SEGURANÇA DA INFORMAÇÃO NO COTIDIANO DO PROFESSOR E ALUNO

Silvane Bianchet Favero[1]
Velcir Barcaroli[2]

RESUMO

O presente artigo tem o intuito investigar as concepções e o conhecimento já adquirido a respeito da segurança da informação entre professores (as) e alunos (as) da terceira série do Ensino Médio que fazem parte 32ª Secretaria de Desenvolvimento Regional (SDR). A principal indagação se refere aos conceitos da segurança da informação no cotidiano desses professores (as) e alunos (as) e o que os torna mais vulneráveis a ataques direcionados a segurança da informação. A metodologia utilizada inicialmente foi à produção de um referencial teórico com o material disponível, seguida da aplicação de questionário fechado ao público pesquisado. Os dados obtidos através da pesquisa de levantamento apontam que o público indagado está despreparado para se proteger contra incidentes causados pela falta segurança da informação. Faz-se necessário capacitar professores (as) e alunos (as) das escolas estudadas para que desenvolvam habilidades de proteção contra os ataques a segurança da informação.

Palavas-chave: Segurança da informação. Tipos de ameaças. Controle de acesso.

ABSTRACT

This paper has the aims investigate the concepts and existing knowledge about information security among teachers and students of the third year of secondary school doing part of the 32nd Secretary of Regional Development (SDR). The main question refers to the concepts of information security in the daily lives of these teachers and students and that makes them more vulnerable to targeted attacks on information security. The methodology was initially used to produce a theoretical framework with the available material, followed by questionnaire closed to the public searched. The data obtained through the survey research suggest that the public is asked unprepared to protect them against incidents caused by lack of information security. It is necessary to train teachers and students of the school studied to develop skills to protection against attacks on information security.

Keywords: Information Security. Types of threats. Access Control.

[1] Tecnólogo em redes de computadores – UCEFF Faculdades – Chapecó. Complementação pedagógica em informática – UNIARP – Caçador.
[2]Bacharel em Ciências da computação. Especialista em tecnologia e desenvolvimento de software.

1 INTRODUÇÃO

A 32ª Secretaria de Desenvolvimento Regional (SDR) é composta por seis municípios, cada um sediando uma escola estadual para atender aos alunos de sua área de abrangência.

Desde 2009 a Secretaria de Educação do Estado de Santa Catarina (SED) vem implantando gradativamente nas escolas estaduais salas informatizadas, proporcionando aos alunos (as) maior aprendizagem através das tecnologias, já que nos dias atuais a informação é sem dúvida um fator de grande importância para as pessoas e nas escolas os alunos têm oportunidade de estarem conectados ao mundo através da internet.

Por meio do computador e a internet é possível realizar as mais diversas atividades, como mandar e-mails, realizar pesquisa para trabalhos escolares, acessar redes sociais, fazer compras e tantas outras possibilidades.

Através da internet é possível disponibilizar informações de sua máquina para o mundo e isso faz com que as pessoas estejam cada vez mais expostas e vulneráveis, e a segurança da informação tem um papel fundamental na era da tecnologia. Nas escolas não é diferente as tecnologias fazem parte do cotidiano do aluno através das salas informatizadas, onde a interação com o computador e o acesso a internet oferece ao aluno novas possibilidades, encantando e seduzindo, mas também traz uma preocupação, a segurança da informação.

Nesse contexto os professores e alunos da terceira série DO Ensino Médio das escolas que fazem parte da 32ª Secretaria de Desenvolvimento Regional (SDR) estão preparados para se proteger contra incidentes de segurança da informação?

O presente trabalho tem como objetivo realizar uma pesquisa com professores e alunos da terceira série do Ensino Médio que fazem parte da 32ª Secretária de Desenvolvimento Regional (SDR), para verificar se os mesmos conhecem os conceitos relacionados à segurança da informação.

Para atingir o objetivo, este estudo utilizou o referencial teórico, e a pesquisa de levantamento, através da aplicação de questionário fechado ao público pesquisado.

Esse estudo justifica-se pela necessidade de se produzir um referencial teórico para estudantes que tenham interesse pelo assunto, uma vez que o mesmo é novo e relevante para os processos educacionais.

2 FUNDAMENTAÇÃO TEÓRICA/ REFERENCIAL TEÓRICO

2.1 Segurança da Informação

Com o aparecimento dos computadores e com a atual dependência das pessoas a essas máquinas, surge a necessidade de se pensar na segurança da informação.

Conforme Sêmola (2003, p.55) “Podemos definir a segurança da informação como uma área do conhecimento dedicada á proteção de ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

Para o Gabinete de Segurança Institucional da Presidência da República, a segurança da informação tem como objetivo a:

> Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão e a modificação desautorizada de dados ou informações, armazenados em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

A cada dia surgem novas vulnerabilidades e com isso segundo Carvalho (2005) surge os crimes virtuais, que podem atingir desde pessoas simples até grandes empresas.

Segundo a revista Fonte (2012, p.21) o estudo *Norton Cybercrime Report,* divulgado anualmente pela Symantec, "apontou que 28 milhões de brasileiros foram vítimas de fraudes na internet, o que representa mais de 34% dos internautas do país.

Para se proteger contra crimes virtuais ou fraudes na internet de acordo com Carvalho (2005, p.1) "surge à necessidade de se identificar, mensurar e registrar essas atividades que em geral são chamados de incidentes de segurança, para que possa tomar medidas de forma a evitar ou reduzir seus efeitos".

A segurança da informação segundo Ferreira (2003) é composta por alguns princípios básicos como: autenticidade, confidencialidade, integridade e disponibilidade. Esses princípios têm como benefícios reduzir os ricos com vazamentos de informações, fraudes, erros, uso indevido, sabotagem roubo de informações entre outros problemas.

