

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO
GRANDE DO NORTE
CAMPUS NATAL - ZONA NORTE
CURSO TÉCNICO INTEGRADO EM INFORMÁTICA

FERNANDA PEREIRA RIBEIRO
HUILYANENAJARA SILVA DE ANDRADE

**DESENVOLVIMENTO DE MATERIAL DIDÁTICO E CAPACITAÇÃO EM
SEGURANÇA DA INFORMAÇÃO, VOLTADOS PARA A COMUNIDADE NO
ENTORNO DO IFRN CAMPUS NATAL – ZONA NORTE**

NATAL-RN
2016

FERNANDA PEREIRA RIBEIRO
HUILYANENAJARA SILVA DE ANDRADE

**DESENVOLVIMENTO DE MATERIAL DIDÁTICO E CAPACITAÇÃO EM
SEGURANÇA DA INFORMAÇÃO, VOLTADOS PARA A COMUNIDADE NO
ENTORNO DO IFRN CAMPUS NATAL – ZONA NORTE**

Relatório apresentado à Coordenação do Curso Técnico e Integrado em Informática, do Campus Natal – Zona Norte, do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, como requisito parcial para obtenção do diploma de Técnico em Informática.

Orientador – Prof. Rodolfo da Silva Costa

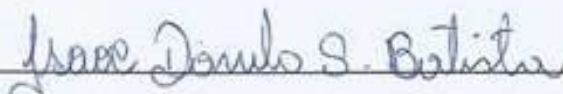
FERNANDA PEREIRA RIBEIRO
HUILYANENAJARA SILVA DE ANDRADE

**DESENVOLVIMENTO DE MATERIAL DIDÁTICO E CAPACITAÇÃO EM
SEGURANÇA DA INFORMAÇÃO, VOLTADOS PARA COMUNIDADE NO
ENTORNO DO IFRN CAMPUS NATAL – ZONA NORTE**

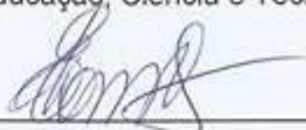
Relatório apresentado à Coordenação do Curso Técnico e Integrado em Informática, do Campus Natal – Zona Norte, do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, como requisito parcial para obtenção do diploma de Técnico em Informática.

Aprovado em: 02/03/17

COMISSÃO EXAMINADORA



Prof. Isaac Danilo Santos Batista – Avaliador
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte



Prof. Edmilson Barbalho Campos Neto – Coordenador do Curso de Informática
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte



Prof. Rodolfo da Silva Costa – Orientador
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

Aos mestres da vida e da sala.

Quando todos nos unirmos contra as injustiças e em defesa da privacidade e dos direitos humanos básicos, poderemos nos defender até dos mais poderosos sistemas.

Edward Snowden

RESUMO

A comunicação evoluiu de acordo com a humanidade, gerando assim novas necessidades de aprimoramento na proteção dos atuais meios de comunicação. Integridade, confidencialidade, autenticidade, não repúdio e a disponibilidade são princípios básicos que garantem a segurança da informação, visando que o ser humano é o principal agente nesse processo, uma vez que é ele o responsável no manuseio e armazenamento da informação, materiais como apostilas foram desenvolvidos para aplicação de minicursos no campus onde alunos, servidores e comunidade entorno do IFRN Campus Natal Zona Norte participaram. Diferentes estudos foram abordados durante o projeto que se dividiu em três módulos, o primeiro módulo direcionado aos conceitos básicos e gerais da segurança da informação nos dispositivos computacionais, o segundo módulo com foco nas redes sociais e os dispositivos móveis, finalizando com o terceiro módulo na configuração segura de roteadores wireless domésticos. Através de conteúdos práticos e teóricos foi repassado aos usuários modos de proteção dos perigos mais comuns encontrados na sociedade da informação, conhecimento considerado primordial na sociedade hodierna.

Palavras-chave: Segurança da informação. Proteção nos dispositivos móveis. Invasão.

ABSTRACT

Communication has evolved according to humanity, thus generating new needs for improvement in the protection of the current media. Integrity, confidentiality, authenticity, non-repudiation and availability are basic principles that guarantee the security of information, aiming that the human being is the main agent in this process, since he is responsible in the handling and storage of information, materials such as handouts Were developed for the application of mini-courses on campus, where students, servers and the community surrounding the IFRN Campus Natal Zona Norte participated, different studies were approached during the project that was divided in three modules, the first module was directed to the basic and general concepts of security of the information in the computational devices, the second module focused on social networks and mobile devices, finishing with the third module in the secure configuration of wireles domestic routers. Through practical and theoretical contents, users were given the most common protection of the dangers found in the information society, a knowledge considered to be of prime importance in today's society.

Keywords: Information security. Protection on mobile device. Invasion.

SUMÁRIO

1 INTRODUÇÃO	8
2 JUSTIFICATIVA	9
3 OBJETIVOS	10
3.1 OBJETIVOS ESPECÍFICOS	10
4 METODOLOGIA.....	11
4.1 PESQUISA DE CAMPO	11
4.2 REVISÃO E ATUALIZAÇÃO DO MATERIAL DIDÁTICO.....	12
4.3 APLICAÇÃO DOS MINICURSOS.....	12
4.3.1 Módulo I – Introdução às práticas da Segurança da informação	13
4.3.2 Módulo II – Segurança em Redes Sociais e Dispositivos móveis.....	17
4.3.3 Módulo III – Instalação e Configuração de roteadores wireless em redes domésticas.....	21
5 RESULTADOS	23
6 CONSIDERAÇÕES FINAIS	24
6.1 ATIVIDADES FUTURAS	24
6.2 LIÇÕES APRENDIDAS	24
REFERÊNCIAS.....	25
APÊNDICE A – Apostila do primeiro módulo	26
APÊNDICE B – Apostila do segundo módulo.....	27
APÊNDICE C – Apostila do terceiro módulo	28

1 INTRODUÇÃO

Conforme Kevin Mitnick diz em sua renomada obra *A Arte de Enganar*, mesmo que uma empresa adquira as melhores tecnologias de segurança, treine seu pessoal e tenha os melhores guardas, essa empresa ainda estará vulnerável, mesmo que os indivíduos sigam cada uma das melhores práticas de segurança e instalem todos os produtos de segurança vigiando suas configurações, eles ainda estarão vulneráveis. (MITNICK, 2002) Essa vulnerabilidade tratada durante sua obra, é algo agravado porque muitos ainda não compreenderam as ameaças que estão submetidos em rede.

