UNIVERSIDADE FEDERAL FLUMINENSE

ANDERSON LOPES ARGOLLO

SEGURANÇA DA INFORMAÇÃO: O SER HUMANO COMO O ELO MAIS FRACO DA CORRENTE

Niterói

2017

ANDERSON LOPES ARGOLLO

SEGURANÇA DA INFORMAÇÃO: O SER HUMANO COMO O ELO MAIS FRACO DA CORRENTE

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Orientador:
Vinícius Corrêa Ferreira

NITERÓI
2017

Ficha catalográfica automática - SDC/BEE
Gerada com informações fornecidas pelo autor

A693s Argollo, Anderson Lopes
Segurança da informação: : o ser humano como o elo mais fraco da corrente / Anderson Lopes Argollo ; Vinicius Corrêa Ferreira, orientador. Niterói, 2017.
44 f.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação)-Universidade Federal Fluminense, Instituto de Computação, Niterói, 2017.

1. Segurança da informação. 2. Produção intelectual.I. Ferreira, Vinicius Corrêa, orientador. II. Universidade Federal Fluminense. Instituto de Computação. III. Título.

CDD -

Bibliotecária responsável: Fabiana Menezes Santos da Silva - CRB7/5274

ANDERSON LOPES ARGOLLO

SEGURANÇA DA INFORMAÇÃO: O SER HUMANO COMO O ELO MAIS FRACO DA CORRENTE

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Niterói,____de_____de 2017.

Banca Examinadora:

_____

Prof. Vinicius Corrêa Ferreira, M.Sc. – Orientador

UFF – Universidade Federal Fluminense

_____

Prof. Jean de Oliveira Zahn, M.Sc. – Avaliador

UFF – Universidade Federal Fluminense

AGRADECIMENTOS

Aos colegas de curso Raul e Humberto que foram fundamentais na conclusão do curso.

RESUMO

O uso cada vez maior de sistemas de informação integrados através das redes é um fato significativo, uma vez que alteraram a rotina das organizações que passaram a realizar as suas mais variadas atividades em sistemas informatizados. Sendo assim, uma enorme quantidade de informações que trafegam diariamente pela rede está sujeita a várias ameaças que colocam em xeque a segurança da tríade organização, sistema e informação. Infelizmente, a tecnologia da informação não é capaz de apresentar uma solução integral do problema uma vez que falhas são inerentes aos humanos. Sendo assim foram criadas as políticas de segurança da informação que devem buscar um equilíbrio apropriado dos aspectos humanos e técnicos da segurança da informação, diferentemente da maioria dos modelos de políticas usados hoje em dia, que não consideram o fator humano como fundamental no que se refere a segurança da informação. O presente trabalho visa mostrar conceitos importantes na área de segurança da informação, as principais ameaças as quais os colaboradores estão suscetíveis além de ferramentas que auxiliarão os colaboradores quando estes forem alvo de ataques.

Palavras-chaves: segurança da informação, fator humano, organizações.

LISTA DE TABELAS

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ACK – *Acknowledgement*

DdoS - *Distributed Denial of Service*

DoS – *Denial of Service*

IP – *Internet Protocol*

PSI – *Política de Segurança da Informação*

SYN - *Synchronize*

TCP – *Transmission Control Protocol*

UDP - *User Datagram Protocol*

VoiP– V*oice over Internet Protocol*

VPN – *Virtual Private Network*

SUMÁRIO

1 INTRODUÇÃO

A Segurança da Informação é um dos assuntos mais debatidos ultimamente, pois, nos dias de hoje, a informação tornou-se um bem intangível de grande valor para as organizações. O sociólogo estadunidense Daniel Bell afirmou, em 1956, que a Era da Informação tem seu marco primordial quando o número de executivos ultrapassou o de operários no seu país. Ao perceber isso ele advertiu: “Que poder operário que nada! A sociedade caminha em direção à predominância do setor de serviços.” Ou seja, o poder direcionava-se àqueles que possuíam algum tipo de conhecimento que interessava a outros[1].

Atualmente, a informação é uma ferramenta fundamental quando as organizações precisam tomar alguma decisão estratégica. Elas coletam o máximo de informação possível sobre o assunto que, muitas vezes, trata-se do crescimento da organização para poder traçar uma estratégia para alcançar um objetivo alvo.

É natural que as organizações queiram proteger as informações devido a tamanha importância que elas têm para a sobrevivência da empresa num mercado extremamente competitivo. Infelizmente, são gastos milhões em aparatos tecnológicos o que não garante por si só a segurança da informação, não levando em conta o fator humano que também deve ser considerado na política de segurança.

A todo instante os negócios, os processos e ativos físicos, tecnológicos e humanos são alvos de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada [2].

No final de 2003 a Módulo Security Solutions S.A., a principal empresa de segurança tecnológica da informação no Brasil, apresentou os resultados de sua Nona Pesquisa Nacional de Segurança da Informação. Foram respondidos 682 questionários entre os meses de março e agosto de 2003, junto a profissionais de segurança de variados segmentos.