Ferreira (2003, p.59) descreve que a autenticidade tem como objetivo fazer a identificação correta de um usuário ou computador. Ainda segundo ele "o serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente da origem informada em seu conteúdo".

Para Sêmola (2003, p.57), a confidencialidade significa que toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, tendo como objetivo à limitação de seu acesso e uso apenas ás pessoas para quem elas são destinadas.

Ainda segundo o autor a integridade diz respeito que toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, tendo como função protegê-las contra alterações indevidas, intencionais ou acidentais.

Disponibilidade conforme Sêmola (2003, p.57), é toda informação gerada ou adquirida por um indivíduo ou instituição, deve estar disponível aos seus usuários no momento em que eles solicitarem.

Segundo Nakamura & Geus (2007) o mundo da segurança é marcado pela evolução contínua, na qual novos ataques têm como resposta novas formas de proteção, que levam ao desenvolvimento de novas técnicas de ataques, formando um ciclo. Criando assim a necessidade da segurança ser um fator contínuo e evolutivo.

Na visão Ferreira (2003) independente da forma que a informação seja apresentada ou o meio que através do qual é compartilhada ou armazenada, recomenda-se que ela seja protegida de forma adequada.

2.2 Tipos de Ameaças

2.2.1 Engenharia Social

Conforme Nakamura & Geus (2007, p.85) "a engenharia social é a técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia". Ela tem como foco enganar e ludibriar pessoas assumindo uma falsa identidade, a fim de que elas revelem senhas ou outros dados que possam comprometer a segurança da organização.

Segundo Brito da Silva (2012) os objetivos básicos da engenharia social são o mesmo do hacker, obter acesso não autorizado a sistemas ou informações, para cometer fraude, invasão de rede, espionagem industrial, roubo de identidade, ou simplesmente perturbar o sistema ou rede.

Para Brito da Silva (2012) um ataque através de engenharia social nas organizações, acontece porque é maneira mais fácil de obter acesso ilícito a informações do que a maioria das formas de pirataria técnica. Ainda segundo o autor os ataques de engenharia social

acontecem através dos níveis físicos e psicológicos. O ataque pode acontecer através do local de trabalho, telefone, lixo, e até mesmo on-line.

Para convencer a vítima segundo Wendt & Nogueira Jorge (2012), normalmente os criminosos dizem ser de determinadas instituições confiáveis, como bancos, órgão do governo, ou outros órgãos públicos para que ela acredite nas informações falsas apresentadas, o que seria uma estratégia para adquirir os referidos dados.

Os hackers de engenharia social segundo Brito da Silva (2012) conseguem a partir de um ponto de vista psicológico, criar um ambiente perfeito para o ataque, através de métodos básicos para convencer a vítima como: "representação, integração, conformidade, difusão de responsabilidade e simpatia". Independentemente do método utilizado, o objetivo principal é convencer a pessoa a revelar a informação desejada. Outro item importante é pedir um pouco de informação de cada vez a várias pessoas, a fim de manter a aparência de uma relação confortável.

Ferreira (2003) afirma que a engenharia social é uma das mais eficientes e perigosas formas de obtenção de informação utilizadas pelos invasores. Para ele a melhor forma de se defender contra este ataque é promover treinamento e conscientização em segurança da informação aos usuários e colaboradores.

2.2.2 Vírus de boot

Segundo Wendt & Nogueira Jorge (2012, p.23), "está modalidade de vírus é considerada a precursora de todos os outros tipos de vírus", sua principal característica é que ele se fixa na partição de inicialização do sistema.

> O vírus de "boot" é um programa muito pequeno que se instala nas áreas iniciais do disco rígido, em que estão armazenadas informações vitais para o funcionamento do microcomputador. Ao se transferir para as áreas de "boot", os vírus dessa espécie têm as condições ideais para a manipulação do disco rígido como um todo, podendo infectar outros arquivos utilizados na operação e funcionamento do micro. (PAIVA, 1995)

O vírus de boot de acordo com Nakamura & Geus (2007, p.128), "modificam setores de boot dos discos flexíveis, quando o computador é iniciado por meio desse disco flexível com setor modificado".

Todos os discos flexíveis possuem uma área de inicialização reservada para informações relacionadas à formatação do disco, dos diretórios e dos arquivos. Como essa área é executada antes de qualquer outro programa esses vírus são muito bem sucedidos. A disseminação ocorre de forma fácil, cada disco flexível não contaminado, ao ser inserido no drive e ser lido pode passar a ter uma cópia do código e, nesse caso, é contaminado, passando a ser um propagador do vírus. (FIREWALL).

Esse tipo de vírus não é transmitido pela rede e pode ser removido com um antivírus.

2.2.3 Worm

O *worm* surgiu segundo Martinelli (2008 p. 21) quando desenvolvedores de programas perceberam que seus softwares eram utilizados sem licenças. "Programadores lançaram assim uma forma de detectar em pequenas redes a integridade dos seus produtos".

Wendt & Nogueira Jorge (2012, p.24) afirmam que "esse tipo de arquivo malicioso, também conhecido como verme caracteriza-se pelo fato de residir na memória ativa do computador e se replicar automaticamente", sem que o usuário o execute. Na maioria das vezes se instala no computador através de vulnerabilidades existentes nos programas instalados.

Segundo previsto na cartilha da CERT.br (2012, p.25) *worms* consomem muitos recursos dos computadores ou redes de computadores , devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar seu desempenho.

2.2.4 Botnets

Na visão de Wendt & Nogueira Jorge (2012), os *botnets* são computadores infectados por arquivos maliciosos que possibilitam ao criminoso, realizar qualquer atividade com o computador da vítima de forma remota. Eles exploram falhas ou vulnerabilidades na configuração dos softwares ou no sistema operacional. A vítima não identifica que seu computador está infectado, nem que está realizando ataques contra outros computadores.