Vivemos em uma sociedade globalizada e interligada, onde todo tipo de informação circula em rede, isto gera uma necessidade que não existia outrora, a proteção desses dados circundantes. Grandes empresas e governos, preocupados com o risco de possíveis vazamentos de informações confidenciais, investem massivamente em equipamentos e programas para sua proteção, entretanto, o que ainda é esquecido por alguns, é o fator humano.

O ser humano moderno vive acoplado às novas tecnologias, as utiliza em seu âmbito pessoal e profissional, e assim como existem pessoas mal intencionadas que buscam atacar grandes organizações, existem aquelas que também procuram obter vantagem através de pessoas que acreditam não ter nada há temer com esses criminosos, o que é uma conclusão extremamente equivocada.

Em razão do ser humano ser o meio mais simples para criminosos, como os engenheiros sociais, obterem dados sigilosos, se faz necessário a orientação na educação de usuários dos dispositivos computacionais. A conscientização dos riscos existentes às pessoas é um processo que interfere diretamente nas empresas e na vida pessoal do indivíduo. Diante disso, o projeto buscou atender essa necessidade, através do desenvolvimento de material e aplicação de aulas a respeito da segurança da informação para servidores, alunos e comunidade entorno do IFRN Campus Natal Zona Norte.

2 JUSTIFICATIVA

Como se sabe, estamos na era da informação, tornando-a objeto de grande valor em nossa sociedade. Ter dados roubados, perdidos ou alterados pode trazer grande prejuízo para um indivíduo e principalmente para grandes organizações. Desse modo, o projeto teve como principal propósito continuar orientando a comunidade em geral à utilização de métodos que evitem a apropriação indevida, perda ou alteração não desejada de informações confidenciais.

A relevância do projeto se mostra desde o seu público alvo, que visa pessoas internas ao campus e entorno do mesmo, até sua forma de ministrar, expondo materiais para compor a conceituação do projeto até a estrutura necessária para trabalhar a prática com os alunos. Por meio dele será possível contribuir de forma decisiva nos resultados de futuros e possíveis ataques virtuais aos participantes, ou até mesmo para que não ocorram, uma vez que os alunos estarão instruídos a como proceder.

3 OBJETIVOS

O projeto tem por objetivos o estudo teórico das mais comuns ameaças que atingem sistemas computacionais, tendo em vista os modos de ataque e os métodos de proteção contra essas ameaças; revisar e atualizar material didático, construído anteriormente, sobre o tema e, principalmente, informar e capacitar a comunidade sobre o uso seguro e consciente de sistemas computacionais, bem como a proteção de suas informações pessoais. Conseqüentemente, os participantes dos cursos a tornam-se agentes multiplicadores desse conhecimento.

3.1 OBJETIVOS ESPECÍFICOS

Dentre os objetivos específicos, destacam-se a apresentação de conceitos gerais e termos usuais a respeito da segurança da informação, orientação na prevenção dos ataques mais comuns e danosos no meio computacional, demonstração de como remover ameaças já presentes no dispositivo ao desinstalar corretamente programas maliciosos, auxílio na configuração adequada das redes sociais mais utilizadas, apresentação de como se prevenir adequadamente para cada risco existente, além de ensinar a configurar os roteadores domésticos de forma segura.

4 METODOLOGIA

Este projeto foi dividido em três módulos, tendo por ênfase a segurança da informação. O tempo em média para a revisão e atualização de cada minicurso/módulo foram de três meses, dependendo da programação e do tempo de desenvolvimento dos materiais e aplicação de cada minicurso, sendo um por módulo. Para chegar a finalização de cada módulo foram realizadas reuniões semanais presenciais, utilização de redes sociais no auxílio ao projeto para resolução de possíveis dúvidas acerca dos diversos temas abordados, além de apresentações prévias ao orientador antes de cada exposição do minicurso.

O primeiro módulo aborda o tema: Introdução à segurança da informação. Módulo básico que aborda conceitos, definições, reconhecimento de termos técnicos e ações pouco conhecidas, possibilitando assim, que o público alvo não necessariamente possua algum conhecimento da área técnica de informática para participar.

O segundo módulo aborda o tema: Segurança em redes sociais e dispositivos móveis. Esse módulo também não exigia do aluno conhecimento técnico prévio e não era dependente do assunto do primeiro módulo.

Por fim, o terceiro módulo, Instalação e configuração de roteadores wireless em redes domésticas, com recomendação que os alunos possuíssem conhecimento na área de redes, ainda que mínimo, já que o conteúdo do minicurso abrangeria um nível mais técnico do assunto.

Visando desenvolver de modo objetivo cada módulo/minicurso, este projeto foi estruturado em ciclos para sua metodologia, sendo eles divididos em três etapas: pesquisa de campo, revisão e atualização de um material didático e aplicação de um módulo do minicurso.

4.1 PESQUISA DE CAMPO

A primeira etapa de cada módulo se dá com pesquisa em livros (levantamento bibliográfico), fichamento de fontes diretas de autores que tenham obras acerca da temática abordada, materiais de sites da internet, cursos online relacionados à segurança da informação, como também uma discussão periódica com o orientador do projeto a fim de esclarecer alguns temas que são abordados na apostila. Essa pesquisa é a base para a reconstrução dos módulos.