Dentre os resultados, pode-se ressaltar os seguintes [3]:

1. 42% das empresas tiveram incidentes de segurança da informação nos seis meses anteriores à pesquisa;

2. 35% das empresas reconheceram perdas financeiras devido a tais incidentes;

3. o percentual de empresas que informa ter sofrido ataques subiu de 43% em 2002 para 77% em 2003;

4. 32% dos respondentes apontaram hackers como responsáveis pelos incidentes reportados;

5. para 78% dos respondentes os riscos e os ataques aumentariam em 2004;

6. 48% não possuíam plano de ação formalizado para o caso de invasões e ataques;

7. 60% indicam a internet como o principal ponto de invasão de seus sistemas;

8. a falta de consciência dos executivos é apontada por 23% dos respondentes como o principal obstáculo para a implementação de segurança, enquanto 18% alegaram ser a dificuldade em justificar o retorno do investimento, 16% o custo de implementação e apenas 6% apontaram a falta de orçamento.

O item 8 da pesquisa citada acima mostra que o aspecto humano constitui um entrave na questão da segurança da informação. O presente trabalho visa discutir sobre tal problema além de fornecer soluções que busquem trazer um equilíbrio apropriado do aspecto humano e técnico da segurança da informação.

Este trabalho está estruturado da seguinte forma:

- no Capítulo 1 traremos a contextualização, objetivos e estrutura do trabalho.
- No Capítulo 2 serão apresentados a definição de informação, diferença entre informação e dado além, comentaremos também sobre o valor da informação e sobre sistemas de informação.
- No Capítulo 3 serão apresentados um breve histórico sobre a segurança da informação, definição e situações que podem comprometer a segurança.

- No Capítulo 4 falaremos o quem vem a ser uma Política de Segurança da Informação, seu conteúdo, suas características, sua origem e como deve ser implantada.
- No Capítulo 5 falaremos dos aspectos tecnológicos presentes nas políticas de informação que são fundamentais na segurança.
- No Capítulo 6 falaremos como o aspecto humano pode influenciar diretamente a questão da segurança. Treinamento e conscientização também serão debatidos neste capítulo
- No Capítulo 7 encerrarei com uma conclusão fazendo um resumo de tudo que foi visto no trabalho.

2 A INFORMAÇÃO

Tempos atrás, uma organização tinha como principais rivais, as outras empresas da mesma região ou estados vizinhos. Atualmente a concorrência é global, e a informação é o recurso que as empresas possuem para realizar as principais tomadas de decisão. Sendo assim, o acesso à informação, bem como seu tratamento e análise, podem influenciar o sucesso ou o fracasso da grande parte das empresas.

No âmbito corporativo, a informação correta, num espaço de tempo adequado e no local certo se transforma numa importante ferramenta para tomada de decisões mais precisas e certeiras, gerando assim, vantagem competitiva para quem a detêm [4].

A informação tornou-se um elemento fundamental para a existência das organizações, funciona como elemento de ligação entre diversos pontos (inclusive os mais extremos). Organizações alimentam-se de informações, e ao mesmo tempo são direcionadas por elas. A cada momento, informações são processadas pelos colaboradores de uma organização; as informações procedem de fontes internas (podemos citar o Departamento de Pesquisas e Desenvolvimento) e externas (podemos citar os consumidores, parceiros de negócio, pesquisas de outras empresas) [5].

2.1 DEFINIÇÃO

Primeiramente traremos as acepções mais genéricas do termo informação. Informação é o ato ou efeito de informar-se, ou seja, o ato de tomar conhecimento, e inteirar-se ou instruir-se sobre algo[6]. Uma outra definição a expressão pode ser en-

tendida como comunicação ou recepção de um conhecimento ou juízo [7]. Uma definição mais completa temos que informação nada mais é que um conjunto de dados com um significado, ou seja, que reduz a incerteza ou que aumenta o conhecimento a respeito de algo[8]. Na definição anterior são citados outras duas importantes expressões que muitas vezes confundem-se com o termo informação, no caso são: dado e conhecimento.

Dado pode ser definido como um elemento numérico, conhecido ou obtido por método de coleta apropriado, que serve de base para um processo de análise. Neste contexto, a palavra dados foi reservada para a representação de fatos, conceitos ou instruções através de sinais, de uma maneira formalizada, passível de ser transmitida ou processada pelos seres humanos ou por meios automáticos [9].

Depois de vista a definição de dados, veremos agora uma possível definição de conhecimento. O conhecimento é o ato ou efeito de apreender intelectualmente, de perceber um fato ou uma verdade: cognição, percepção [7]. As informações são valiosas na compreensão dos sistemas, mas o conhecimento constitui um estágio superior. O conhecimento é capaz de contribuir na produção de novas idéias, por outro lado a informação por si só não é suficiente para ampliar o saber o humano. Portanto o conhecimento exige a capacidade de identificar o que é importante e assim gerar o saber. Se informação é dado trabalhado, então conhecimento e informação trabalhada.[10]

Na Tabela 1 temos uma tabela comparativa entre os termos definidos nos parágrafos anteriores.

