UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS VII – GOVERNADOR ANTÔNIO MARIZ
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS
CURSO DE LICENCIATURA PLENA EM COMPUTAÇÃO

JESSICA THAILANA DA SILVA ARAUJO

SEGURANÇA DA INFORMAÇÃO: OS CUIDADOS NO AMBIENTE DIGITAL

PATOS – PB
2015

JESSICA THAILANA DA SILVA ARAUJO

SEGURANÇA DA INFORMAÇÃO: OS CUIDADOS NO AMBIENTE VIRTUAL

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Licenciatura em Ciências da Computação da Universidade Estadual da Paraíba, Campus VII, Patos - PB, como parte das exigências para obtenção do Título de graduada em Licenciatura em Computação.

Prof. Orientador: Dr. Wellington Candeia de Araújo

PATOS – PB
2015

É expressamente proibida a comercialização deste documento, tanto na forma impressa como eletrônica. Sua reprodução total ou parcial é permitida exclusivamente para fins acadêmicos e científicos, desde que na reprodução figure a identificação do autor, título, instituição e ano da dissertação.

A663s Araújo, Jessica Thailana da Silva
Segurança da Informação [manuscrito] : os cuidados no Ambiente Digital / Jessica Thailana da Silva Araujo. - 2015.
42 p. : il. color.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Computação) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas, 2015.
"Orientação: Prof. Dr. Wellington Candeia de Araújo, CCEA".

1. Ameaça virtual. 2. Crime virtual. 3. Segurança da Informação. I. Título.

21. ed. CDD 005.8

uepb
Universidade
ESTADUAL DA PARAÍBA

Jessica Thailana da Silva Araujo

SEGURANÇA DA INFORMAÇÃO: OS CUIDADOS NO AMBIENTE DIGITAL

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Computação da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Licenciado em Computação

Aprovado em 19 de junho de 2015

uepb
Universidade
ESTADUAL DA PARAÍBA

BANCA EXAMINADORA

Wellington C. Araújo.

Wellington Candeia de Araújo
(Orientador)

Rodrigo Alves Costa
(Examinador)

Rosângela de Araújo Medeiros
(Examinadora)

uepb
Universidade
ESTADUAL DA PARAÍBA

DEDICATÓRIA

A Deus, por ter me concedido o dom da vida, e a minha família em especial minha mãe Lucia de Fátima, propulsora de valores éticos que interagem na minha personalidade no anseio de uma vida melhor.

AGRADECIMENTOS

A Deus, por me permitir ser quem sou, da maneira que sou.

Ao meu orientador, Prof. Dr. Wellington Candeia de Araújo pela dedicação e contribuição, para a concretização deste trabalho.

Àqueles da minha família e amigos que, em algum momento dessa jornada, estiveram ao meu lado me apoiando.

Aos colegas e professores da UEPB, que conviveram comigo, pela confiança, pelo apoio, estimulo informações a realização desta pesquisa.

A todos que confiaram e contribuíram direto ou indiretamente para a realização e êxito desse trabalho. Muito Obrigada.

“Risco é a incerteza inerente a um conjunto de possíveis consequências (ganhos e perdas), as quais ocorrem como resultado de escolhas e decisões exigidas por toda corporação. Risco está relacionado à escolha, não ao acaso”

Ives P. Mulle.

RESUMO

O crescimento progressivo da tecnologia está permitindo uma imensa transformação no processo de informatização, porém problemas com a segurança da informação também cresce em escalas gigantescas, criminosos usam o poder intelectual que possuem ou agem de má fé para atingir países, nações, empresas, pessoas. O presente estudo tem como objetivo realizar um levantamento bibliográfico sobre os perigos no ambiente virtual e os cuidados que garantam a segurança da informação. Trata-se de uma pesquisa bibliográfica a partir de material já publicado, constituído principalmente de livros-técnicos, artigos, periódicos e material disponível na internet em sites de pesquisa específicos. Os resultados evidenciados mostram que a espionagem frequentemente é feita por pessoas que tem acesso a informações privilegiadas, mas também pode ser feita por empresas para conseguir vantagens em relação às empresas concorrentes conhecido como espionagem comercial ou industrial. Percebeu-se que na sociedade da informação, ao mesmo tempo que as informações são consideradas o principal patrimônio de uma organização estão também sobre constante risco. Com isso a segurança da informação tornou-se um ponto relevante para a sobrevivência das instituições. Conclui-se que, no Brasil, as políticas públicas direcionadas, ao combate de crimes e ameaças virtuais estão vigorando, a exemplo da Nº 12.737- Lei Carolina Dieckmann que trata da invasão de dispositivo informático e o Projeto de Lei nº 6630/2013 de autoria do Deputado Romário que trata da divulgação indevida de material íntimo.

PALAVRAS-CHAVE: Ameaça virtual. Crime virtual. Segurança da Informação.

ABSTRACT

The progressive growth of technology is allowing an immense transformation in the computerization process, but problems with information security also grows into gigantic scales, criminals use the intellectual power they possess or act in bad faith to reach countries, nations, companies, people. This study aims to conduct a literature about the dangers in the virtual environment and care to ensure information security. This is a literature search from already published material, consisting mainly of technical-books, articles, journals and material available on the internet in search of specific sites. The disclosed results show that espionage is often made by people who have access to privileged information, but can also be made by companies to achieve advantages over competitors known as commercial or industrial espionage. It was noticed that in the information society, while the information is considered the main asset of an organization are also under constant risk. With that information security has become an important issue for the survival of the institutions. We conclude that, in Brazil, targeted public policies to combat crime and cyber threats are in effect, such as the No. 12.737- Law Carolina Dieckmann which deals with the computing device of invasion and Bill No. 6630/2013 of authorship Romario Mr dealing with the improper disclosure of intimate material.

KEYWORDS: virtual threat. Cybercrime. Information security.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A informática proporcionou uma revolução digital, acelerando o ímpeto das invenções, possibilitando o surgimento de uma nova realidade virtual na condição de novas condutas.

A introdução de novas tecnologias e o crescimento assustador no número de usuários na grande rede acabou de abrir portas ao aparecimento de condutas ilícitas e criminosas oriundas de usuários mal intencionados que se favorecem do conhecimento e brechas nos sistemas, para inserir atividades.

A segurança da Informação possui vários aspectos importantes, porém destacam-se três: a confidencialidade, a integridade e a disponibilidade. A confiabilidade é a capacidade de um sistema de permitir que os usuários acessem determinadas informações impedindo que outros não autorizadas a vejam. A integridade o indivíduo passa a ter certeza de que as informações enviadas por ele pela internet chegam ao interlocutor sem alterações maliciosas.

