, outros aplicativos) pelos usuários?

( ) não ( ) parcialmente ( ) totalmente

7 – Existe algum tipo de monitoramento e/ou controle de acesso aos recursos físicos (hardware) e lógicos (softwares) dos sistemas de informação?

( ) não ( ) parcialmente ( ) totalmente

8 – A instituição utiliza ferramentas de segurança da informação, tais como antivírus, AntiSpam, Firewall, Proxy e outras?

( ) Não utiliza ( ) raramente ( ) frequentemente ( ) sempre utiliza

9 – A instituição possui website próprio?

( ) Sim ( ) Não

10 – A instituição já registrou a ocorrência de incidentes de segurança da informação, tais como vírus, ataques, acessos indevidos, golpes, fraudes, furtos de informações ou equipamentos?

( ) nunca ( ) poucas vezes ( ) muitas vezes