Os temas de cada apostila foram divididos e distribuídos entre os componentes para a revisão e atualização. A cada reunião foi levado os temas reconstruídos para análise e discussão por todos os participantes do projeto, após isso, o tema reconstruído era aderido a apostila e slides.

4.2 REVISÃO E ATUALIZAÇÃO DO MATERIAL DIDÁTICO

A revisão e atualização do módulo do minicurso está atrelada intimamente à pesquisa, havendo a seleção do conteúdo reconstruído. Está envolvida nessa etapa a reconstrução do material didático, dos slides para a aplicação, testes de laboratório, entre outros.

4.3 APLICAÇÃO DOS MINICURSOS

Cada minicurso foi aplicado em dois turnos, com duração de 6 horas cada turno, realizado em 2 dias e dividido em duas turmas, com o total de 12 horas de aula. Cada turno ficava sob a responsabilidade de 2 bolsistas (de um total de 4), sempre sob a supervisão do orientador. Cada turma possuía um total de 20 pessoas, quantidade definida através da capacidade do laboratório de redes do campus.

Na aplicação de cada módulo do minicurso foi utilizada como ferramenta principal a apresentação de slides contendo informações relevantes acerca do assunto, bem como exemplos práticos em laboratório. Considera-se ainda a utilização de outras ferramentas dentro da própria apresentação, tal como vídeos, gráficos, imagens e testes práticos em laboratório.

O minicurso foi composto por aulas práticas e teóricas. No primeiro dia eram aplicadas as aulas teóricas para compreensão prévia do conteúdo prático, que seria aplicado no dia seguinte. No segundo, foram realizadas as aulas práticas, para exercício e fixação do conteúdo. Nas aulas práticas, foram utilizadas ferramentas de auxílio, visando aproximar o aluno do computador, de modo a aplicar os conceitos aprendidos com a teoria na prática. No primeiro módulo utilizamos ferramentas como Máquinas virtuais: para rodar o sistema operacional infectado com malwares sem danificar a máquina física, no caso, foi escolhido o SO Windows 7; Antivírus e Antispywares: foi demonstrado como funciona e como utilizar essas ferramentas e segurança; Programa de captura de teclas digitadas (Keylogger): utilizado para

demonstrar sua funcionalidade maliciosa. No terceiro módulo utilizamos Roteadores: para montar uma rede privada, simulando uma rede doméstica.

4.3.1 Módulo I – Introdução às práticas da Segurança da informação

No primeiro módulo o minicurso se baseou nos conceitos básicos acerca da segurança da informação, passando desde aos princípios científicos até a identificação e remoção de malwares. Diversos temas relacionados foram abordados, conceitos de extrema importância para que os usuários pudessem conhecer e compreender os procedimentos de proteção, sabendo posteriormente como proceder diante de problemas virtuais. Sem a necessidade de conhecimentos prévios ou técnicos na realização do minicurso.

A segurança da informação é dividida em cinco pilares básicos, que permitem que o usuário utilize seus serviços em rede de maneira segura. Os princípios básicos da segurança da informação são: integridade, confidencialidade, autenticidade, não repúdio e a disponibilidade.

- **Integridade:** é a garantia que a informação não foi alterada sem a autorização do remetente durante o envio ou armazenamento.
- **Confidencialidade:** consiste em proteger a informação para que só pessoas autorizadas tenham acesso a ela. Esse mecanismo permite a privacidade dos dados.
- **Autenticidade:** é a comprovação de que a mensagem é realmente de quem diz ser, geralmente usamos senhas para comprovar nossa autenticidade.
- **O não repúdio:** são métodos que comprovam que o remetente enviou a mensagem, deixando-o impossibilitado de negar sua autenticidade.
- **Disponibilidade:** que garante que a informação esteja acessível quando o usuário necessitar dela.

Para a garantia desses pilares, duas técnicas são corriqueiramente utilizadas, a criptografia e a esteganografia.

A criptografia é a primeira técnica utilizada para proteção de informações. Ela consiste em transformar um dado legível em um dado ilegível, só sendo interpretada com o auxílio de uma chave, que funciona como uma espécie de senha, sem essa senha o dado não pode ser interpretado.

Garantindo dessa forma que apenas aqueles que possuam a chave tenham acesso a mensagem. A criptografia existe desde os primórdios e foi se aperfeiçoando juntamente as demais tecnologias.

A segunda técnica utilizada para proteção de dados é a esteganografia. Usada para mascarar mensagens, seu funcionamento consiste em inserir uma informação dentro de outra. Dessa forma, apenas o receptor saberá a existência da mensagem oculta dentro de outra. Ao longo da história muitas técnicas de esteganografia foram desenvolvidas, um exemplo disso são as tintas invisíveis, que visualmente não apareciam nos papeis, mas quando aquecidas mostravam as mensagens escritas. (ARTZ 2001).

Apesar da existência dessas tecnologias e as suas utilizações em grande escala, principalmente no que diz respeito à criptografia, as informações que circulam em rede não podem ser tratadas como totalmente seguras, uma vez que são os humanos que manipulam essas informações. A manipulação e conseqüente vulnerabilidade humana foi um dos principais assuntos trabalhados neste módulo.

Para compreendermos isso melhor, precisamos entender alguns conceitos, como a engenharia social, que é uma técnica utilizada por criminosos para ter acesso não autorizado a sistemas, redes ou informações que possuam valor estratégico, através da manipulação de uma vítima. Geralmente dotado de boa aparência, educado, criativo e carismático, o engenheiro social costuma ser agradável, daí seu caráter manipulador.