> Os avanços científicos e tecnológicos dos últimos 30 anos promoveram um aumento substantivo por produtos e serviços baseados em tecnologia, especialmente os relacionados computação, telecomunicações, automação, robótica, bioinformática, mecatrônica, nanotecnologia. (BRASIL ,2010, p.17)

Qualquer reflexão advinda da sociedade da informação deve apoiar-se numa análise da mutação contemporânea da relação com o saber, em que a velocidade do surgimento e da renovação dos saberes é a avassaladora. Constata-se que a maioria das competências adquiridas no início do percurso profissional será praticamente obsoleta ao final da carreira. Outro fenômeno refere-se à natureza do trabalho: trabalhar, atualmente, equivale cada vez mais, a aprender, transmitir saberes e produzir conhecimentos (BRASIL, 2010).

> Soma-se, ainda, que o ciberespaço ou (espaço cibernético) suporta tecnologias que ampliam, exteriorizam e alteram muitas funções cognitivas humanas, a memória (bancos de dados, hipertextos, fichários digitais, de todas as ordens), a imaginação (simulações, a percepção (sensórias digitais, telepresença, realidade virtuais), os raciocínios (inteligência artificial, modelização de fenômenos complexos). (BRASIL , 2010,p.17)

Para Pierre Levy, espaço cibernético “é entendido numa visão de inteligência coletiva e mutante, totalmente baseados em redes e troca de saberes”. Em decorrência dos avanços tecnológicos e da velocidade com o que os mesmos vêm ocorrendo é possível verificar um movimento acentuado de re-arrajo das preposições das noções em termos de segurança e defesa. (BRASIL ,2010, p.19)

Na sociedade da informação, ao mesmo tempo em que as informações são consideradas principal patrimônio de uma organização, estão também sob constante risco, como nunca antes. Com isso, a segurança da informação tornou-se um ponto crucial para a sobrevivência das instituições.

Sabe-se que atualmente, os sistemas de informação adquiriram vital importância para a sobrevivência da maioria das organizações modernas. Nelas, sem computadores e redes de comunicação, a prestação de serviços da informação pode se tornar inviável.

Neste sentido, pode-se observar que uma das mais importantes ferramentas de comunicação é a internet. Com ela é possível trocar informação com pessoas de qualquer parte do mundo, como bem frisa Gustavo Testa Corrêa (2000, p. 8).

> A internet é um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina a qualquer outra máquina conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento.

É importante destacar que é preciso ter cautela e evitar fornecer dados pessoais, senhas e números de cartão de crédito, por exemplo. Dessa forma é preciso ficar atento ao disponibilizar informações. Esses dados se tornam em informações valiosas. Com eles as pessoas acabam disponibilizando suas informações na rede ou cedendo dados para empresas de forma indireta.

Atualmente existe um mercado em que essas informações são vendidas “Na Rua Santa Efigênia, no Centro de São Paulo é possível comprar informações dados sigilosos de bancos, empresas e órgãos públicos as informações são vendidas em CDs durante todo o dia.” (PORTAL GLOBO 2007).

Como quase todas as atividades passaram a ser realizados através de um sistema computacional, há uma preocupação de se manter seguras as informações que circulam na rede de computadores. Elas passaram do meio físico para o meio digital, não estando mais nos armários e impressas em papeis, mas em servidores, podendo ser acessadas de qualquer lugar.

Constantemente, questões sobre a segurança da informação têm sido um tema fortemente abordado nas mídias. Os números de crimes digitais, vazamento de informações, vêm aumentando devido ao crescimento do número de usuários na rede como também os recentes casos de espionagens, deixando claro a presente questão da insegurança digital.

Diante deste contexto delimita-se a problemática da pesquisa em torno de: Quais são as informações necessárias encontradas na literatura referentes à segurança da informação do ambiente virtual?

Neste estudo busca se provocar um debate reflexivo sobre a segurança da informação e os cuidados no ambiente virtual, considerando imperiosa a abordagem de tal temática.

A escolha do tema surgiu da necessidade de verificar se estão sendo adotadas medidas de segurança para os cuidados de segurança no ambiente virtual, tendo em vista o aumento dos números de usuários na rede e com isso o crescimento dos casos de crimes digitais

O objetivo geral do presente estudo foi realizar um levantamento bibliográfico sobre os perigos no ambiente virtual e os cuidados que garantam a segurança da informação. Para concretização deste objetivo desmembraram-se os seguintes objetivos específicos: verificar métodos e técnicas da segurança da informação; analisar as políticas públicas direcionadas a segurança do ambiente virtual.

2 CONTEXTUALIZANDO A SEGURANÇA DA INFORMAÇÃO

2.1 Informação E Tecnologia

Vive-se nos dias atuais com os avanços da tecnologia, especificamente, das Tecnologias de Informação e Comunicação (TIC) grandes cenários de mudanças na sociedade. Segundo Pinheiro (2007, p.29) “a revolução da informação, iniciada em 1957, com a criação do primeiro *mainframe*, marcou o começo da digitalização da sociedade. Hoje, vivemos uma interdependência completa, globalizada, interativa e em rede.”

Diante dessa sociedade em constante e rápida transformação percebe-se que a influência exercida pelos recursos das novas tecnologias no comportamento dos indivíduos faz com que sejam necessárias mudanças efetivas na maneira de ver o mundo.

Ainda de acordo com Pinheiro (2007, p.13)

> A informática surgiu da necessidade de se beneficiar e trazer facilidades para a vida do homem em suas atividades cotidianas e, principalmente, em seus afazeres mais repetitivos. O computador é, assim, o dispositivo que permite o tratamento de dados e, por conseguinte, das informações.

Com os avanços das tecnologias é preciso se adequar a essa nova forma de fazer coisas simples antes feitas fisicamente como realizar uma compra em uma loja. Torna-se notório que os avanços tecnológicos e suas influências no desenvolvimento da humanidade afetam o modo de realizar atividades normais.

2.2 A Tecnologia Como Recurso

Silva (2012, p.15) a invenção do primeiro computador pessoal com *mouse* e *interface* gráfica pela *Xerox,* tem-se finalmente o surgimento da internet, evento este que causou uma verdadeira revolução na vida das empresas e das pessoas, na

medida em que propiciou não somente o encurtamento das distâncias, como também transmissão de texto, voz e imagem, a denominada multicomunicação.

As telecomunicações proporcionam à oportunidade de se manter em contato com qualquer pessoa em qualquer lugar do mundo, e com isso pode-se ter uma troca de informações. Criando ambientes virtuais de amizade, relacionamentos pessoais quebrando limitações geográficas e possibilitando oportunidades de compartilhamento entre várias pessoas sem a necessidade de estar no mesmo local e na mesma hora é o exemplo de grupos no aplicativo de trocas de mensagens *Whatsapp* através de *smartphones*.

Nesses últimos anos houve mudanças significativas com os avanços tecnológicos, os recursos disponíveis, a globalização, inclusão digital tudo isso influencia na sociedade. Atualmente quase tudo gira em torno das tecnologias.

Neste contexto, Brasiliano (2002, p.27), diz que “a globalização se constitui em uma peça essencial para explicar os fenômenos e processos mundiais no início deste novo milênio.”