Conforme a cartilha da CERT.br (2012, p.26),

> *Botnet* é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos *bots*. Quanto mais zumbis participarem da *botnet* mais potente ela será. O atacante que a controlar, além de usá-la para seus próprios ataques, também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada.

2.2.5 Deface

Utilizada segundo Wendt & Nogueira Jorge (2012, p.26), "para caracterizar aqueles que desfiguram sites ou perfis de redes sócias".

Para Nogueira Jorge (2011) os defacers são semelhantes a pichadores, porém suas atividades não são realizadas em muros e sim em sites, blogs e outros meios. "Se um indivíduo desfigura um site e produz um dano contra ele, pode ser enquadrado no Código Penal e receber uma pena de detenção que varia entre 1 e 6 meses ou multa".

2.2.6 Spam

A CERT.br define *spam* como o termo utilizado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo exclusivamente comercial.

Segundo Martinelli (2008) o usuário passa a receber propagandas sobre itens relacionadas com data em que realizou a pesquisa ou sobre assuntos desconexos. Algumas empresas pagam por uma quantidade de e-mails validos, também conhecidos como *spam list.*O *spam* movimenta todo tipo de lixo eletrônico causando transtornos e aborrecimentos aos usuários. Pode estar associado ás técnicas de contaminação como trojans, worms, vírus com links ou executáveis.

Para a CERT. BR "s*pams* estão diretamente associados a ataques à segurança da internet e do usuário, sendo um dos grandes responsáveis pela propagação de códigos maliciosos, disseminação de golpes e venda ilegal de produtos".

Segundo o Comitê Gestor da Internet no Brasil nos últimos anos tem se observado uma um crescimento no volume de *spams* na internet, também tem aumentado o número de uso de *spam* na disseminação de vírus/ worms e em atividades relacionadas a fraudes (como phishingscam).

O Comitê Gestor da Internet no Brasil (2008) acredita que o anonimato provido através de computadores mal configurados de usuários finais, principalmente via banda larga, tem contribuído para esse cenário. "Para que seja possível reduzir o número de *spams* na internet é necessária à adoção não só de soluções técnicas, mas também de boas práticas e políticas que tratem dessa questão".

2.2.7 Cavalo de Tróia

Os autores Wendt & Nogueira Jorge (2012), afirmam que *trojan horse* ou cavalo de tróia é um arquivo malicioso que permite que o computador do invasor acesse de forma remota outra máquina, e obtenha informações confidenciais da vítima e envie para o invasor.

De acordo com a Symantec, o cavalo de tróia é um programa que se apresenta como um programa desejável, mas que na verdade é malicioso, ele contêm um código que causa a perda ou o roubo dos dados.

O Comitê Gestor da Internet no Brasil (2008) referencia cavalo de tróia como um programa geralmente recebido como um presente (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc.), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem consentimento do usuário.

Ainda segundo eles a estratégia utilizada consiste em enviar um arquivo malicioso que, ao ser executado compromete o computador da vítima liberando acesso ao criminoso para que ele tenha controle sobre o computador infectado.

2.2.8 Keylogger

De acordo com a Revista Fonte (2012, p.41) "*keylogger* é um pequeno aplicativo que pode vir embutido em vírus, spywares ou softwares de procedência duvidosa". Seu objetivo é capturar tudo o que é digitado pelo usuário. É uma das formas utilizadas para a captura de senhas.

Para Wendt & Nogueira Jorge (2012, p.30), o *keylogge*r é utilizado [...] "para a coleta de informações sensíveis sobre o usuário do computador e dessa forma oferecer subsídios para que o *cibercriminoso* cometa seus crimes contra a vítima".

Wendt & Nogueira Jorge (2012), explicam que atualmente os softwares *keylogger* permitem gravar não só o que digitado pelo usuário no teclado, mas tudo o que é feito na tela do computador, para posteriormente enviar para o e-mail anteriormente cadastrado pelo criminoso.

2.2.9 Rootkit

Conforme a cartilha CERT.br, *rootkit* é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

Para Wendt & Nogueira Jorge (2012), um dos problemas dos *rootkits* é que ele passa despercebido por grande parte dos antivírus, e suas chaves permanecem ocultas no registro e seus processos no gerenciador de tarefas, para que não sejam encontradas.Caso o sistema operacional solicite a abertura ou leitura de um determinado arquivo, o *rootkit* faz uma filtragem dos dados e não deixa chegar até ele o código malicioso. Assim dificilmente o *rootkit* é notado no computador.

2.2.10 Hijacker

De acordo com Wendt & Nogueira Jorge (2012), o *hijacker* é usado para sequestrar o navegador da internet dessa forma direciona o usuário do computador para sites diferentes daquelas digitadas, ou definindo o site como sendo a página inicial do navegador. É comum também à abertura automática de pop-ups, não solicitas pelo usuário com conteúdos pornográficos ou relacionados a sites fraudulentos.

Com muita propriedade Karasinsk informa que

> Os *hijacker* são "sequestradores" e o sentido real não fica muito longe disso. Estes programas entram em seu computador sem você perceber, utilizando controles ActivX e brechas na segurança. Assim modificam o registro do 7 TTP 7 ws, "seqüestrando" seu navegar e modificando a pagina inicial dele. Depois aparecem novas barras e botões, e páginas abrem sem parar na tela, contra a sua vontade.

2.2.11 Sniffer

Para Wendt & Nogueira Jorge (2012), o *sniffer* tem como objetivo monitorar todo o tráfego da rede, interceptando dessa forma os dados transmitidos para que possam posteriormente ser analisados.

Ainda segundo os autores este tipo de software pode ser utilizado por *cibercriminosos* para capturar *logins* e senhas de usuários de computadores, seus sites acessados, áreas da rede consideradas vulneráveis, conteúdos de e-mails e outras informações sensíveis.

2.2.12 Backdoor

Na visão de Wendt & Nogueira Jorge (2012), o *backdoor* ao ser instalado no computador deixa uma porta dos fundos aberta, ou seja, deixa o computador vulnerável para ataques ou invasões.