Tabela 1: Conceito de dados, informação e conhecimento [11]

Dados, Informação e Conhecimento		
Dados	**Informação**	**Conhecimento**
Simples observações sobre o estado do mundo	Dados dotados de relevância e propósito	Informação valiosa da mente humana. Inclui reflexão, síntese, contexto.
• Facilmente estruturado • Facilmente obtido por máquinas • Frequentemente quantificado • Facilmente transferível	• Requer unidade de análise • Exige consenso em relação ao significado • Exige necessariamente a mediação humana	• De difícil estruturação • De difícil captura em máquinas • Frequentemente tácito • De difícil transferência

Podemos perceber através da Tabela 1 que dados, informação e conhecimento se complementam e se relacionam estreitamente. Pode-se concluir que dos dados derivam-se as informações. E estas por sua vez, após interpretadas, tomadas como verdadeiras e guardada na memória tornam-se conhecimento, isto é, uma informação memorizada, que pode ter alguma utilidade no futuro.

2.2 VALOR DA INFORMAÇÃO

O valor atribuído a informação é proporcional ao impacto que ela pode provocar a empresa. Em outras palavras, se uma decisão for tomada através dela e trouxer alguma vantagem competitiva para organização, então esta informação terá grande valor para a empresa.

O conceito de valor da informação está relacionado com [12]:

- A redução da incerteza no processo de tomada de decisão.
- A relação do benefício gerado pela informação versus custo de produzi-la.
- Aumento da qualidade da decisão.

No processo decisório, o volume de informações e dados colocados à disposição de quem toma a decisão deve ser na medida certa. Se esse volume for excessivo, os dados e informações pertinentes à solução do problema serão mascarados por aqueles considerados espúrios. Para resolver esse problema, é necessário escalonar a informação em uma hierarquia capaz de diferenciar as necessidades nas diversas situações, o que reforça a importância de reconhecer que a informação possui valor [13].

O valor da informação pode variar de acordo com o tempo e sua perspectiva sendo classificada nos seguintes tipos [14]:

- valor de uso: baseia-se na utilização final que se fará com a informação; valor de troca: é aquele que o usuário está preparado para pagar e variará de acordo com as leis de oferta e demanda, podendo também ser denominado de valor de mercado;
- valor de propriedade, que reflete o custo substitutivo de um bem;

- valor de restrição, que surge no caso de informação secreta ou de interesse comercial, quando o uso fica restrito apenas a algumas pessoas.

Da mesma forma, a informação terá valor econômico para uma organização, se ela gerar lucros ou alavanca a vantagem competitiva. De modo geral, a percepção de valor pode ser influenciada pelos seguintes fatores [15]:

- identificação de custos;
- entendimento da cadeia de uso; incerteza associada ao retorno dos investimentos em informação; dificuldade de se estabelecerem relações causais entre os insumos de informação e produtos específicos;
- tradição de se tratar a informação como uma despesa geral; diferentes expectativas e percepções dos usuários;
- fracasso em reconhecer o potencial comercial e o significado da informação.

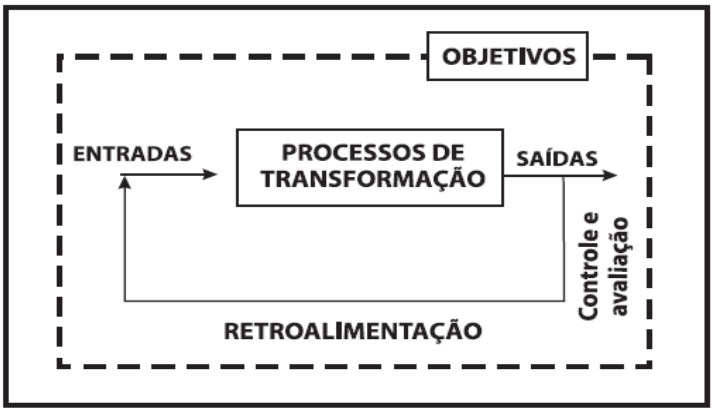
Concluindo este assunto, é importante reconhecer que, de modo geral, raramente toma-se uma decisão com uma informação perfeita, pois é muito difícil encontrar o equilíbrio entre o excesso e a insuficiência de informação. O valor da informação está relacionado com o efeito que ela possui sobre o futuro da organização. Sendo assim decisões tomadas no nível estratégico por conta de alguma informação tendem a impactar mais o futuro da empresa em relação a alguma decisão tomada a partir de uma outra informação no nível operacional da empresa. Consequentemente as informações que influenciam a atuação estratégica da empresa possuem um maior valor agregado [15].

2.3 SISTEMAS DE INFORMAÇÃO

Antes de definirmos sistemas de informação é necessário definir sistema. Sendo assim, sistema pode ser definido como um conjunto de elementos interdependentes, ou um todo organizado, ou partes que interagem formando um todo unitário e complexo [16].

Qualquer sistema é composto por entradas, mecanismos de processamento, saídas e a realimentação, conforme ilustrado na Figura 1.

Figura 1: Atividades de um sistema [17]



Depois de definição vista acima podemos definir sistemas de informações como um conjunto de componentes inter-relacionados, desenvolvidos para coletar, processar, armazenar e distribuir informação para facilitar a coordenação, o controle, a análise, a visualização e o processo decisório [18]. Em outras palavras, é uma combinação estruturada de informação, recursos humanos, tecnologias de informação e práticas de trabalho, organizado de forma a permitir o melhor atendimento dos objetivos da organização [19].