Apreende-se da citação do autor que no mundo globalizado, torna-se importante ter claro e objetivamente a explicação de fenômenos, processos e as inúmeras mudanças da sociedade

2.3 Segurança Da Informação

A segurança da informação faz referência a proteção de informação tanto no ambiente coorporativo quanto no doméstico, protegendo-as de ameaças, diminuindo os riscos e os danos. Informação é um conteúdo que tem valor material ou moral para uma empresa ou para uma pessoa, podendo ser restrita, pública, confidencial, interna e secreta, como as usada na área militar. A segurança entra justamente nessa parte, proteger o que é importante tanto para uma pessoa quanto para uma organização.

Pela Medida Provisória n° 2.216-37 de 31 de Agosto de 2001 foi criado o Gabinete de Segurança Institucional da Presidência da República. Uma de suas competências é regularizar a segurança na administração pública. Na medida

provisória é citado o Decreto Nº 3.505/2000 que fala sobre o conceito de segurança da informação.

> 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.

Portanto, é a prevenção de bens, valores, direitos digitais contra o uso ou acesso não autorizado. Sabe-se que existem vários mecanismos para defender um sistema, pois um só não dá conta tendo em vista que ataques a grandes servidores vem de todas as partes do mundo. Para proteger tem-se que conhecer as ameaças para saber com o que está lidando, assim, pode se montar estratégias de combate as mesmas.

Ainda existe ameaças físicas e lógicas: as físicas são problemas com hardwares e acontecimentos da natureza que pode vir a destruir o sistema ocasionando perda de dados e informações. As lógicas são *malwares* (programa mal intencionado) e técnicas usadas por *hackers*. As causas de sistemas serem facilmente invadidos são a gestão de senhas fracas, apesar disso vir melhorando bastante, por que é uma tecla que especialista vem falando; aumentar o nível de segurança de senhas dificulta de certa forma o acesso de intrusos.

A segurança da informação se baseia em princípios que devem prevalecer para se manter seguro às informações. Para Oliveira (2001, p.09) os elementos básicos da segurança da informação são:

- Confidencialidade: proteger informações confidenciais contra revelação não autorizada ou captação compreensível;
- Disponibilidade: garantir que informações e serviços virtuais estejam disponíveis quando requerido;
- Integridade: manter informações e sistemas computadorizados, dentre outros, ativos, exatos e completos.

Com esses três elementos têm-se uma maior garantia de que as informações estão seguras, inclusive ter a informação disponível, ou seja, vinte e quatro horas por dia, sete dias da semana, a confidencialidade da mesma sem que seja compartilhada com que não tem autorização e integridade dela, somente modifica quem tem permissão os dados não podem ser alterados, isso permite uma maior segurança. Se um sistema atender a esses princípios ele é dito como seguro.

Porém não existe sistema totalmente seguro quando não é a falha da política de segurança proposta pela empresa ou corporação é o quesito fator humano, por mais que exista ferramentas de proteção sofisticada interfere, pois, informações valiosas podem facilmente ser vazadas por funcionários mal intencionados ou sem o menor preparo necessário.

Segundo Oliveira (2001, p.11),

> O único sistema totalmente seguro é aquele que não possui nenhuma forma de acesso externo, está trancado em uma sala totalmente lacrada de qual uma única pessoa possui a chave. E esta pessoa morreu no ano passado.

Percebe-se que a segurança da informação não está limitada somente a formatos digitais e sistemas computacionais. Cada informação deve ser estabelecida um nível de proteção, quanto mais a informação for valiosa precisará de uma maior proteção. Há várias formas de proteger um sistema *firewalls*, políticas de informação, criptografia, ferramentas modernas, antivírus.

2.4 Políticas De Segurança Da Informação

Para se colocar em prática métodos de segurança é preciso ter toda uma política envolvida, que são as regras determinadas pelo pessoal de TI da empresa em questão ou instituição, o que pode e o que não pode se fazer, geralmente é um documento feito por profissionais qualificados e especialistas no ramo de segurança que constitui essas normas, ficam estabelecidos neste documento as regras, avisos, normas.

Um exemplo de uma política de segurança em uma empresa é a não permissão de uso pessoal nos computadores da empresa. Neste caso, os funcionários não podem acessar e-mail ou redes sociais no âmbito corporativo não sendo também permitido divulgar informações confidenciais da empresa nem vazar o que foi dito em reuniões.

Segundo Mitnick e William (2003, p.211)

> As políticas de segurança são instruções claras que fornecem as orientações de comportamento do empregado para guardar as informações, e são um elemento fundamental no desenvolvimento de controles efetivos para contra-atacar as possíveis ameaças à segurança.

A segurança é um fantasma quando os funcionários de uma empresa não conhecem as políticas de segurança que constituem aquela empresa. Porém, não basta ter os melhores equipamentos do mercado nem os melhores profissionais, quando se trata do termo engenharia social, é necessário que a política seja reforçada, seguir à risca as normas e conscientizar o pessoal.

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis. (MITNICK; SIMON, 2003, p. 3).

A política é a forma como a empresa deve ser protegida quais ferramentas usar, qual setor responsável por cada área, quem pode ter acesso ao que, quem não pode. O planeta está mais inteligente e com isso os ataques estão mais sofisticados com isso é necessário ter uma política eficiente e atual e não adianta ter em sua empresa políticas voltadas para formas de ataques ultrapassadas, os próprios *hackers* vem se qualificando.

Figura 1- Ambiente sem políticas de segurança.

Fonte: (PEIXOTO, 2006)

Tudo que desobedecer as normas descritas na política pode ser considerado um incidente, na política da empresa também deve estar claro qual penalidade aplicar para quem desobedecer as normas. A segurança de uma empresa não pode ser praticada somente pelo pessoal de TI, todos os funcionários dela precisam ter essa preocupação com a segurança, porque uma empresa não é constituída somente pelas equipes dessa área. Alguns funcionários são leigos no assunto, aí que é preciso seguir à risca a política de segurança da informação.

3 AMEAÇAS E CRIME NO AMBIENTE VIRTUAL

3.1 Ameaças Virtuais

Ferreira (2007) atribui ao termo ameaça como sendo “palavra ou gesto que anuncia a alguém o mal que lhe queremos fazer” Na linguagem virtual, ameaçar uma pessoa via e-mail ou postagem em site, por exemplo, afirmando que ela será vítima de algum mal.

Inellas (2009, p.77) afirma que “sua conduta é a de ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave. Portanto, a finalidade do delito ou ameaça é atemorizar a vítima”.

Essas citações demonstram claramente as definições para o termo ameaçar no sentido amplo, e, também direcionado a ambiente virtual, temática foco desse estudo. Bem como mostrar os possíveis motivos que levam os atacantes a deferir ataques na internet.

Segundo a Cartilha de Segurança para Internet: Ataques na Internet, os motivos que levam os atacantes a desferir ataques na Internet são bastante diversos, variando da simples diversão até a realização de ações criminosas. Alguns exemplos são apresentados a seguir.