O motivo que leva pessoas maliciosas praticarem a engenharia social é o fato do ser humano ser o elo mais fraco na segurança da informação. O desenvolvimento de tecnologias avançadas na segurança torna invasões técnicas mais complexas, e encontrar vulnerabilidades nesses sistemas demanda maior tempo e risco, sendo assim a exploração do fator humano é muito mais simples e menos arriscada. (PEIXOTO, 2006).

O ser humano naturalmente adota comportamentos que facilitam a ação do engenheiro social. Alguns exemplos são a vaidade, autoconfiança, vontade de ser útil e busca de amizades, isso ocorre porque quando esses comportamentos são adotados sem o devido cuidado facilita a aproximação do criminoso a vítima.

Para se precaver das ações dos engenheiros sociais é importante compreender como eles agem. Em uma espécie de ciclo, esses criminosos variam apenas as técnicas que utilizam em cada etapa, o ciclo realizado é composto de quatro passos básicos que não obedecem necessariamente a uma ordem fixa. (ALLEN, 2006)

Na primeira etapa o engenheiro social faz uma pesquisa, recolhendo informações fáceis, geralmente de domínio público, para assim ficar a par do alvo a ser explorado. As redes sociais podem ser um exemplo de local de encontro dessas primeiras informações. Em seguida, o engenheiro começa a desenvolver um relacionamento com o alvo, conquistando a confiança da vítima. Uma das técnicas usadas nessa etapa é se passar por outra pessoa que seja leiga e busca ajuda, ou então fingir autoridade. Após isso, quando ele já conhece e possui a confiança do seu alvo, ele parte para terceira etapa, iniciando assim a exploração das vulnerabilidades da vítima e através da manipulação recolhe as informações que realmente o interessa. Por último, ele faz o uso das informações adquiridas, caso essas informações sejam apenas uma etapa, ele retorna ao início do processo, até que o objetivo seja alcançado.

Existem muitas ferramentas e tecnologias que auxiliam a ação do engenheiro social, como as páginas fakes, phishing e os malwares. Páginas fakes nada mais são do que páginas falsas, que em sua maioria tentam simular o conteúdo e o layout de outros sites importantes, como bancos ou redes sociais. O phishing consiste numa espécie de fraude eletrônica, caracterizada pela tentativa de obter dados pessoais ao se passar por uma pessoa confiável ou empresa, através de uma suposta comunicação oficial, phishing em inglês, significa pescando, ou seja, as informações são “pescadas” por engenheiros sociais através de e-mails ou formulários HTML. Já os malwares que em muitos momentos trabalham lado a lado das páginas fakes e phishing, possuem uma vasta variedade.

Malware é qualquer software malicioso destinado a causar danos em computadores ou servidores de maneira ilegal. Ou seja, são softwares indesejados que possuem o objetivo de apagar dados, roubar informações, alterar ou impedir o funcionamento do sistema operacional, dentre outros.

O malware mais conhecido é o vírus, muitas vezes confundido com os demais malwares. De forma similar ao biológico, o vírus necessita de um hospedeiro, por isso se infiltra nos arquivos e programas os alterando, sempre se multiplicando e se escondendo para que não seja excluído. Os worms se diferenciam do vírus por não necessitarem de um hospedeiro, se replicam e podem excluir arquivos, enviar documentos e deixar o sistema vulnerável a outros tipos de ataque, podendo ser espalhado pela rede, drives, USB e e-mails infectados. Também existem os screenloggers, evolução dos keyloggers que capturam apenas as teclas, os screenlogger capturam a imagem das telas, um indício desses malwares, que preferem passar despercebidos, é lentidão e piscadas na tela. Os ransomwares são malwares que restringem o acesso ao sistema ou a arquivos específicos e cobram um valor resgate para o acesso ser restabelecido. Podem ser instalados através de links falsos, e-mails ou em sites maliciosos. Os spywares, por sua vez, são espiões que tem como principal função capturar informações, pop-ups é um dos sintomas mais comuns, mas também costumam alterar a página de navegação e configurações de pesquisa, os espiões costumam se instalar através de programas sobrepostos ou downloads guiados. Os adwares exibem propagandas e anúncios sem autorização através de pop-ups, enviam spam, fazem redirecionamento automático nas páginas. Cavalo de Tróia ou trojan chegam como presentes disfarçados de outros arquivos, quando aceitos abrem portas para outras pragas, roubam senhas, alteram e destroem arquivos.

São numerosos os tipos de malwares e diversas as formas de contaminação, todavia podemos destacar a contaminação pela exploração de vulnerabilidades existentes nos programas instalados, execução de arquivos previamente infectados obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores através do compartilhamento de recursos.

Para a remoção de malwares em sistemas infectados e a prevenção de possíveis contaminações futuras, foi orientado a utilização de ferramentas como o antivírus, antispyware, virusTotal e o firewall. O antivírus é uma ferramenta desenvolvida para detectar, remover e bloquear ações mal intencionadas provocadas por vírus e outros malwares que prejudicam o bom funcionamento de diversos dispositivos. Já o antispyware é um software de

segurança utilizado para detectar, bloquear ou remover malwares do tipo spyware ou adware, bloqueando pop-ups, barra de ferramentas indesejadas, baixo desempenho e ameaça de segurança provocados por estes softwares maliciosos. O virusTotal é um serviço gratuito online que analisa arquivos e URLs suspeitas e facilita a rápida detecção de vírus e de todos os tipos de arquivos maliciosos até mesmo de falsos positivos, composto por 52 antivírus que escaneam separadamente os arquivos ou URLs, não causando conflito entre os antivírus e tornando-o ainda mais seguro. Por fim, o firewall que é um software ou hardware que gerencia a comunicação com a internet e filtra o fluxo de dados impedindo a passagem de conteúdos maliciosos que possam infectar o computador. Existem dois tipos principais de firewall, o de filtragem de pacotes e firewall de aplicação.