A finalidade dos sistemas de informações fornecer informações para a tomada de decisões, a partir da coleta de dados que serão processados e transformados em informação. Estes sistemas permitem aos gestores obter de forma dinâmica e prática as informações necessárias para embasar as decisões que norteiam as em-

presas, seja em questões administrativas internas, em estratégias de vendas ou outras áreas que necessitem de uma gestão mais apurada de indicadores [20]. Para a eficácia de uma organização está relacionada aos resultados obtidos em ralação ao resultados pretendidos [21]. Neste cenário entende que o sistema de informação atua como solução organizacional e administrativa baseada em tecnologia da informação, enfrentado os desafios apresentados pelo ambiente no qual a organização está inserida [22].

Quanto às atividades de um sistema anteriormente mencionadas (entrada, processamento, saída e realimentação) podemos assim associá-las ao sistema da informação [23]:

- entrada – em sistemas de informação a entrada é a atividade de captar e juntar dados primários. Ao se produzir cheques de pagamento por um sistema informatizado, por exemplo, as hora trabalhadas de cada empregado devem ser informadas antes que o cheque seja efetivamente calculado e emitido. Independentemente do sistema envolvido, o tipo de entrada é determinado pela saída desejada do sistema;
- processamento – envolve a conversão ou transformação dos dados nas saídas úteis e desejadas pelo usuário. Um exemplo tradicional é o cálculo de folha de pagamento. Nele as horas trabalhadas de cada empregado junto com o valor da hora de trabalho devem ser multiplicadas e calculados o pagamento líquido, as horas-extras e os descontos, segundo as regras;
- saída – envolve a etapa na qual a informação propriamente dita é emitida. É a etapa que realmente interessa ao usuário do sistema. Se uma saída gerada por um sistema não for útil para algum propósito, então deve-se fazer uma crítica ao sistema para avalizar sua real necessidade. Por mais simples que isso possa parecer, há muitos sistemas que geram saídas desnecessárias;
- realimentação – a realimentação é uma saída usada para fazer ajustes ou modificações nas atividades de entrada ou no processamento. Erros de digitação, por exemplo, podem fazer com que dados de en-

> trada tenham que ser corrigidos antes de seu processamento. A realimentação também ocorre quando o sistema gera saídas que demandam uma tomada de decisão que provocará uma nova entrada no sistema. Um sistema que indique que os níveis de estoque de uma empresa estão baixos poderá provocar uma decisão de aquisição, que por sua vez gerará a atualização dos produtos em estoque, ou seja, uma nova entrada no sistema.

A maioria das pessoas acreditam que para que se tenha um sistema de informação é necessário um computador, o que não é verdade. Uma simples agenda contendo os contatos de um cliente pode ser considerada um sistema de informação. Ao ordenar seus contatos por ordem alfabética, por exemplo, o indivíduo estará fazendo seu processamento, para facilitar um a busca futura da informação. Contudo, a utilização de computadores potencializou a realização de inúmeras tarefas de manipulação da informação, que seriam inviáveis se realizadas manualmente.

Como as organizações lidam diariamente com um número gigantesco informações se torna imprescindível a utilização de sistemas de informação, seja para tomada de decisões estratégicas, seja para analisar os hábitos de consumo de seus clientes por exemplo. Com cada vez mais rotinas informatizadas, as organizações veem na segurança da informação uma forma de mitigar os riscos causados por fraudes ou ataques causados por invasores.

3 SEGURANÇA DA INFORMAÇÃO

Neste capítulo serão apresentados a definição, contexto histórico da segurança da informação e, posteriormente serão abordados os conceitos e atributos a respeito da segurança da informação além de alguns tipos de ataques que comprometem a segurança da informação de qualquer organização.

3.1 DEFINIÇÃO DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação é a área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Os ativos são recursos, pessoas, bens e serviços, que a empresa possui e que geram receita [24].

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio [25].

A mudança e o crescimento da tecnologia da informação tomam conta dos ambientes corporativos quebram paradigmas e acesso local à informação, e chegam a qualquer lugar do mundo através da rede mundial de computadores: a internet [24].

Os três princípios fundamentais da segurança da informação são [26]:

- Confidencialidade (sigilo): É a garantia de que a informação não será conhecida por quem não deve. O acesso às informações deve ser limitado, ou seja, somente as pessoas explicitamente autorizadas podem acessá-las. Perda de confidencialidade significa perda de segredo. Se uma informação for confidencial, ela será secreta e deverá

ser guardada com segurança, e não divulgada para pessoas não autorizadas.

- Integridade: Esse princípio destaca que a informação deve ser mantida na condição em que foi liberada pelo seu proprietário, garantindo a sua proteção contra mudanças intencionais, indevidas ou acidentais. Em outras palavras, é a garantia de que a informação que foi armazenada é a que será recuperada.
- Disponibilidade: É a garantia de que a informação deve estar disponível, sempre que seus usuários (pessoas e empresas autorizadas) necessitarem, não importando o motivo. Em outras palavras, é a garantia que a informação sempre poderá ser acessada.