- Demonstração de poder: mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente.
- Prestígio: vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar sites considerados visados ou difíceis de serem atacados; disputar com outros atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo.
- Motivações financeiras: coletar e utilizar informações confidenciais de usuários para aplicar golpes.

- Motivações ideológicas: tornar inacessível ou invadir sites que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia.
- Motivações comerciais: tornar inacessível ou invadir sites e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas, Cert.br (2012.p17).

3.2 Crimes Virtuais

Vários estudiosos na área apresentam suas definições para o termo crimes virtuais, dentre eles, citam-se:

Paiva (2006, p.5), diz que:

> Apesar da discrepância doutrina, são denominadas de ‘crimes de informática’ as condutas descritas em tipos penais realizadas através de computadores ou voltados contra computadores, sistemas de informática ou os dados e as informações neles utilizados (armazenamento ou processamento).

Segundo Guimarães (2000,p.120)

> Em vez de pistolas automáticas e metralhadoras, os ladrões de banco podem agora usar uma rede de computadores e sofisticados programas para cometer crimes. E o pior, fazem isso impessoalmente, de qualquer continente, sem a necessidade de presença física, pois atuam num “território” sem fronteiras, sem leis, acreditando que, por isso, estão imunes ao poder de polícia.

Pelo exposto, pode-se entender que os crimes digitais normalmente acontecem por parte de indivíduos mal intencionados com a finalidade de lesar pessoas legais com relação a segurança da informação.

Na maioria das vezes, essas pessoas são lesadas por si próprias, quando inocentemente dispõem seus dados na rede. Esses criminosos atingem também

instituições privadas e públicas de alto nível, o que demonstram que toda sociedade pode ser vítima desses tipos de crime.

Para melhor esclarecimento sobre crimes, cita-se o exemplo do que ocorreu com a atriz Carolina Dieckmann, que de tão grave chamou a atenção das autoridades competentes, tornando-se lei que será apresentada a seguir.

3.2.1 Lei brasileira nº 12.737- Lei Carolina Dieckmann

Indubitavelmente, a internet revolucionou os modelos de comunicação, permitindo também que novas formas de entretenimento fossem desenvolvidas, assim como o acesso a informações dos mais variados conteúdo. Sabe-se que são inúmeros os benefícios da internet para os indivíduos, mas ocorrem também manifestações contrárias, ou seja, psicopatológicas vinculadas ao campo eletrônico as quais vem sendo discutidas, a exemplo da dependência de jogos eletrônicos e cibercrimes.

A legislação deriva-se segundo o wikipedia do Projeto de Lei 2.783/2011, apresentado em 29 de novembro de 2011, pelo Deputado Paulo Teixeira (PT – SP), que tramitou em regime de urgência e em tempo recorde no Congresso Nacional em comparação com outros projetos informáticos que as Instituições de Leis apreciavam, a exemplo do PL 84/1999, a Lei Azeredo que dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências, também transformada em Lei Ordinária.

Os crimes ou delitos previstos na Lei Carolina Dieckmann:

> Art. 154 A – invasão de dispositivo informático alheio conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança e com a finalidade de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tática do titular do dispositivo ou instalar vulnerabilidade para obter vantagem ilícita pena-detenção de 3 (três) meses a 1 (um) ano e multa.
> Art. 266 – Interrupção ou perturbação de serviço telegráfico, informático, telemático ou de informação de utilidade pública pena-detenção, de 1 (um) a 3 (três) anos e multa.
> Art. 298 – Falsificação de documentação particular/ cartão – pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa. A referida Lei entrou em vigor no dia 02/04/2013.

De modo geral, pode-se perceber que a Lei 12.737 Lei referido estabelece penas de multa e prisão para vários tipos de crimes digitais. É a primeira a acrescentar no Código Penal dispositivos que tipificam determinados delitos informáticos (ou mais precisamente cibercrimes). Na norma, o legislador preocupa-se com a invasão a computadores para fins de informações pessoais, bem como equipara a clonagem de caráter à falsificação de documentos particular, além de abordar os casos de interrupção de serviços de comunicação.

Neste contexto, as penas referentes aos novos crimes variam de acordo com a gravidade da conduta do infrator, e englobam hipóteses de detenção ou de reclusão e aplicação de multa. Ademais, buscou-se prever algumas causas de aumento da pena, como os casos de divulgação, comercialização ou transmissão a terceiros, a qualquer título, os dados ou informações obtidas. Caso o crime cometido esteja relacionado contra certas autoridades dos Poderes Executivo, Legislativo e Judiciário, a punição pode ser majorada.

Na atualidade, um dos temas mais comentado e debatido entre as esferas federal, estadual e municipal é o de crime virtual. Vários Projetos de Lei e Leis tramitam, uns já aprovados como a Lei citada anteriormente, e o Projeto de Lei nº 6630/2013, qual será apresentado a seguir.

3.2.2 Projeto de Lei nº 6630/2013

O Projeto de Lei nº 6630/2013 de autoria do Deputado Romário (PSB – RJ) acrescenta artigo ao Código Penal, tipificando a conduta de divulgar fatos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima e dá outras providências. A seguir apresenta-se na íntegra como foi decretado pelo Congresso referido Projeto.

O Congresso Nacional decreta:

> Art. 1º Esta lei torna crime a conduta de divulgar fotos ou vídeos com cena de nudez ou ato sexual sem autorização da vítima.
> Art. 2º O Decreto-lei nº 2848, de 7 de dezembro de 1940, passa a vigorar acrescido do seguinte art. 216-B: “Divulgação indevida de material íntimo Art. 216-B. Divulgar, por qualquer meio, fotografia, imagem, som, vídeo ou qualquer outro material, contendo cena de nudez, ato sexual ou obsceno sem autorização da vítima. Pena –

> detenção, de um a três anos, e multa. §1º Está sujeito à mesma pena quem realiza montagens ou qualquer artifício com imagens de pessoas. §2º A pena é aumentada de um terço se o crime é cometido: I - com o fim de vingança ou humilhação; II – por agente que era cônjuge, companheiro, noivo, namorado ou manteve relacionamento amoroso com a vítima com ou sem habitualidade; §3º A pena é aumentada da metade se o crime é cometido contra vítima menor de 18 (dezoito) anos ou pessoa com deficiência"(NR.)
> Art. 3º O agente fica sujeito a indenizar a vítima por todas as despesas decorrentes de mudança de domicílio, de instituição de ensino, tratamentos médicos e psicológicos e perda de emprego.
> Art. 4º O pagamento da indenização prevista no artigo anterior não exclui o direito da vítima de pleitear a reparação civil por outras perdas e danos materiais e morais.
> Art. 5º Se o crime foi cometido por meio da Internet, na sentença penal condenatória, o juiz deverá aplicar também pena impeditiva de acesso às redes sociais ou de serviços de e-mails e mensagens eletrônicas pelo prazo de até dois anos, de acordo com a gravidade da conduta.
> Art. 6º Esta Lei entra em vigor na data de sua publicação.