Para a CERT.br (2012, p.28) o *backdoor*

> permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo.

2.2.13 Hoax

Wendt & Nogueira Jorge (2012), colocam que o *hoax* é um conjunto de falsas histórias divulgadas na internet normalmente relacionadas a fatos alarmantes e inexistentes, como necessidade de ajuda financeira para pessoas doentes ou entidades, notícias sobre conspirações, perigos inexistentes, desastres prestes a acontecer, mensagens religiosas ou outro fato que traga transtorno ou prejuízo à vítima.

Wendt & Nogueira Jorge (2012), salientam que um dos pontos principais desses "boatos cibernéticos" é que as pessoas quando recebem a informação encaminham para outras pessoas como forma de ajudar, sejam através de e-mails, blogs ou redes sociais.

2.2.14 PhishingScan

De acordo com Wendt & Nogueira Jorge (2012, p.39), *phishing* "é a conduta daquele que pesca informações sobre o usuário do computador". No inicio ele era usado para definir a fraude que consistia no envio de e-mails não solicitados pelo usuário, que era estimulada a acessar sites fraudulentos. Os sites tinham a intenção de permitir o acesso aos dados eletrônicos do usuário que lhe acessava.

Hoje segundo Wendt & Nogueira Jorge (2012), o *phishing* é usado para definir também a conduta de pessoas que encaminham mensagens com objetivo de induzir a vítima a preencher formulários com suas informações pessoas ou instalar códigos maliciosos, capazes de enviar para os criminosos cibernéticos as informações solicitadas.

Segundo a CERT.br (2012, p.9) o *phishing* ameaça que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito.

2.2.15 Segurança em e-mail

Para Ferreira (2003) quando o assunto é e-mail existem muitos riscos associados a ele. Desde a contaminação por vírus até a falsificação de informações. Apesar de ser um meio eficiente para a toca de informações, novas formas de burlá-lo tem sido utilizadas para torná-lo um meio de propagar vírus pela internet.

Conforme descrevem Wendt & Nogueira Jorge (2012), para que um usuário da internet possa enviar e receber e-mails, ele deve possuir um nome de usuário vinculado a um domínio, no formato padrão "usuário@nomededominio.com.br". Obrigatoriamente, este domínio deve possuir um serviço de provedor de e-mail vinculado.

Ainda segundo Wendt & Nogueira Jorge (2012), essas informações são importantes caso seja necessário investigar um e-mail, pois é necessário ter noção de qual caminho percorrido por ele. Portanto para acessar um serviço de e-mail o usuário deve estar conectado a internet por um provedor de serviços de internet (PSI). Dessa forma é possível buscar informações sobre o usuário de e-mail, suas concepções e acessos, junto ao provedor de e-mail e ao PSI.

2.2.16 Senhas

Conforme descreve a cartilha da CERT.br (2012) é através de contas e senhas que o sistema identifica quem você é, confirma sua identidade e defende as ações que você pode realizar. Em um determinado sistema as pessoas normalmente conhecem seu usuário, já que é por meio de dele que as pessoas e serviços conseguem identificar quem você é. Por isso proteger sua senha é fundamental para se prevenir dos riscos envolvidos no uso da internet, pois é o seu sigilo que garante a sua identidade, ou seja, que você é dono daquele usuário. Caso outra pessoa saiba sua conta de usuário e senha poderá usá-las para se passar por você na internet e realizar ações em seu nome.

Ferreira (2003) coloca que para evitar esses problemas os usuários devem ser orientados a escolher senhas seguras, não utilizando senhas curtas ou muito longas, que obriguem a escrevê-las para lembrá-las. Fazer uso da mesma senha para sistemas distintos é uma prática comum, porém vulnerável.

Segundo o Comitê Gestor de Tecnologia da Informação da PR – CGTI/PR. Para proteger suas informações de outras pessoas, ao elaborar suas senhas nunca utilize nomes próprios, datas ou combinações existentes em dicionários. "Misture caracteres especiais (ex.: @#$%¨&*()+=.;) e combinações entre números e letras minúsculas e maiúsculas".Para elaborar uma senha, fácil de lembrar pense em uma frase, use a primeira, a segunda ou a última letra de cada palavra.

Na visão de Nakamura & Geus (2007, p.365) "as senhas são consideradas, até mesmo, o segundo elo mais 'fraco' da cadeia de segurança, vindo depois dos próprios seres humanos". Em função de suas vulnerabilidades as senhas estão sendo substituídas por outros métodos mais eficientes, como a biometrias ou certificados digitais.

Para Nakamura & Geus (2007) as senhas também apresentam características positivas como simplicidade de integração com diversos sistemas a torna fácil de ser implementada. Um ponto negativo é o fato de que a segurança depende da manutenção do sigilo da senha, que pode ser quebra de várias formas.

2.3 Controle de Acesso

2.3.1 Firewall

Para Nakamura & Geus (2007), a necessidade de utilização cada vez maior da internet levaram a uma crescente preocupação a segurança. Para eles o *firewall* é um dos componentes mais antigo e conhecido quando se fala em um sistema de segurança.

Conforme Sêmola (2003, p.133), o *firewall* tem como função realizar análises do fluxo de pacotes de dados, filtragem e registros dentro de uma estrutura de rede. [...] "Ele representa uma parede de fogo que executa comandos de filtragem previamente especificados com base na necessidade de compartilhamento, acesso e proteção requeridos pela rede e pelas informações disponíveis através dela".

Segundo Nakamura & Geus (2007), o *firewall* é formado por vários componentes, onde cada um deles tem uma função e desempenha um papel que influencia diretamente no nível de segurança.

A Symantec salienta que "todas as informações recebidas ou enviadas pela rede devem passar por um *firewall*, que examina os pacotes de informações e bloqueia aqueles que não atendam aos critérios de segurança".