Outro tópico levantado foi a definição, história e riscos da internet, orientando, em seguida, como os usuários podem se prevenir por meio de procedimentos simples e eficazes. Um exemplo básico é o hábito de realizar backup, que consiste na cópia de dados específicos que podem ser restaurados caso ocorra uma perda dos originais devido a problemas nos dispositivos, infecção por malware ou qualquer tipo de exclusão involuntária, e a cópia na nuvem, que nada mais é do que um termo para se referir à Internet. Além dos serviços de armazenamento mais seguros em nuvem, também foi orientado a não divulgação de boatos em rede, que podem provocar diversos problemas, tanto para aqueles que os recebem tanto para aqueles que os distribuem, concluindo na análise e conhecimento das extensões de arquivo, frisando nas extensões de arquivo mais propensas a conter softwares danosos.

A finalização deste módulo foi dada através de procedimentos práticos onde os alunos infectaram com diversos malwares máquinas virtuais e em seguida removeram os programas maliciosos. Limpando a máquina de qualquer dano. Também foi demonstrado um exemplo de esteganografia e a criação de contas de armazenamento em nuvem.

4.3.2 Módulo II – Segurança em Redes Sociais e Dispositivos móveis

O Segundo módulo foi desenvolvido com foco nos dispositivos móveis e a utilização adequada das redes sociais. Para isso, introduzimos conceitos presentes no módulo I fundamentais na compreensão dos tópicos abordados

nesta segunda etapa, como engenharia social, malwares, páginas falsas e phishing.

Desde os primórdios o homem buscou maneiras de se comunicar, necessitando de interações sociais de acordo com suas semelhanças e compatibilidade. É notório se recordar disso para entender o conceito de rede social, que nada mais é do que a definição dada a qualquer grupo reunido que partilhe interesses em comum. Nascermos e crescemos rodeados de redes, como a igreja, clubes de esportes, salas de aulas. Quando essa interação se torna virtual, temos as chamadas redes sociais digitais.

As redes sociais passaram por constantes mudanças, acompanhando a humanidade. Tal qual, continua a passar por uma série de evoluções. Nos dias atuais, as redes sociais digitais, já nos permitem desde a busca de velhos conhecidos e novas amizades, até encontrar um emprego. Ao saber dessa realidade, e da importância dessas redes, é que surgem os cuidados que devem ser tomados na hora de compartilhar informações.

Algumas das ameaças já citadas que se utilizam das redes são as páginas fakes e phishing, que podem simular as próprias páginas das redes sociais imitando desde a URL ao layout, fazendo com que os usuários acreditem que a página é autêntica e insira seus dados verídicos que serão coletados através do phishing e enviados a um engenheiro social.

Além das redes sociais o e-mail, por ser uma importante ferramenta de comunicação, também é alvo de ações maliciosas. O cuidado dos usuários deve ser desde a exibição dos e-mails, até, e principalmente, ao download de anexos.

Nesse módulo também introduzimos conceitos que estão presentes nos princípios da segurança da informação, a autenticidade. Que pode ser dada por três maneiras: por característica, por propriedade e por conhecimento. (ANTUNES, 2014)

- A autenticação baseada no conhecimento: refere-se à autenticação cujos dados de acesso ou o mecanismo, baseia-se em algo que o usuário sabe. É o método mais comum, geralmente utiliza um dado único (e-mail, nome de usuário, id) e uma senha que deve ser de conhecimento apenas do usuário ao qual pertence.

- A autenticação baseada na propriedade: diz respeito à autenticação baseada naquilo que o usuário possui que pode ser um cartão ou qualquer outro dispositivo eletrônico capaz de fazer comunicação com um sistema. Existe a desvantagem que esse objeto pode ser perdido.
- A autenticação baseada na característica: é aquela à qual se baseia em algo que o usuário é. O exemplo mais clássico é a biometria baseada na entrada da digital do usuário. Outros métodos já são conhecidos, como a leitura da íris, batimentos cardíacos, reconhecimento facial, da mão, dentre outros.

Existe ainda autenticação de dois passos, que é um processo que se dá através da autenticação da senha e código relacionado a algo físico do usuário. Por exemplo, quando cadastramos o nosso e-mail e o vinculamos a algum celular e fazemos esta atualização, a conta trabalhará com este tipo de autenticação, na qual, qualquer mudança que requerida pelo usuário – que já autenticou sua senha - também necessitará a autenticação do código que seria enviado ao celular do usuário para comprovar virtual e fisicamente sua autenticidade. Quase todas as redes sociais e serviços web já oferecem a possibilidade de autenticação em dois passos.

Para garantir a segurança de suas contas, existem algumas dicas de elaboração de senhas gerais, por exemplo, é recomendável criar senhas misturando letras maiúsculas e minúsculas, números e sinais de pontuação, a utilização de oito caracteres no mínimo, a troca frequentemente das senhas e a não utilização da mesma senha para outras contas. Caso seja necessário é preferível que o usuário anote a senha e guarde em local seguro, em vez de optar por senhas fracas e de fácil memorização. Também existem técnicas para criar senhas fortes e simples de ser decorada, uma dessas técnicas foi repassada aos interlocutores das aulas ministradas.

Além do cuidado com as contas em redes sociais o cuidado com os dispositivos móveis deve andar lado a lado, visto que se tornaram uma dupla inseparável na sociedade hodierna. Os smartphones invadiram de tal forma nossa vida que levaram muitos computadores ao desuso. Seja pela praticidade ou pela mobilidade, a questão é que depositamos confidencialidades do ramo

pessoal e profissional nestes pequenos aparelhos, sujeitos desde ações de engenheiros sociais até perdas ou roubo.