3.3 Computação Forense

A sociedade mudou forma de se comunicar, evoluiu, então o direito também mudou, passando a levar em consideração provas eletrônicas. Da necessidade de descobrir soluções de casos específicos dos meios digitais surgiu a computação forense, com técnicas de recuperação de dados, a mesma é de suma relevância para o descobrimento e resolução de crimes digitais como pornografia infantil entre outros.

Para entender o que é computação forense e perícia digital, necessário faz- se apresentar algumas definições do termo. Para Alves (2011, p.23), "a Computação Forense é uma área de estudos da investigação forense que cresce juntamente com o avanço dos crimes cibernéticos. "

Já Pinheiro (2010, p.226), mostra que computação forense é: "o uso de métodos científicos na preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais." Complementando o pensamento o autor supra citado (2010, p.226) informa que, "a ciência forense busca desvendar cinco elementos: Quem? O quê? Quando? Como? Onde? e Por quê?",

Conforme explica Freitas (2006, p.2), "A perícia forense possui quatro procedimentos básicos: todas as evidências devem ser identificadas, preservadas,

analisadas e apresentadas.” Neste contexto pode-se considerar a computação forense como uma ciência aliada a perícia digital.

No pensamento de Pinheiro, entende-se a investigação forense é a busca por qualquer outro dispositivo eletrônico que possa ser apresentado de forma que qualquer pessoa possa entender.

De modo geral, pode-se apreender das definições anteriormente comentadas que a apuração de um crime virtual está relacionada a capacidade do perito para identificar, preservar, analisar e apresentar as evidências colhidas dos dispositivos aprendidos.

Um caso que ficou bastante conhecido na mídia e que a computação forense foi de grande importância para a resolução foi o caso da atriz Carolina Dieckmann que logo depois virou a Lei 12.737/2012 a polícia usou programas de contraespionagem para chegar nos acusados, usada por profissionais que procuram esclarecer casos envolvendo meios digitais.

3.4 ENGENHARIA SOCIAL

Nakamura; Geus (2003), definem Engenharia Social como sendo,

> É a técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. Ela tem como objetivo enganar e ludibriar pessoas assumindo-se uma falsa identidade, a fim de que elas revelem senhas ou outras informações que possam comprometer a segurança da organização (2003 p,70)

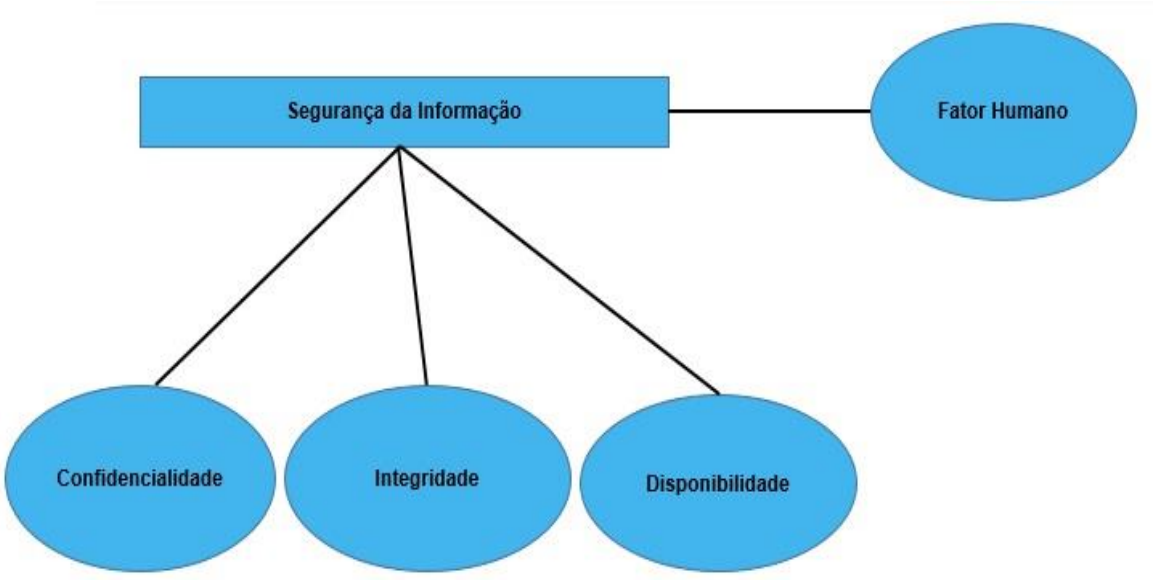
A citação mostra que engenharia social é a prática para obter informações enganando as pessoas ou explorando informações sem que as mesmas deem permissão. Engenheiros sociais usam as pessoas para obter informações, utilizando linguagem natural. Antigamente a engenharia social era praticada por telefonemas, quando os engenheiros se passavam por funcionários, clientes das empresas.

Meios físicos, políticas de segurança, ferramentas sofisticadas e ótimos profissionais da área de segurança não são suficientes para garantir a proteção da

informação quando depara-se com o fator humano. Ele é o grande responsável por vazamento de informação confidencial. Empresas com todos esses aparatos ficam vulneráveis a exposição, pois o fator humano é a parte mais frágil de uma rede de segurança.

Para melhor compreensão da temática, apresenta-se na Figura 2 uma configuração do atual modelo de segurança da informação:

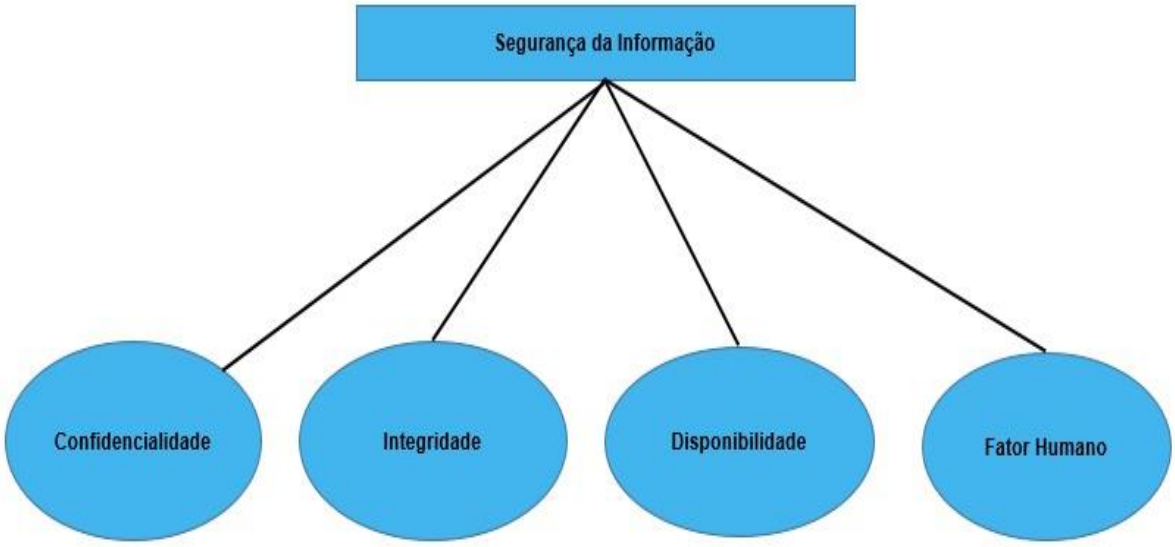
Figura 2 – **Atual modelo da segurança da informação**.