2.3.2 Autenticação

A autenticação tem uma função fundamental para a segurança da informação segundo Nakamura & Geus (2007) ao validar a identificação dos usuários. Após a autenticação o sistema pode permitir a autorização para o acesso aos recursos.

Para Ferreira (2003, p.47) "o controle de acesso lógico deve abranger (i) o recurso informatizado que se pretende proteger e (ii) o usuário a quem se pretende dar certos privilégios e acessos". A proteção dos recursos está baseada na necessidade de acesso de cada usuário, já a identificação e autenticação normalmente são realizadas por user ID e uma senha durante o processo de logon.

Ainda segundo Ferreira (2003, p.47 e 48) "o controle de acesso pode ser resumido em termos de funções de identificação de usuários, gerenciamento de privilégios, limitação e desabilitação de acessos e na prevenção de acessos não autorizados".

De acordo com Nakamura & Geus (2007, p.363), o acesso aos sistemas e recursos de uma empresa ou organização depende do processo de verificação do usuário, que deve ser realizado de forma que somente o usuário legítimo tenha acesso. "As funções responsáveis por essa verificação são a identificação e autenticação".

O processo de logon conforme Ferreira (2003, p.48) é utilizado para obter acesso aos aplicativos em um sistema informatizado. "Para dificultar a tarefa de um invasor, recomenda-se limitar o número de tentativas incorretas de acesso (logon), bloqueando a conta do usuário ao alcançar o número limite".

Ferreira (2003, p.48) referencia que a identificação do usuário deve ser única e cada usuário deve ter sua própria identificação. "Essa unicidade de identificação permite um controle das ações praticadas pelos usuários por meio de log's de acesso e atividades dos sistemas operacionais e aplicativos".

Depois da identificação do usuário de acordo com Ferreira (2003) acontece à autenticação, dessa forma o sistema confirma se o usuário é mesmo quem diz ser. Pra realizar a autenticação o usuário deve apresentar algo que ele sabe ou possui. Na maioria dos sistemas solicita-se uma senha, algo que só o usuário deve conhecer. Na elaboração de senhas os usuários devem ser orientados a elaborar senhas seguras, evitando senhas muito curtas, fáceis ou longas demais, que os obrigue a escrevê-las em um papel para lembrá-las.

3 METODOLOGIA

Utilizou-se a pesquisa bibliográfica e também de levantamento. Segundo Gil (2008) “a pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos”.

Ainda conforme Gil (2008) levantamento é a interrogação direta das pessoas cujo comportamento se deseja conhecer. Procede-se á solicitação de informações a um grupo significativo de pessoas acerca do problema estudado para em seguida, mediante análise quantitativa, obtém-se as conclusões correspondentes aos dados coletados. Quando o levantamento recolhe informações de todos os integrantes do universo pesquisado, tem-se um consenso.

Para Bandeira o levantamento das características do grupo estudado é realizado através da aplicação de questionários auto-administrados ou através de entrevistas dirigidas por um questionário.

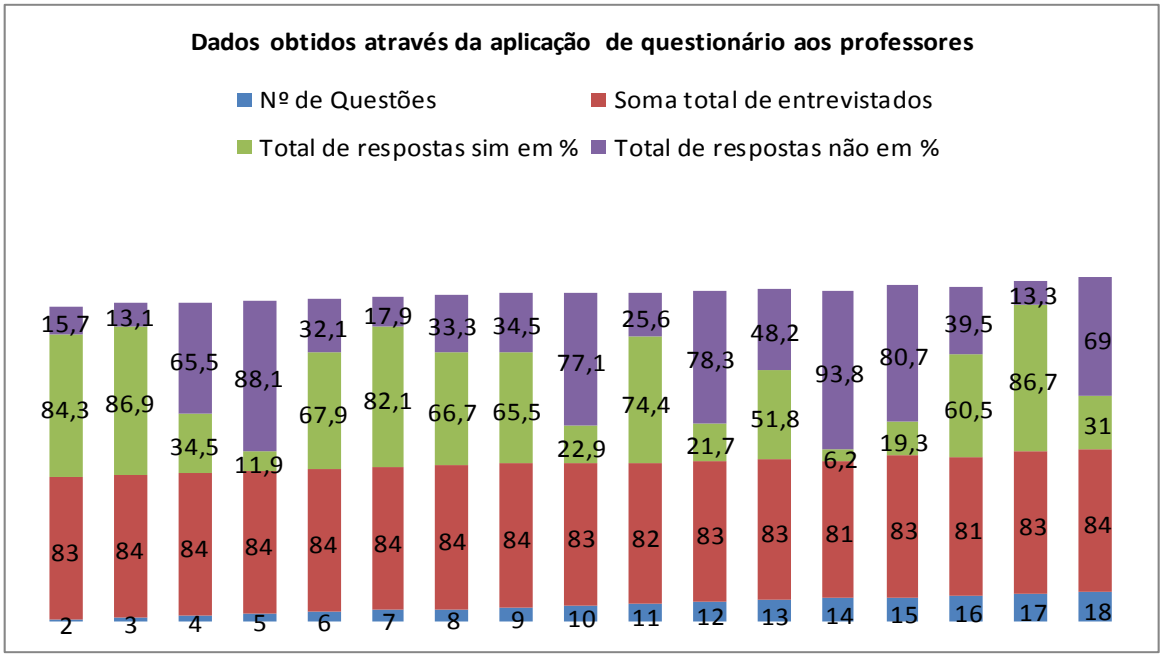
Para fazer a pesquisa de levantamento foi aplicado questionário com perguntas fechadas a população objeto de estudo composta por professores e alunos da terceira série do ensino médio das escolas que fazem parte da 32ª Secretária de Desenvolvimento Regional.