3.2 BREVE HISTÓRICO DA SEGURANÇA DA INFORMAÇÃO

Sabe-se que a criptografia já existe há bastante tempo, ela nasceu com o Hebreus por volta de 600 anos antes de Cristo. Posteriormente, em 800 anos depois de Cristo, nasceu a criptoanálise, cujo objetivo era decifrar códigos baseados na criptografia hebraica. Séculos após, no início da I Guerra Mundial, por volta de 1914, Alexander´s Weekly criou métodos que permitiu aos britânicos para quebrarem os códigos criptografados pelos alemães [27].

Não podemos deixar de falar de um importante artefato na história da segurança da informação, a máquina Enigma, desenvolvida e patenteada por Arthur Scherbius, em 1918. Naquela época, o seu potencial ainda não era conhecido. Em 1926, a Alemanha fez algumas adaptações da máquina para o uso militar, dando-a o nome de Funkschlussel C. Já em 1928, os alemães a aperfeiçoaram, batizando-a de Enigma G, ou “A máquina M”, sua função era codificar e decodificar mensagens. A vantagem ao usá-la era que se algum soldado fosse capturado com a mensagem ou o exército inimigo interceptasse o seu sinal, ela de nada serviria, já que o inimigo não tinha como decifrar a informação. Todavia alguns gênios da matemática, como Newman e Turing, quebraram o código criado pelo Enigma. Alguns alegam que a Segunda Grande

Guerra terminou antes devido a este fato. Depois de visto o breve histórico sobre segurança da informação a seguir vamos ver sua definição e conceitos [27].

3.3 AMEAÇAS

A ameaça pode ser considerada um agente externo ao ativo de informação, pois se aproveita de suas vulnerabilidades para quebrar a os princípios básicos da informação – a confidencialidade, integridade ou disponibilidade [28].

As ameaças podem ser classificadas como [29]:

- naturais: são aquelas que se originam de fenômenos da natureza;
- involuntárias: são as que resultam de ações desprovidas de intenção para causar algum dano;
- intencionais: são aquelas deliberadas, que objetivam causar danos, tais como hacker.

O conhecimento das ameaças e ataques potenciais podem enfraquecer o ambiente computacional das organizações é fundamental antes de decidir sobre quais serão os investimentos na área de segurança, pois tais ameaças podem comprometer gravemente a segurança do patrimônio tecnológico como um todo.

3.4 ATAQUES

Atualmente as ameaças e os ataques estão cada vez mais poderosos, trazendo prejuízos incalculáveis para as empresas, desde perda de informações sigilosas até grandes perdas financeiras. As ameaças podem ser classificadas como acidentais ou intencionais, podendo ambas serem ativas ou passivas. Ameaças acidentais são as que não estão associadas à intenção premeditada. As ameaças intencio-

nais variam desde a observação de dados com ferramentas simples de monitoramento de redes, a ataques sofisticados baseados no conhecimento do funcionamento do sistema [30]. O ataque define-se por usuários que utilizam recursos computacionais de maneira ilícita. A seguir veremos alguns tipos de ataques:

3.4.1 Ataques DoS

O ataque de negação de serviço é a forma de ataque mais utilizada na internet. Tem como objetivo esgotar os recursos de um host ou uma rede causando indisponibilidade dos serviços.

Os ataques do tipo DoS mais frequente podem ser feitos devido a algumas peculiaridades do protocolo TCP/IP (*Transmission Control Protocol / Internet Protocol*), sendo possível ocorrer em qualquer computador que o utilize. Uma forma de ataque bastante conhecida, por exemplo, é a *SYN Flooding*, onde um computador tenta estabelecer uma conexão com um servidor por meio de um sinal do TCP conhecido por SYN (*Synchronize*). Se o servidor atender ao pedido de conexão, enviará ao computador solicitante um sinal chamado ACK (*Acknowledgement*). O problema é que, em ataques deste tipo, o servidor não consegue responder a todas as solicitações e então passa a recusar novos pedidos.

Outra forma de ataque comum é o *UPD Packet Storm*, onde um computador faz solicitações constantes para que uma máquina remota envie pacotes de respostas ao solicitante. A máquina fica tão sobrecarregada que não consegue executar suas funções.

Menos frequente, outro exemplo de ataque explora falhas de segurança em softwares, especialmente sistemas operacionais (daí a importância de sempre mantê-los atualizados e protegidos com ferramentas de segurança). Neste tipo, um atacante pode rastrear a rede à procura de máquinas vulneráveis e enviar a elas pacotes que, por alguma razão, fazem o sistema interromper sua atividade.

3.4.2 Ataque DDoS

Um ataque de Negação de Serviço Distribuído, traduzido do inglês *Distributed Denial of Service* – DDoS, consiste em fazer um serviço online indisponível por sobrecarregá-lo com tráfego ilegítimo utilizando diversas fontes. Esses ataques objetivam uma ampla variedade de recursos, de DNSs, sites a serviços na web em geral.