Fonte: (SILVA, M.; COSTA, 2009), adaptada pela autora

Para melhor segurança da informação seria melhor um modelo que agregasse o fator humano como mostra a figura abaixo (Figura 3):

Figura 3 – Proposta de novo modelo para Segurança da Informação



. Fonte: (SILVA, M.; COSTA, 2009), adaptada pela autora

As pessoas não têm ideia de que emprestar uma senha pode causar danos já que se a pessoa a quem a mesma entregou a senha cometer algum crime com a senha quem é culpado é o dono da senha, pois as senhas são identidades digitais. Casos como esse acontecem todos os dias, já que o engenheiro social pode ser alguém em quem se confia e pode passar os dados confidenciais para desconhecidos. Também é uma grande falha do ser humano e isso é muito fácil de ver, pessoas se passando por funcionários ou clientes querendo obter informações enganando funcionários.

A falha humana é a principal causa de vazamento de informações em uma simples conversa ao telefone ou pessoalmente ao falar com alguém. Ao telefone acaba-se por muitas vezes divulgando dados, números de cartão de banco, endereços residenciais, endereços eletrônicos e nos lugares menos improváveis está um engenheiro social ouvindo na conversa tentando obter lucro das informações divulgadas.

O perfil de um engenheiro, normalmente é de uma pessoa, educada, simpática, criativa e carismática, detentor de uma boa conversa. “Geralmente o engenheiro social é um tipo de pessoa agradável. Ou seja, uma pessoa educada, simpática, carismática. Mas, sobretudo criativa, flexível e dinâmica. Possuindo uma conversa bastante envolvente.” (ARAUJO, 2005, p. 27).

3.5 Espionagem

A espionagem frequentemente é feita por pessoas que tem acesso a informações privilegiadas, esse tipo de espionagem acontece por medidas de segurança de uma nação, chefes de estados permitem essa espionagem que no caso leva nome de monitoramento, pessoas com grandes cargos são monitoradas para seu próprio bem. Mas também existe a espionagem feita por empresas para conseguir vantagens em relação a empresas concorrentes conhecida como espionagem industrial ou comercial.

Segundo Daniel Aisenberg (1999, p.68)

> A espionagem industrial é muito mais eficaz quando realizada dentro de casa, por pessoas com acesso às informações certas e armadas de intenções erradas. O vazamento de dados promovido por funcionários merece a atenção de qualquer empresa que decida proteger seu maior capital: a informação.

Existem sistemas desenvolvidos para espionagem, vigilância eletrônica, esses sistemas trabalham com o uso de palavras chaves tais como, presidente, EUA, Casa Branca. O poder público possui formas de vigiar as nossas informações e o estado tem acesso a dados confidenciais como, por exemplo, nome, RG, CPF, endereço de todos os cidadãos.

3.6 Vírus

Os vírus de computador são programas, rotinas, macros, que se auto-duplicam e fazem diversas atividades não solicitadas, ilícitas e talvez tudo ao mesmo tempo.

Os primeiros vírus de computador eram pequenos programas que se juntavam com programas executáveis, ou área de iniciação do sistema operacional e iam se duplicando, normalmente, toda vez que se rodava um programa infectado o mesmo ficava ativo na memória e contaminava todos os programas que chamados, ou área de iniciação de discos, ou os dois. Em uma determinada data eles faziam algo como

formatar seu *winchester* (ou HD) ou fazer cair às letras no monitor, ou mesmo fazer aparecer uma bolinha na tela que pula de um lado para outro.

Atualmente, os vírus são mais complexos e mais fáceis de serem adquiridos, devido à internet e de suas facilidades.

4 OS CUIDADOS NO AMBIENTE VIRTUAL

4.1 Antivírus

Os antivírus são programas de computador utilizados para detectar, prevenir, eliminar os vírus de computadores ou celulares. Sabe-se que existe no mercado variedades de produtos para combater os vírus. AVG, Avast, Avira e Microsoft Security Essentials são alguns dos mais usados e conhecidos. É aconselhável utilizar apenas um antivírus.

Para Dias (2000), o software antivírus foi originalmente desenvolvido para detectar e remover vírus de computadores, daí o surgimento do nome. No entanto, como a proliferação de outros tipos de *malware*, softwares antivírus começam a fornecer proteção contra ameaças de objetos maliciosos.

4.2 Criptografia

Segundo Oliveira (2001, p.19), criptografia significa transformar uma mensagem em outra (“escondendo” a mensagem original) com a elaboração de um algoritmo com funções matemáticas e uma senha especial, chamada chave.

Nesse sentido, pode-se entender pelo termo que criptografia é método que utiliza fórmulas matemáticas para esconder informações ou embaralhá-las tornando-as ilegível para quem não possui a chave que nada mais é que um código de segurança para somente pessoas que tenha permissão a este código ter acesso a informação, pessoas que não possuem essa chave são incapazes de enxergarem esses documentos.

Segundo O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br, com o apoio do Comitê Gestor da Internet no Brasil – CGI.br (2006), define criptografia como “é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet.”

A criptografia pode ser usada para garantir a autenticidade e privacidade dos dados. Com ela as empresas, por exemplo, têm uma maior segurança com e-mails corporativos e dados de clientes evitando assim que invasores se apossem dos dados

da empresa em questão. Muitos sistemas utilizam a criptografia como medida de segurança.

4.3 Firewall

Filho (2002, p. 183) afirma que o firewall é um dispositivo de hardware e software que tem como principal função filtrar pacotes na rede, com o objetivo de proteger, negando informações ou repassando comunicações a respeito do evento.

4.4 Senhas

As senhas são medidas segurança simples, porém eficazes usadas para ter acesso a redes sociais ou a sistemas. Com elas é possível identificar a pessoa, a senha é de um exclusivo da pessoa não é aconselhável dividir senha com outras pessoas e nem usar a mesma senha para diferentes tipos de acesso, o ideal é ter uma senha diferente para cada rede social ou sistema que precise da utilização da mesma.

> Uma senha, ou password, serve para autenticar uma conta, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. É um dos principais mecanismos de autenticação usados na Internet devido, principalmente, a simplicidade que possui. CERT.br, (2012, p.59)

É preciso criar boas senhas para manter uma maior segurança, mistura letras maiúsculas e minúsculas com números e símbolos seria uma dica para criação de uma senha segura, como também ter o cuidado ao compartilhar suas senhas e usa-las em computador de terceiros, encerrar ou fechar a sessão sempre que terminar o acesso também ajuda.