4 APRESENTAÇÃO E ANÁLISE DOS DADOS

O presente capitulo trata da descrição e discussão dos resultados a partir da pesquisa de levantamento realizado através da aplicação de questionário fechado ao público pesquisado. Os dados a seguir foram analisadas e tabulados utilizando o Microsoft Excel.

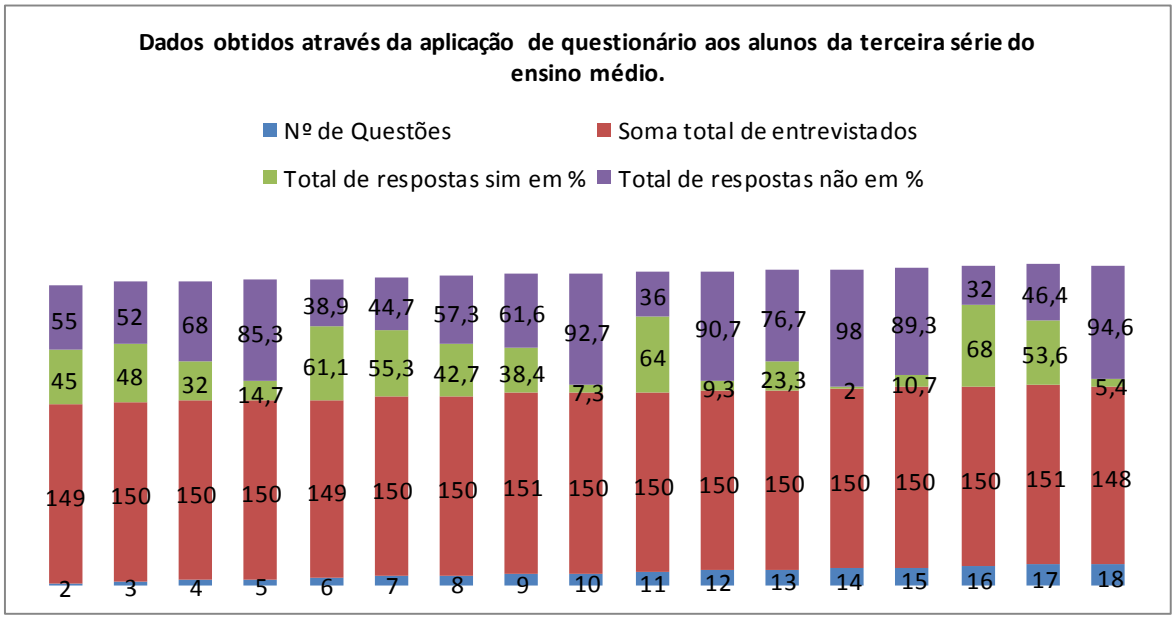
Essa pesquisa foi aplicada a uma amostra de 84 professores (as) e 151 alunos (as) da terceira série do Ensino Médio que trabalham e estudam nos municípios de abrangência da 32ª Secretaria de Desenvolvimento Regional (SDR), sendo apresentados nos gráficos a seguir:

Gráfico 1 – Resultado do questionário aplicado aos professores (as)



Fonte: Construído pela própria autora, 2014.

Gráfico 2 – Resultado do questionário aplicado aos alunos (as) da terceira série do Ensino Médio



Fonte: Construído pela própria autora, 2014.

A pesquisa de levantamento foi aplicada no mês de fevereiro de 2014, tendo como base o número de professores (as) e alunos (as) da terceira série do Ensino Médio para o ano de 2014.

Segundo a pesquisa realizada 15,7% dos professores (as) e 55,0% dos alunos (as) afirmaram não saber o significado de segurança da informação. 13,1% professores (as) e 52,0% dos alunos (as) afirmam não conhecer o significado de autenticidade, confidencialidade, integridade e disponibilidade.

Engenharia social se apresenta como uma eficiente e perigosa forma de obter informações. 34,5% dos professores (as) e 32,0% dos alunos (as) pesquisados afirmaram ter sido vítimas de pessoas que através de especulação tentaram descobrir senhas ou dados pessoais. O público pesquisado foi alvo de pessoas que através da engenharia social tentaram obter informações sem autorização.

Com a expansão das redes sociais também cresce a preocupação com a segurança da informação relacionado ao perfil de cada usuário, o deface tem sido utilizado para desfigurar sites, ou perfis nas redes sócias sem a permissão do usuário. 14,7% dos alunos (as) e 11,9% dos professores (as) afirmam que já tiveram seu perfil nas redes sociais modificado por outra pessoa sem tua autorização. Porém do total pesquisado 61,1% dos alunos (as) e 67,9% dos professores (as) conhecem alguém que teve o perfil de sua rede social modificado por outra pessoa sem sua autorização.

O e-mail é uma ferramenta muita utilizada para a comunicação, porém também usada para disseminar vírus. 82,1% dos professores (as) e 55,3% dos alunos (as) pesquisados afirmam ter recebido através de e-mail arquivos não solicitados induzindo a executá-lo.

Brechas de segurança estão sendo utilizados pelo hijacker para modificar o navegador da internet e abertura de pop-ups. 66,7% dos professores (as) e 42,7% dos alunos (as) confirmaram que seu navegador de internet já mudou a página inicial sem que ele tivesse feito isso.

O hoax, “boatos cibernéticos” compartilhados através de e-mails ou redes sociais. Ao receber essas mensagens as pessoas se comovem e como forma de ajuda repassam para outras pessoas. 65,5% dos professores (as) e 38,4% dos alunos (as) responderam que já receberam e-mails pedindo ajuda financeira para pessoas doentes ou com mensagens religiosas. Dos

professores (as) 22,9% encaminharam o e-mail para outras pessoas enquanto que dos alunos (as) 7,3% enviaram.

Hoje quem possui uma conta de e-mail percebe o grande número de mensagens recebidas através dele sem ter solicitado, com diversos fins. 74,4% dos professores (as) e 64,0% dos alunos (as) responderam que receberam e-mails não solicitados estimulando a acessar algum site, 21,7% dos professores (as) e 9,3% dos alunos (as) afirmam ter acessado o site indicado.