O mecanismo desses ataques se dá por diversas máquinas infectadas em diversas partes do mundo. Conhecidos como *botnets*, esses malwares podem chegar por email, sites e mídias sociais. Uma vez infectados, esses dispositivos podem ser controlados remotamente sem conhecimento de seus proprietários sendo usados como armas para lançar um ataque cibernético.

3.4.3 Cavalo de Tróia

É um tipo *software* malicioso que pode invadir um computador como se fosse um programa legítimo. Seu principal objetivo é abrir uma porta de forma que *hackers* possam invadir a máquina invadida.

Seu nome originou-se da Guerra de Troia onde no final da guera ocorre a destruição dessa cidade. Resumindo a historia um enorme cavalo feito de madeira seria um presente para o rei, os troianos levaram o mesmo para o interior das muralhas da cidade. Durante a noite, este revelou-se uma armadilha e os soldados gregos que se ocultaram dentro do falso presente saíram e abriram os portões para que todo o exército invadisse e queimasse a cidade.

Assim como na narrativa, um Trojan se passa por um programa que disfarça alguma funcionalidade útil quando de fato ele esconde um código que pode causar prejuízos aos computadores e seus usuários, como abrir portas e possibilitar invasões ou roubar senhas de usuário. A principal forma de disseminação destes é pela internet, onde são fornecidos como ferramentas com funções úteis para os computadores.

3.4.4 Spoofing

Este ataque visa obter acesso a um sistema se passando por um outro computador da rede. Há várias maneiras de ludibriar o servidor, uma delas é através do IP. Explicando sucintamente, o atacante usa um *software* que altera o cabeçalho dos pacotes IP de tal maneira que aparentam ter origem da máquina que legitimamente teria acesso ao sistema.

3.4.5 Sniffer

È um *software* de computador que controla o tráfego de rede, ele é uma ferramenta que permite ao administrador do sistema para verificar problemas de rede ou pode ser usado com más intenções por quem deseja alguma informação do sistema, como por exemplo nomes de usuários e senhas. Este tipo de ataque explora o fato dos pacotes das aplicações TCP/IP não serem criptografados. Entretanto, para a execução do ataque, é necessário que o sniffer esteja instalado em num ponto de rede, onde circule pacotes de interesse para o invasor.

3.4.6 Vírus

Considera-se vírus qualquer tipo de código malicioso que exclua os dados ou prejudique o funcionamento da máquina infectada. Devido a extensa variedade de vírus, os mesmos são classificados em vários tipos, cada um com suas particularidades de funcionamento, formas de contágio e disseminação. Os principais tipos são:

- Vírus simples: é um software com capacidade de duplicação, corrompendo outros programas instalados na máquina, geralmente com intenção maliciosa. Um vírus depende de um programa hospedeiro seja executado para que posso ativá-lo;

- Worm ou “verme”: diferentemente do vírus simples, o worm pode se executar independentemente, propagar-se pela rede sozinho, seu objetivo é consumir os recursos dos computadores destrutivamente;
- Vírus polimorfo: tipo de vírus que sofre alterações a medida que se multiplica, com o fito de dificultar a sua localização e eliminação;
- Vírus de Macro: utiliza-se da linguagem VBScript dos softwares Microsoft e pode ser executado em qualquer máquina que contenha algum aplicativo da Microsoft.

4 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A política de segurança é uma diretriz que orienta assuntos relacionados à proteção da informação, assumindo um papel de extrema importância em todas as organizações, sendo assim ao desenvolvimento de uma política de segurança da informação é primordial, pois nela são definidas normas, procedimentos e responsabilidades de forma que garanta o controle e a segurança da informação corporativa.

Política de segurança é apenas uma formalização dos anseios da organização [31]. Um mecanismo preventivo de proteção dos dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pelo corpo técnico e gerencial e pelos usuários, internos ou externos [32].

Em um país, temos a legislação que deve ser seguida para que tenhamos um padrão de conduta considerado adequado às necessidades da nação para garantia de seu progresso e harmonia. Não havia como ser diferente em uma empresa. Nesta precisamos definir padrões de conduta para garantir o sucesso do negócio [31].

Comentando o parágrafo anterior, política de segurança é equiparada com a legislação na qual todo cidadão deve respeitar, de forma que a obediência à legislação nos garante que um padrão de comportamento ou conduta está sendo seguido, assim como a política de segurança também deve balizar todas as atividades dos colaboradores dentro da organização, visando garantir a proteção das informações e, consequentemente, o crescimento do negócio. Uma política de segurança atende a vários propósitos [33]:

- Descreve o que está sendo protegido e por quê;
- Define prioridades sobre o que precisa ser protegido em primeiro lugar e com qual custo;
- Permite estabelecer um acordo explícito com várias partes da empresa em relação ao valor da segurança;

- Fornece ao departamento de segurança um motivo válido para dizer “não” quando necessário;
- Proporciona ao departamento de segurança a autoridade necessária para sustentar o “não”;
- Impede que o departamento de segurança tenha um desempenho fútil.