Se uma outra pessoa souber a sua conta de usuário e tiver acesso à sua senha ela poderá usá-las para se passar por você na Internet e realizar ações em seu nome, como mostra a Cartilha de Segurança para Internet 2012 conforme lista-se abaixo:

- acessar a sua conta de correio eletrônico e ler seus e-mails, enviar mensagens de spam e/ou contendo phishing e códigos maliciosos, furtar sua lista de contatos e pedir o reenvio de senhas de outras contas para este endereço de e-mail (e assim conseguir acesso a elas);
- acessar o seu computador e obter informações sensíveis nele armazenadas, como senhas e números de cartões de crédito;
- utilizar o seu computador para esconder a real identidade desta pessoa (o invasor) e, então, desferir ataques contra computadores de terceiros;
- acessar sites e alterar as configurações feitas por você, de forma a tornar publicas informações que deveriam ser privadas;
- acessar a sua rede social e usar a confiança que as pessoas da sua rede de relacionamento depositam em você para obter informações sensíveis ou para o envio de boatos, mensagens de spam e/ou códigos maliciosos. CERT.br, (2012, p.60)

5 METODOLOGIA

5.1 Caracterização De Pesquisa

Trata-se de uma pesquisa bibliográfica que segundo Marconi e Lakatas (2008) refere-se a um levantamento, relação e documentação de bibliográfico acerca de um determinado assunto.

5.2 Fonte De Informação

A fonte de informação foi constituída dos livros e dos artigos de revisão e original relacionada ao tema de investigação no presente estudo. Os artigos foram localizados nas bases de consulta no meio eletrônico da biblioteca digital SCIELO e Google Acadêmico. No tocante aos livros que deram suporte a revisão bibliográfica foram localizados na Biblioteca da Universidade Estadual da Paraíba- UEPB.

Os descritores utilizados para a busca de artigos nas bases de dados incluíram os termos: Ameaça virtual. Crime virtual. Segurança da informação. A busca bibliográfica foi realizada entre Agosto e Dezembro de 2014.

5.3 Instrumentos Para Coleta De Dados

Os instrumentos utilizados para coleta das informações foram um formulário para efetuar os fichamentos necessários das informações, os próprios artigos e livros na busca bibliográfica.

5.4 Procedimentos para coleta dos dados

Em um primeiro levantamento foi definido o tema para o desenvolvimento dessa pesquisa, na sequência foi determinada a forma de busca das informações que utilizou uma pesquisa em bases de dados na internet e o levantamento de informações em livros. Por fim, foram realizados os fichamentos e a construção da revisão bibliográfica com base nos objetivos propostos para essa pesquisa que envolveu o tema Segurança da Informação: os cuidados no ambiente virtual.

5.5 Análise Das Informações

As informações foram analisadas qualitativamente com objetividade e imparcialidade, procurando absorver as intenções dos autores, sem julga-las identificando as ideias chaves através de grifos e anotações em cada parágrafo, e em seguida organizando de acordo com a sua importância. Após a organização dos dados, estes foram descritos para melhor compreensão das referências.

6 RESULTADOS E DISCUSSÃO DO TRABALHO

6.1 Ameaças, Crimes, Perigos

Os estudos de caso mostrados nesse trabalho tomam como fonte os principais fatos que envolvem os crimes na Internet no Brasil.

6.1.1 Caso 1 – Carolina Dieckmann

Este estudo abordará o caso Carolina Dieckmann

6.1.1.1 Situação

Hackers invadiram a caixa de e-mail da atriz por meio de um (Spam) um falso e-mail, a vítima infelizmente abriu esse e-mail e preencheu um formulário com seus dados incluindo a senha de acesso do seu endereço eletrônico (e-mail), com isso dando acesso os criminosos, eles copiaram e furtaram ao todo 60 arquivos entre eles fotos pessoais intimas, as imagens foram furtadas de seu e-mail.

Para não divulgar as fotos eles chantagearam a atriz por dinheiro onde pediam R$ 10 mil reais, após uma tentativa frustrada de chantagearem a vítima, os criminosos compartilharam as fotos intimas em sites pornográficos.

6.1.1.2 Solução

E-mails infectados chegam todos os dias na nossa caixa de entrada, leigos no assunto relacionado à segurança da informação se prejudicam nesse aspecto. A sugestão, com base na pesquisa monográfica, é:

- Não abrir e-mail de fonte desconhecidas evitando assim ser vítima de algum criminoso;

- Configurar adequadamente seu provedor de e-mail e seu navegador de internet para manter uma maior segurança e privacidade;
- Não solicitar permissão a programas não confiáveis para não servir como porta de entrada a seu sistema;
- Manter sempre um antivírus de boa qualidade atualizado no seu computador caso ocorra alguma invasão;
- Se possível utilizar um sistema operacional Linux a exemplo do Ubuntu, que possibilita uma maior segurança para o usuário.

6.1.2 Caso 2 – Funcionária Pública Estadual (Professor)

Este estudo abordará o caso de uma Funcionária Pública (Professor) do interior da Paraíba. Fonte: A pessoa lesada (Amália Machado dos Santos); Secretaria de Administração do Estado da Paraíba e Secretaria de Educação do Estado da Paraíba.

6.1.2.1 Situação

O criminoso através do uso de telefone conseguiu os dados cadastrais da funcionária junto à Secretaria Estadual de Administração onde se encontra armazenado no computador. A chefe de departamento cometeu um crime de confiabilidade, ou seja, repassou informações alheias sem autorização prévia.

O criminoso usando de má fé fez um empréstimo no valor elevado, no banco Pan Americano. O repasse do empréstimo foi para a conta do agiota (criminoso), e os descontos mensais foram atribuídos no contracheque da professora, ou seja, os descontos (débitos) quem arcou foi a funcionária.

6.1.2.2 Solução

Infelizmente por falta de leis que inibam esse tipo de crime, a cada dia sucessivos casos acontecem e está se intensificando. Necessário e urgente se faz a criação e promulgação de leis severas que inibam ou mesmo exterminem esses casos.

Casos como esse acontecem todos os dias em todo o mundo, quando criminosos aproveitam-se da inocência das pessoas ou de funcionários não qualificados. Os criminosos hoje em dia estão cada vez mais sofisticados nos seus golpes, não utilizam somente programas, softwares, fazem uso de outros métodos, aproveitam-se da boa oratória para tentar roubar informações e aplicar golpes.

Para tentar diminuir casos iguais a esse, sugere-se:

- Não divulgar seus dados pessoais na internet, a não ser em casos de utilização em meios seguros e de extrema necessidade para o usuário;
- Treinar adequadamente funcionários de empresas e instituições, alertando assim para possíveis casos do tipo adequando os funcionários aos novos golpes;
- É de responsabilidade também das instituições ou empresas elaborar a política de segurança englobando o quesito Engenharia Social;
- O funcionário deveria pedir códigos de segurança que só o detentor dos dados teria acesso.

CONSIDERAÇÕES FINAIS

O presente estudo teve como objetivo geral realizar um levantamento bibliográfico sobre os perigos no ambiente virtual e os cuidados que garantam a segurança da informação.