Sendo assim, buscamos instruir os usuários aos cuidados básicos de prevenção aos danos mais comuns, como a inserção de senha para acessar o dispositivo, o backup frequente dos arquivos, o cuidado com os aplicativos maliciosos e a verificação das permissões que os usuários liberam ao instalarem aplicativos.

Após explanarmos sobre a história e características dos sistemas operacionais mais usados, Android, Windows phone e IOS, focamos na segurança oferecida por cada um dos sistemas operacionais.

Embora o sistema Android busque constantes atualizações e melhorias, sua segurança é constantemente criticada devido a falhas de segurança que são exploradas facilmente por pessoas mal intencionadas. Diferente do Android, o Windows Phone tem uma plataforma desenvolvida de modo a ser seguro por design, muitos recursos de segurança estão ligados por padrão, aplicativos baixados da loja do Windows Phone são testados pela Microsoft e criptografados para garantir que o usuário do dispositivo não instale softwares maliciosos. Já o sistema operacional IOS apesar de ser uma distribuição unix exclusiva da Apple, e diferente do que muitos pensam, também possui vírus, se diferenciando apenas pela quantidade desenvolvida pelos criminosos, que em relação ao Android e Windows Phone é mínima, entretanto a prevenção e proteção é fundamental a todos os dispositivos.

As práticas destinadas a este módulo focaram na segurança pessoal dos participantes, foi ensinado como retirar informações pessoais do Google através da política de remoção Google. Em seguida exploramos as configurações de privacidade existentes nas redes sociais mais utilizadas, demonstrando como e o porquê de manter as informações dos usuários privadas. Além disso, orientamos como filtrar e-mails utilizando antiSpam e passamos vídeos elucidativos a respeito de danos causados pelo uso exacerbado ou descuidado nas redes sociais.

4.3.3 Módulo III – Instalação e Configuração de roteadores wireless em redes domésticas

O terceiro e último módulo desenvolvido buscou pessoas que já possuíam algum tipo de conhecimento na área, principalmente em redes, já que o minicurso trabalhava uma parte mais técnica, a instalação e configuração de roteadores wireless. Mesmo assim, foi realizada uma explanação a respeito de alguns conceitos gerais de redes, para revisão e maior assimilação do conteúdo ministrado.

Começamos com a definição de roteador, equipamento utilizado na comunicação de redes de computadores. Uma rede de computador é por sua vez, um conjunto de dispositivos computacionais capazes de trocar e compartilhar informação. Existem variados tipos de redes, as necessárias para a compreensão deste módulo se restringiram a LAN e WAN, respectivamente rede local e rede geograficamente distribuída. A internet, é o maior exemplo de conglomerados de redes, por funcionar em escala mundial é uma WAN, o que permite seu funcionamento é sua ligação pelo TCP/IP.

Outros conceitos tratados importantes na configuração dos roteadores foram o endereço IP (que é um número de 32 bits existente para cada host de forma única), classes de rede, redes privadas, serviços de rede como DNS, que de forma sucinta funciona como um tradutor de IPs de endereços visitados. Além do DHCP, usado para configuração dos roteadores, preenchendo endereços solicitados automaticamente. As Definições e demonstrações dos equipamentos de redes como Hub, Switch, Roteador, Access Point, redes sem fio, canais e protocolos de segurança WEP, WPA, WPA2, WPS. De maneira geral, às seguintes configurações foram ensinadas.

- Conexão dos cabos e recomendações na hora de ligar o aparelho.
- Acesso a interface de instalação.
- Alteração do usuário/senha do equipamento.
- Modificação do SSID da rede wifi.
- Configuração dos protocolos (preferencialmente WPA2-PSK).
- Configuração da conexão WAN e utilização de frase comprida de difícil adivinhação nas opções de segurança.
- Efetuação dos filtros de máquinas por endereço MAC.

- Desligamento da divulgação do SSID.
- Troca de faixa de endereços fornecidos pelo DHCP.
- Desligamento do DHCP (necessário inserir IPs manualmente nas estações);
- Troca do endereço IP do roteador.

Finalizamos este módulo com a instalação e configuração prática dos roteadores, cada usuário possuía um roteador e seguia os passos já demonstrados em aula e treinados através de emuladores de roteadores web, enquanto auxiliávamos em possíveis dúvidas.

5 RESULTADOS

Com a finalização de cada minicurso foi aplicado um questionário a respeito, com espaço para críticas e sugestões. De modo geral, o minicurso foi satisfatório atendendo às expectativas dos interlocutores presentes nas aulas.

Algo levantado em alguns questionários foi a sugestão de disponibilizar material impresso para o acompanhamento dos minicursos, também foi colocado a sugestão dos minicursos terem uma maior duração, juntamente com a integração dos três módulos, demonstrando interesse dos alunos na participação de módulos que já haviam sido passados, ou que seriam em um momento posterior.

Ao final do projeto tivemos três apostilas revisadas e atualizadas; Introdução à segurança da informação, a qual foi acrescentado, como exemplo, a pesquisa sobre os melhores antivírus no meio digital, mais vídeos explicativos que auxiliaram no entendimento e assimilação do conteúdo, como também uma explanação acerca da Deep Web, onde muitos ainda não conhecem ou compreendem esse meio; Segurança dos dispositivos móveis em redes sociais, atualizamos a linha do tempo das redes mais conhecidas, além de acrescentar as medidas de proteção a cerca dos sistemas operacionais Windows Phone e IOS; e por último, Configuração e instalação de roteadores wireless. Também revisamos e desenvolvemos novos materiais para ministração das aulas, como atualização de slides, novos vídeos e exemplos, e conseguimos repassar para os participantes aquilo que foi proposto em nossos objetivos.

6 CONSIDERAÇÕES FINAIS

De acordo com o desenvolvimento deste projeto, podemos perceber os variáveis riscos que as pessoas estão submetidas diariamente com o uso inadequado das tecnologias, juntamente com a importância de fornecer o conhecimento básico a respeito da segurança da informação para a população.