As políticas, normas e procedimentos de segurança da informação devem ser [34]:

1) Simples;
2) Compreensíveis ou seja, escrita de maneira clara e objetiva;
3) Homologadas e assinadas pela Alta Administração;
4) Estruturadas, estabelecendo padrões;
5) Alinhadas com a estratégia da missão da organização;
6) Orientadas aos riscos, ou seja, direcionadas para os riscos da organização;
7) Flexíveis, ou seja, moldáveis aos novos requerimentos de tecnologia;
8) Protetoras dos ativos de informação, priorizando os de maior valor e de maior importância;
9) Positivas e não apenas concentradas em ações proibitivas ou punitivas;
10) Devem conter atribuições de regras e responsabilidades;
11) Devem conter a forma de educar os usuários;
12) Devem ser dinâmica e atualizadas sempre que necessário;
13) Devem ser acessíveis a todos; e
14) Devem ser exequíveis, ou seja, devem descrever regras de comportamentos que possam ser cumpridos seja na área tecnológica ou humana.

4.1 REFERÊNCIA NORMATIVA

A série ISO 27000 estabelece um padrão de certificação de sistemas e gestão pela Internacional Organization for Standardization, neste caso aplica-se à implementação de Sistemas de Gestão de Segurança da Informação, através da estipulação de uma política de controles adequados e da gestão de riscos.

A sua implementação não traz garantias que uma organização não possa ser atacada, mas fornecera ferramentas para que uma política de segurança seja mais poderosa e apropriada à necessidade de segurança da organização, reduzindo os riscos que possam causar prejuízos consideráveis à organização.

4.2 IMPLANTAÇÃO DA POLÍTICA DE SEGURANÇA

Considerando o aumento da informatização nos setores organizacionais é natural que as organizações desenvolvam políticas de segurança de informação e busquem certificação, pois além da proteção as informações, traz um fator diferencial, que é a garantia que as informações de seus clientes estão seguras.

Uma politica bem clara de segurança deve ser implementada na empresa de forma que deixe claro para o funcionário como agir e em geral deve incluir o seguinte [35]:

a) política de senhas: define as regras sobre o uso de senhas nos recursos computacionais, como tamanho mínimo e máximo, regra de formação e periodicidade de troca;

b) política de backup: define as regras sobre a realização de cópias de segurança, como tipo de mídia utilizada, período de retenção e frequência de execução;

c) política de privacidade: define como são tratadas as informações pessoais, sejam elas de clientes, usuários ou funcionários;

d) política de confidencialidade: define como são tratadas as informações institucionais, ou seja, se elas podem ser repassadas a terceiros;

e) política de uso aceitável: também chamada de "Termo de Uso" ou "Termo de Serviço", define as regras de uso dos recursos computacionais, os direitos e as responsabilidades de quem os utiliza e as situações que são consideradas abusivas.

5 ASPECTO TECNOLÓGICO

Neste capítulo iremos abordar algumas ferramentas que juntamente com a política da informação visam reduzir vulnerabilidades no ambiente organizacional. Por si só estas ferramentas por si só não garantem a segurança da informação, deverá haver uma conscientização dos colaboradores a adotarem alguns cuidados especiais que serão detalhados no próximo capítulo.

A segurança física não envolve apenas a garantia dos equipamentos instalados, mas também a prevenção de que nenhum novo ponto de acesso não autorizado seja adicionado à rede [36].

Através dos equipamentos de controles técnicos que são ferramentas de hardware e software, tais como dispositivos biométricos, bloqueios, software antivírus, firewalls etc. é possível restringir o acesso a prédios, sistemas de computador, programas e etc. a fim de evitar seu uso indevido [37]. Não basta apenas o controle somente externos, mas também deve-se criar mecanismos de controles internos à empresa, incluindo criptografia, controle de acesso, privilégio mínimo, acompanhamento, auditoria e relatórios [38].

Abaixo veremos as definições de algumas ferramentas de controle que auxiliam na proteção das informações.

5.1 CRIPTOGRAFIA SIMÉTRICA E ASSIMÉTRICA

A palavra criptografia que vem do grego kriptos que significa escondido e grifos que significa escrita, é uma técnica utilizada para codificar uma informação, tornado-a ininteligível a qualquer um que venha interceptá-la, sendo decifrada apenas a que se destina a mensagem [39].

Exitem dois tipos de criptografia: a simétrica e a assimétrica [40]. A diferença básica entre os dois tipos de criptografia é a quantidade de chaves usada no momento de criptografar e descriptografar.

A criptografia simétrica exige apenas uma chave, sendo utilizada pelo receptor para leitura da informação. Precisa-se haver uma relação de confiança entre o emissor e o receptor para sua utilização. O programador ao desenvolver um sistema deve ocultar o algoritmo de construção da chave de criptografia visto que se este algorítimo for visível tornará o sistema vulnerável a ataques.

A criptografia assimétrica apresenta dois tipos de chaves: chave pública e outra privada. Ambas são distintas, a primeira é usada para codificação da mensagem enquanto a segundo irá decodificar o conteúdo da mensagem. Apenas o proprietário, ou seja, aquele que receberá a mensagem deverá possuir a chave privada. A chave pública, por outro lado pertence a ambos, portanto quem possui apenas a chave pública jamais conseguirá decifrar a mensagem. Assim, na codificação com a chave pública, o proprietário das chaves confirma a confidencialidade da informação e a autenticidade [41].