Com o crescente uso da internet, também tem aumentado o roubo de informações de usuários que são estimulados a preencher formulários com dados pessoas como, CPF, RG e endereço. 51,8% dos professores (as) e 23,3% dos alunos (as) afirmam ter recebido essas mensagens sem que tenham solicitado. 6,2% dos professores (as) e 2,0% dos alunos (as) retornaram mensagem com os dados solicitados.

Senhas são utilizadas juntamente com o login para identificar um usuário, são pessoais e não devem ser compartilhadas. Segundo a pesquisa realizada 10,7% dos alunos (as) e 19,3% dos professores (as) confirmaram que compartilham com amigos ou familiares a senha de seu e-mail ou rede social.

Para proteger seus dados e informações pessoais e criar senhas seguras, algumas regres devem seguidas no momento de elaborar a senha, como por exemplo, letras maiúsculas, minúsculas, números e caracteres especiais. 32,0% dos alunos (as) e 39,5% dos professores (as) afirmam não utilizar senhas seguras em seu e-mail, sites acessados ou conta nas redes sociais.

Os usuários de e-mails tem sido alvo do spam, e-mails não solicitados enviados para um grande número de pessoas. Conforme dados coletados através da pesquisa 86,7% dos professores e 53,6% dos alunos (as) confirmaram ter recebido e-mails não solicitados com propaganda de produtos. Onde 31,0% dos professores (as) e 5,4% dos alunos (as) afirmaram ter acessado o site indicado para visualizar ou comprar os produtos indicados.

De acordo com os dados coletados percebe-se que na maioria das vezes o aluno (a) se utiliza mais dos conceitos relacionados à segurança da informação em seu cotidiano do que o professor (a).

5 CONSIDERAÇÕES FINAIS

Através deste trabalho observou-se que os professores (as) e alunos (as) da terceira série do Ensino Médio que pertencem a 32ª Secretaria de Desenvolvimento Regional (SDR) estão despreparados para se proteger contra incidentes de segurança da informação.

Do total de professores (as) e alunos (as) da terceira série do Ensino Médio pesquisados, 70, 7% afirmaram não conhecer o significado de segurança da informação e 65,1% deles confirmaram desconhecer o significado de autenticidade, confidencialidade, integridade e disponibilidade.

Do público alvo da pesquisa 75,1% afirmam ter recebido sem solicitação mensagens com formulários perguntando dados pessoais, 8,2% retornaram a mensagem com os dados solicitados e desses 6,2% são professores (as).

Segundo dados coletados através do questionário aplicado, 72,2%, sendo 39,5% professores (as) afirmam não utilizar senhas seguras em seu e-mail, sites acessados ou conta nas redes sociais.

Conforme as respostas do público alvo da pesquisa compartilham com amigos ou familiares a senha de seu e-mail ou rede social 30% dos professores (as) e alunos (as) da terceira série do Ensino Médio pesquisados, desses 19,3% são professores (as).

Percebe-se pela pesquisa realizada que a escolas alvo do estudo necessitam de uma capacitação, para professores (as) e alunos (as) sobre segurança da informação, para que estejam preparados para se proteger contra ataques e vulnerabilidades que se apresentam no seu cotidiano.

Sugiro que seja implementado nas escolas alvo do estudo, um firewall com filtro de acesso, e para melhorar ainda mais a segurança da informação, que seja implantado um sistema de autenticação, onde cada usuário que acessar a internet deve ter um login e senha de acesso.

O login deve ser a matricula do professor (a) ou aluno (a) e a senha deve ser criado através de regras, para que sejam seguras. Dessa forma vai ser possível acompanhar o que cada usuário acessa através da rede da escola, podendo dessa forma ser identificado e responsabilizado caso seja necessário.

Para que um sistema de autenticação seja implantado nas escolas será necessário fazer um treinamento com os professores (as) e alunos (as). No inicio isso trará resistências, mas com o passar do tempo será uma norma como qualquer outra.

RFERÊNCIAS

BANDEIRA, Marina; **Tipos de pesquisa.** Disponível em<http://www.ufsj.edu.br/portal-repositorio/File/lapsam/texto%201b%20-%20TIPOS%20DE%20PESQUISA.pdf>. Acesso em: 13 ago. 2013.

BRITO DA SILVA, Tiago. **Segurança Informática – Vulnerabilidades Aplicacionais.** Universidade Católica Portuguesa, Faculdade de Engenharia. 2012. Disponível em: <http://repositorio.ucp.pt/bitstream/10400.14/12040/1/Tese_TiagoSilva.pdf>. Acesso em: 08 de fev. 2014.

CARVALHO, Luciano Gonçalves. **Segurança de Redes**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2005.

CERT.BR. **Cartilha de segurança para internet – Fascículo senhas.** Disponível em: <http://cartilha.cert.br/fasciculos/senhas/fasciculo-senhas.pdf>. Acesso em: 26 fev. 2013.

CERT.BR. **Cartilha de segurança para -Glossário.** Disponível em: <http://cartilha.cert.br/glossario>. Acesso em: 21 jul. 2013.

CERT.BR. **Cartilha de segurança para internet.** Disponível em: < http://cartilha.cert.br>. Acesso em: 25 mar. 2013.

COMITÊ Gestor da Internet no Brasil.**Proposta da Comissão de Trabalho Anti-Spam do Comitê Gestor da Internet no Brasil: Tecnologias e Políticas para Combate ao Spam.**São Paulo, 2008. Disponível em <http://www.cert.br/docs/ct-spam/ct-spam-tecnologias-politicas.pdf >. Acesso em 08 de fev. de 2014.