Podemos considerar que o projeto atendeu seu objetivo, transmitindo essas informações aos alunos, servidores e comunidade entorno do campus. O material desenvolvido poderá servir de consulta e novas aplicações, sejam elas implementadas ou não.

6.1 ATIVIDADES FUTURAS

As sugestões propostas em possíveis trabalhos futuros é a atualização do material - já que o mundo virtual e o desenvolvimento de novas tecnologias apresentam avanço exponencial e extremamente veloz - juntamente com a continuação dos minicursos e extensão, com aplicação de palestras em escolas, alcançando assim o maior número de pessoas possível. Também sugerimos o desenvolvimento de novas metodologias educacionais, como a criação de jogos e aplicativos que tratem sobre a segurança da informação de forma mais dinâmica.

6.2 LIÇÕES APRENDIDAS

Além de servir como trabalho de conclusão de curso, para a obtenção do diploma de técnico em informática, este projeto de extensão nos proporcionou a oportunidade de desenvolver habilidades além daquelas propostas e ensinadas em nossa grade, como conhecimentos mais específicos acerca da segurança, a comunicação na ministração das aulas e o papel social que devemos exercer enquanto alunos, como agentes modificadores de nossa realidade.

REFERÊNCIAS

ALLEN, Malcolm. **Social Engineering: A Means to Violate a Computer System.** **SANS Institute InfoSec Reading Room.** Disponível em: <http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-means-violate-computer-system_529>. Acesso em: 06 de nov. de 2016.

ANTUNES, BRUNO. **Conheça os 3 tipos de métodos de autenticação.** Disponível em: <<http://segurancaemsimplesatos.com.br/blog/conheca-os-3-tipos-de-metodos-de-autenticacao/>> Acesso em: 05 de nov de 2016.

ARTZ, D. **Digital Steganography: Hiding Data within Data.** IEEE Internet Computing, p. 75-80, maio/junho 2001.

BANDEIRA, Denise. **Material didático: conceito, classificação geral e aspectos da elaboração.** Disponível em: <<http://www2.videolivrraria.com.br/pdfs/24136.pdf>>. Acesso em: 06 de nov. de 2016.

MARTINI, Renato. **Criptografia e cidadania digital.** Rio de Janeiro: Ciência Moderna, 2001. 164 p.

MITNICK, Kevin D.; SIMON, William L.. **A arte de enganar.** São Paulo: Pearson Makron Books, 2003. 284 p. MORAES, Alexandre. **Segurança em redes: fundamentos.** São Paulo: Érica Ltda, 2010.

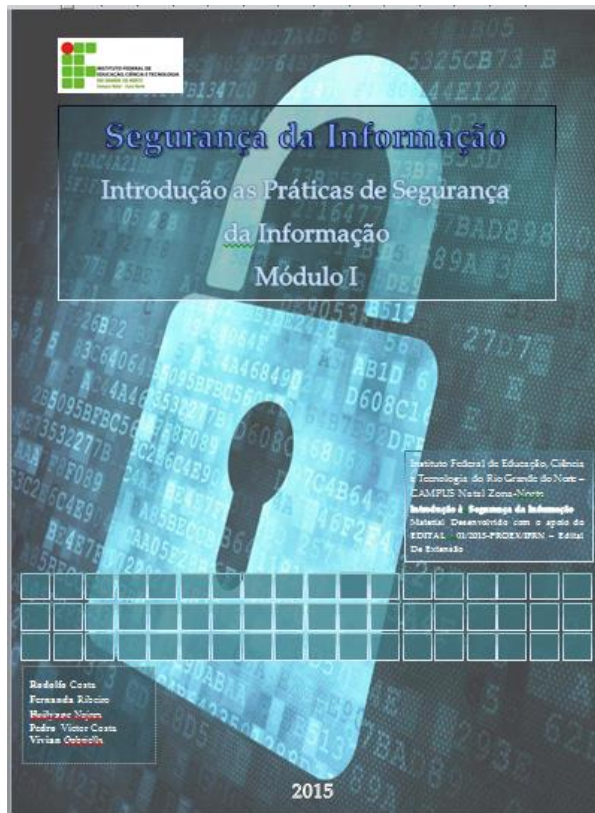
OTTE, Peter. **A super-rodovia da informação: além da Internet.** Rio de Janeiro: Axcel Books, 1995. 241 p.

PEIXOTO, Mário C.P. **Engenharia Social e Segurança da Informação na Gestão Corporativa.** Rio de Janeiro: Brasport, 2006. Disponível em: <<http://www.cippguide.org/2010/08/03/cia-triad/>>. Acesso em: 25 de nov. de 2016

SIMON, William L.. **A arte de invadir.** São Paulo: Pearson Prentice Hall, 2006. 236 p.

VASCONCELLOS, Márcio José Accioli de. **A internet e os hackers: ataques e defesas.** 3. ed. São Paulo: Chantal, [200-?]. 336 p.