Durante o desenvolvimento desta produção acadêmica foi possível observar que os crimes cometidos através do uso de computadores deixaram de ser um mero sinal de ameaça para se tornarem corriqueiros, e mais comuns na vida dos indivíduos.

Evidenciou-se que atualmente, a tendência de que todos os serviços prestados, tanto pelas empresas privadas como órgãos públicos sejam incorporados na internet é indiscutivelmente uma evolução e democratização para todos, mas requer um alerta para que estes mesmos serviços não sejam alvos de criminosos e se forem, sejam rapidamente identificados e punidos.

Percebeu-se que inúmeras são as perdas provocadas por crimes virtuais porém, pode-se prever que podem provocar desfalques enormes e imensuráveis em todos os ramos da sociedade se nada for feito ou regulamentado para prevenir e/ou contê-los.

Constatou-se que o computador, há tempos, deixou de ser um instrumento de apenas diversão para se tornar um instrumento de trabalho, portanto deve-se tomar os devidos cuidados com os instrumentos do meio virtual especificamente, a internet, a qual possui o intuito de democratizar a informação, a cultura e o conhecimento em geral. Dessa maneira, é preciso acabar com a impunidade e desordem dos crimes e ameaças dos computadores através da internet, assim procedendo a transformação em um local seguro e confiável para que todos possam utiliza-los e manter-se bem informados e capacitados em uma área de trabalho.

Espera-se que pessoas comuns ou até mesmo empresas possam utilizar esse estudo como fonte de estratégia de segurança na modelagem ou organização dos recursos humanos.

Sugere-se ainda que as informações contidas nesta pesquisa sejam aplicadas na busca de resultados mais eficazes baseados na segurança da informação eficiente e com inovação tecnológica, além de dicas seguras para que as pessoas que

convivem no mundo virtual, vivam de forma saudável, os recursos e benefícios da ideologia da informação.

REFERÊNCIA

_____. Ministério da Ciência e da Tecnologia**. Livro Verde da Sociedade da Informação no Brasil**. Brasília: Ministério da Ciência e Tecnologia, 2000.

_____. CERT.Br, **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**, 2012. Disponível em: <http://cartilha.cert.br/>. Acesso em 10 de junho de 2014.

AISENBERG, Daniel. **O feitiço contra o feiticeiro**. In: Internet Business. Rio de Janeiro, v.2, n. 18, 0, p. 68-71, fev.1999.

ALVES, Levi Pereira. **Um Estudo sobre a Perícia Forense Computacional no âmbito do Exército Brasileiro**. Monografia (especialização) – Universidade de Brasília. Instituto de Ciências Exatas. Departamento de Ciência da Computação. Brasília, 2011.

ARAUJO, Eduardo E. de. **A Vulnerabilidade Humana Na Segurança Da Informação**. 2005. 85 f. Monografia (Graduação)– Faculdade de Ciências Aplicadas de Minas, União Educacional Minas Gerais S/C LTDA, Uberlândia, 2005. Disponível em: . Acesso em: 11 jul. 2014.

BRASILIANO, Antonio Celso Ríbeiro. **A Era da Informação Estratégica, A Inteligência Competitiva e a Segurança Empresarial** Disponível em:http://www.viaseg.com.br/artigos/erainf.htm: Acesso em: 11 out. 2014.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde : segurança cibernética no Brasil** / Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010.

BRASIL. Decreto nº 3.505 de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. **Diário Oficial da República Federativa do Brasil,** Brasília, nº 114, pag. 2, 14 jun. 2000.

BRASIL. Lei nº 12.737,30 De Novembro De 2012.

Cartilha de Segurança para Internet. **Comitê Gestor da Internet no Brasil**, São Paulo, 2006. Disponível em <http://cartilha.cert.br>. Acesso em: 01 nov. 2014.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da Internet**. São Paulo: Saraiva, 2000.

DIAS, Claudio. **Segurança e Auditoria de tecnologia da Informação**. 2000, Editora: Axcel Books, ISBN85-7323-231-9.

FREITAS, Andrey Rodrigues de. **Perícia Forense Aplicada à Informática: Ambiente Microsoft.** Rio de Janeiro. Editora Brasport, 2006.

FERREIRA, Aurélio Buarque de Holanda. **Dicionário Aurélio ilustrado**. CURITIBA: Positivo, 2010. 560p.

FILHO, André Stato. **Domínio Linux: Do Básico a Servidores**. Florianópolis – SC: Visual Books, 2002.

GUIMAROES, A. **Segurança em redes virtuais** – VPNS. São Paulo: Editora Brasport, 2000.

INELLAS Gabriel César Zacarias De. **Crimes na Internet**. 2. ed. São Paulo: Juarez de Oliveira, 2009.

Informações sigilosas são vendidas em CDs na Santa Efigencia em SP. Portal de noticias da Globo. Abr. 2007. São Paulo. Disponível em <http://g1.globo.com/Noticias/SaoPaulo/0,,MUL26277-5605,00%20INFORMACOES+SIGILOSAS+SAO+VENDIDAS+EM+CDS+NA+SANTA+EFIGENIA+EM+SP.html>Acesso em: 12 mar. 2015.

LAKATOS, E. M.; MARCONI, M. A. **Técnicas de pesquisa**: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados. 7. ed. São Paulo: Atlas, 2008.

Lei Carolina Dieckmann. Disponível em <https://pt.wikipedia.org/wiki/Lei_Carolina_Dieckmann> Acesso em: 17 mar. 2014.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar: ataques de harckers: controlando o fator humano na segurança da informação.** São Paulo: Person Education, 2003.

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio; **Segurança de Redes em ambientes Cooperativos**; Editora Futura; 2003.

OLIVEIRA, Wilson – **Segurança da Informação: Técnicas e Soluções**. Porto: Centro Atlântico Editora,2001.

PEIXOTO, Mário César Pintaudi. **Engenharia Social & Segurança da Informação na Gestão Corporativa**. 1ª ed. Rio de Janeiro: Brasport, 2006.

PINHEIRO, Patrícia Peck. **Direito digital.** São Paulo: Saraiva, 2010.

PAIVA, Luciano Carneiro de Paiva. **A prova nos crimes de informática.** Aspectos Técnicos e Jurídico. Dissertação, 2006.

SILVA, Maicon H. L. F. da; COSTA, V. A. de S. F. **O fator humano como pilar da Segurança da Informação**: uma proposta alternativa. Serra Talhada (PE), 2009.

SILVA, Antônio Everardo Nunes da. **Segurança da Informação – Vazamento de informações – As empresas estão realmente seguras em sua empresa?** Rio Janeiro: Editora Ciência Moderna Ltda., 2012.

Snowden divulga novos documentos sobre espiões dos EUA e britânicos. Portal de noticias da Globo. Mar. 2015. São Paulo. Disponível em <http://g1.globo.com/bom-dia-brasil/noticia/2015/02/snowden-divulga-novos-documentos-sobre-espioes-dos-eua-e-britanicos.html> Acesso em: 23 Mar. 2015.