COMITÊ Gestor de Tecnologia da Informação da PR – CGTI/PR. **Cartilha da segurança – simples atitudes podem evitar grandes problemas.** Disponível em: <http://www4.planalto.gov.br/cgti/cartilha-de-seguranca-da-informacao/cartilha-seguranca-da-informacao>. Acesso em: 10 set.. 2013.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2003

FIREWALL, Segurança na Rede. **Tipos de Vírus. Disponível em:** <http://firewall.powerminas.com/o-que-e-um-virus-de-computador/tipos-de-virus/>. Acesso em: 08 de fev. de 2014.

FONTE, Tecnologia da Informação na Gestão Pública. **Segurança da informação em Rede – A vida on-line e suas contingências. Segurança dos dados pessoais e privacidade.** 2012, p. 21. Disponível em: <http://www.prodemge.mg.gov.br/images/revistafonte/revista_12.pdf>. Acesso em: 08 de fev. de 2014.

FONTE, Tecnologia da Informação na Gestão Pública. **Segurança da informação em Rede – A vida on-line e suas contingências. Glossário.** 2012, p. 21.Disponível em: <http://www.prodemge.mg.gov.br/images/revistafonte/revista_12.pdf>. Acesso em: 08 de fev. de 2014.

GABINETE de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. **Segurança da Informação.** Disponível em: <http://dsic.planalto.gov.br/seguranca-da-informacao>. Acesso em: 11 dez. 2013.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

KARASINSKI, Eduardo; **O que é Hijack?** Disponível em: <http://www.tecmundo.com.br/pdf/212-o-que-e-hijack-.pdf>.Acesso em: 23. abr 2013.

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio de. **Segurança de Redes em Ambientes Corporativos**. São Paulo: Novatec, 2007.

NOGUERIRA JORGE, Higor Vinicius. **Segurança da informação e Crimes Cibernéticos.**2011. Disponível em:<http://www.crimesciberneticos.net/2011_07_01_archive.html >. Acesso em: 08 de fev. de 2014.

PAIVA, Maurício Pinheiro. **Saiba o que é vírus de "boot"**. São Paulo, 1995. Disponível em: <http://www1.folha.uol.com.br/fsp/1995/1/11/informatica/11.html>. Acesso em 08 de fev. de 2014.

SÊMOLA, Marcos. **Gestão da segurança da informação – uma visão executiva**. Editora Campus, 2003.

SYMANTEC. Glossário. **Firewall.** Disponível em:<http://www.symantec.com/pt/br/security_response/glossary/define.jsp?letter=f&word=firewall>. Acesso em: 14 dez. 2013.

SYMANTEC. Glossário. **Trojan horse (Cavalo de Troia).** Disponível em: <http://www.symantec.com/pt/br/security_response/glossary/define.jsp?letter=t&word=trojan-horse> Acesso em: 20 jun. 2013.

WENDT, Emerson; NOGUEIRA JORGE, Higor Vinicius; **Crimes cibernéticos: ameaças e procedimentos de investigação**. –Rio de Janeiro: Brasport, 2012.

APÊNDICE A- Questionário para entrevistas com professores e alunos da terceira série do Ensino Médio

UCEFF FACULDADES
PÓS – GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Questionário para pesquisa aplicado aos professores e alunos da terceira série do Ensino Médio da SDR de Quilombo. Essa pesquisa foi autorizada pela Sra. Odila Fortti, Gerente de Educação Ciência e Tecnologia da 32ª Secretaria de Desenvolvimento Regional.
OBS- NÃO PRECISA SE IDENTIFICAR

Você é: ( ) Professor ( ) Aluno
2- Você sabe o que significa segurança da informação?
( ) Sim ( ) Não
3- Você sabe o significado de autenticidade, confidencialidade, integridade e disponibilidade?
( ) Sim ( ) Não
4 - Você já foi vítima de pessoas que através de especulação tentaram descobrir senhas ou dados pessoais seus?
( ) Sim ( ) Não
5- Seu perfil nas redes sociais como, orkut ou facebook, já foi modificado por outra pessoa sem tua autorização?
( ) Sim ( ) Não
6- Você conhece alguém que teve o perfil de sua rede social como, orkut ou facebook, modificado por outra pessoa sem sua autorização?
( ) Sim ( ) Não
7- Você já recebeu através de e-mail arquivos não solicitado, te induzindo a executá-lo?
( ) Sim ( ) Não
8- Seu navegador de internet já mudou a página inicial sem que você tenha feito isso?
( ) Sim ( ) Não
9- Você já recebeu algum e-mail pedindo ajuda financeira para pessoas doentes ou com mensagens religiosas?
( ) Sim ( ) Não
10- Se você já recebeu e-mail pedindo ajuda financeira para pessoas doentes ou mensagens religiosas você encaminhou esse e-mail para outras pessoas?
( ) Sim ( ) Não
11- Você já recebeu algum e-mail não solicitado estimulando a acessar algum site?
( ) Sim ( ) Não
12- Se você recebeu e-mail estimulando a acessar determinado site, você o acessou?
( ) Sim ( ) Não
13- Você já recebeu sem solicitação mensagens com formulários perguntando dados pessoais como, CPF, RG, endereço, entre outros dados pessoais?
( ) Sim ( ) Não
14- Caso tenha recebido sem solicitação mensagens com formulários perguntando dados pessoais como, CPF, RG, endereço, entre outros dados pessoais, você retornou a mensagem com os dados solicitados?
( ) Sim ( ) Não

15- Você costuma compartilhar com seus amigos ou familiares a senha do e-mail ou rede social?
( ) Sim ( ) Não
16- Suas senhas de e-mail, facebook ou outros sites acessados na internet possuem letras maiúsculas, minúsculas, números e caracteres especiais (#@)?
( ) Sim ( ) Não
17- Você já recebeu e-mails com propagandas de produtos sem ter solicitado?
( ) Sim ( ) Não
18- Ao receber e-mail com propagandas de produtos você acessa o site indicado para visualizar ou comprar os produtos indicados?
( ) Sim ( ) Não