APÊNDICE A – Apostila do primeiro módulo





Sumário	
Unidade 1	3
↳ INTRODUÇÃO	4
Segurança Da Informação	4
A Segurança Da Informação No Tempo	4
Segurança Da Informação Científica	5
↳ TECNOLOGIA DA INFORMAÇÃO	6
↳ INVASÃO	7
↳ CRIPTOGRAFIA	8
↳ ESTEGANOGRAFIA	8
↳ ENIGMA	9
↳ ENGENHARIA SOCIAL	10
O Comportamento Humano	10
Como Agem Os Engenheiros Sociais	12
↳ TERMOS DA SEGURANÇA DA INFORMAÇÃO	13
Unidade 2	14
↳ O QUE É INTERNET?	15
Contexto Histórico	15
↳ AMEAÇAS NA INTERNET	17
Página Fake	17
Phishing	17
Downloads De Arquivos Maliciosos	18
Botto	20
Pop-ups	20
↳ DEEP WEB: UMA LENDA CIBERNÉTICA	22
↳ BACKUP	24
Armazenamento Em Nuvem	24
Tutorial De Armazenamento Em Nuvem	25
Unidade 3	27
↳ MALWARES	28
↳ TIPOS DE MALWARES	28

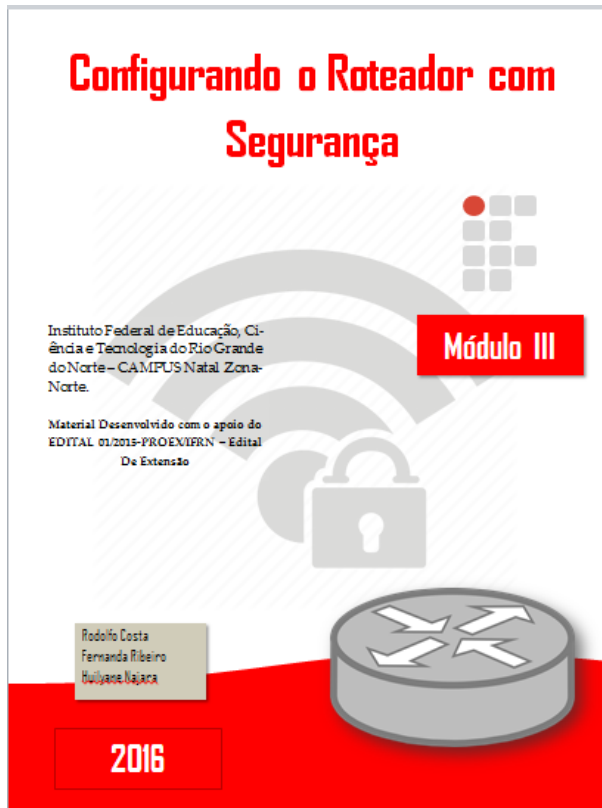
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte - CAMPUS Natal Zona-Nova
Curso Segurança da Informação - Módulo I

1

APÊNDICE B – Apostila do segundo módulo

<h1 style="text-align: center;">Segurança em Redes Sociais e Dispositivos Móveis</h1>	
	
<p>Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte - CAMPUS Natal Zona-Norte</p>	
<p>Material Desenvolvido com o apoio do EDITAL 01/2015-PROEX/FRN - Edital De Extensão</p>	
<h2 style="background-color: #004a7c; color: white; padding: 5px;">Módulo II</h2>	
	
<p>Rodolfo Costa Fernanda Ribeiro Nullyane Najara Pedro Costa Yvian Gabriella</p>	
<p>2015</p>	
<h3 style="text-align: right;">Sumário</h3>	
<p>UNIDADE I – ALGUNS CONCEITOS SOBRE SEGURANÇA DA INFORMAÇÃO..... 5</p>	
<p>Invasão..... 6</p>	
<p>Malhaca..... 7</p>	
<p>Engenharia Social..... 8</p>	
<p> O que é engenharia social e por que é perigosa?..... 8</p>	
<p> Como o comportamento humano influencia esse processo?..... 9</p>	
<p> Como agir em engenharia social?..... 9</p>	
<p>UNIDADE II – HISTÓRICO DAS REDES SOCIAIS..... 12</p>	
<p>As redes sociais antes de m e internet..... 12</p>	
<p> Surgimento..... 12</p>	
<p> Evolução..... 12</p>	
<p> Linha Do Tempo..... 13</p>	
<p>As principais Redes Sociais..... 14</p>	
<p> Classificados.com - (1995)..... 14</p>	
<p> ICQ - (1996)..... 14</p>	
<p> AOL Instant Messenger - (1997)..... 15</p>	
<p> Sixdegrees - (1997)..... 15</p>	
<p> Friendster - (2002)..... 16</p>	
<p> MySpace - (2003)..... 17</p>	
<p> LinkedIn - (2003)..... 17</p>	
<p> Orkut - (2004)..... 18</p>	
<p> Facebook - (2004)..... 18</p>	
<p> Youtube - (2005)..... 19</p>	
<p> Badoo - (2006)..... 20</p>	
<p> Twitter - (2006)..... 20</p>	
<p> Tumblr - (2007)..... 21</p>	
<p> WhatsApp - (2009)..... 22</p>	
<p> Pinterest - (2010)..... 22</p>	
<p> Instagram - (2010)..... 23</p>	
<p> Google+ - (2010)..... 24</p>	
<p> Ask.fm - (2010)..... 24</p>	
<p> Snapchat - (2011)..... 25</p>	
<p> Tinder - (2012)..... 26</p>	
<p> Telegram - (2013)..... 27</p>	
<p> Secret - (2013)..... 27</p>	
<p>2</p>	
<p><small>Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte - CAMPUS Natal Zona-Norte Página Seguranca da Informaçao: Módulo II</small></p>	

APÊNDICE C – Apostila do terceiro módulo



Conceitos: Roteador e Internet	5
REDES LAM E WAM	5
ENDEREÇAMENTO IP	5
Notação Decimal Pontilhada	7
Classes de Redes	8
Rede privada	8
Gateway	9
SERVIÇOS DE REDE	13
DNS	15
DHCP	17
EQUIPAMENTOS DE REDE	17
Hub	20
Switch	22
Roteador	22
Access Point	26
REDES SEM FIO	28
Redes sem fio 802.11	28
Padrão 802.11ac	29
SSID	31
PROTOCOLOS DE SEGURANÇA	33
WEP	33
WPA	33
WPA2	33
WPS	34
CONFIGURAÇÕES DE ROTEADORES	34
Instalando o Roteador	36
Acessando o Roteador	36
Configurando o Roteador	37
Recuperando as configurações de fábrica	39