5.2 CERTIFICADOS DIGITAIS

Sabemos que em toda comunicação temos o emissor e o receptor. Quando se trata de Certificação Digital, aparecerá um terceiro elemento que garantirá a confi-

abilidade da mensagem. Este terceiro elemento é a certificadora que confere a identidade do transmissor. O transmissor da mensagem tem sua identidade conferida pela certificadora.

A assinatura digital não dá privacidade a um documento, ela apenas assegura a integridade e o não-repúdio. Para que haja privacidade é necessário que o documento seja criptografado com a chave pública do destinatário e a ele seja enviado, de forma que somente ele poderá decodificar e ler o conteúdo da mensagem com a chave privada dele [42].

5.3 REDES PRIVADAS VIRTUAIS - VPN

A rede virtual privada permite criar uma ligação ponto a ponto, no interior de uma rede de baixa confiabilidade. Grande parte das VPNs recorrem ao uso de criptografias. Através dela é possível estabelecer uma conexão entre redes distintas ou duas estações de trabalho, tornando-se quando se quer estabelecer comunicação de dados entre dois pontos em sistemas com baixa confiabilidade, aliando o custo mais baixo do acesso à Internet com as vantagens de uma rede mais segura [43].

Além dos pontos fixos, os móveis também são beneficiados por este recurso. Uma conexão segura pode ser estabelecida com uma VPN de qualquer lugar basta para tanto ter apena acesso à internet.

Um dos maiores benefícios proporcionado por uma VPN está no baixo custo com infraestrutura, já que os links dedicados tornam-se desnecessários uma vez que podem ser trocados pela internet [44].

5.4 SMARTCARDS

O smartcard nada mais é do que uma maneira de guardar senha de forma adequada. Os smartcards processam dados e encontram soluções inteligentes e mais seguras, como o bloqueio automático do cartão após alguma atividade suspeita. Para

garantir maior segurança, é armazenada uma representação eletrônica da impressão digital de forma a garantir que o portador do cartão é o proprietário do mesmo. O smartcard pode ainda levar informações de certificação ou assinatura digital [45].

5.5 FIREWALL

O Firewall é uma técnologia de segurança que utiliza-se de hardware ou software que, considerando regras pré-determinadas, determina operações de transmissão ou recepção de dados podem ser realizadas. Como o próprio nome sugere trata-se de uma barreira defesa repelindo tudo o que possa ser nocivo ao sistema. O seu objetivo, em poucas palavras, é bloquear tráfego de dados que possam causar algum tipo de prejuízo ao sistema.

A funcionalidade de restringir o acesso a rede pode ser feito em conjunto com a configuração de outros dispositivos de rede (roteadores, switches, etc) e deve ser feita de acordo com o planejamento da segmentação da rede, potencializando a segurança da rede [46].

Um *firewall* infelizmente não tem capacidade de identificar todo o tipo de ameaça, portanto cada vez tem sido descobertas soluções para a prevenção e detecção de invasões [47].

6 ASPECTO HUMANO

O vazamento de informações é um dos maiores temores das organizações nos dias de hoje. Na maioria dos casos estes vazamentos tem origem em falhas humanas. Todos os colaboradores devem ser responsável pela confidencialidade destas informações, mas infelizmente por ignorância não são aptos que se deparam com alguma situação de risco.

Se defender de técnicas da conhecida Engenharia Social é uma dos maiores desafios da Segurança da Informação, pois através dela o engenheiro social explora falhas inerentes ao humanos sendo assim uma técnica considerada muito poderosa.

6.1 ENGENHARIA SOCIAL

É a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos [48].

Os ataques de Engenharia Social podem ser realizados através de algumas ferramentas, são elas [48]:

- Telefone ou VolP (voz sobre IP) - passar-se por alguém que não é seria um dos típicos ataques de

engenharia social, como na personificação - help-desk;

- Internet (coleta de informações) - como, por exemplo, sites que fornecem id;
- Intranet (acesso remoto) - Por exemplo, por acesso remoto, capturando-se o micro de determinado usuário da rede e se passando por alguém que na verdade não é.
- E-mail (*Fakemail,* e-mails falsos, os famosos phishing scam);
- Pessoalmente (*In Person Social Engineering*) - poder de persuasão, habilidade em saber conversar, tipo de ataque mais raro.
- Chats (bate papo) - Fazer-se passar por alguém que na verdade não é fica muito mais fácil pelos canais de bate-papo.
- Spyware - Software "espião" usado para monitorar de modo o-culto as atividades do computador de um alvo;
- Mergulho no lixo ("Dumpster diving") - Várias coisas que são descartadas para o lixo muitas vezes contêm informações essenciais ao suposto engenheiro social;
- P2P (Peer-to-Peer) - Tecnologia empregada para estabelecer comunicação entre inúmeros computadores, como uma rede, onde cada estação possui capacidades e responsabilidades equivalentes.

Os colaboradores devem ser treinados e educados a fim de se proteger de ataques de Engenharia Social, identificando situações de perigo e se esquivando delas de maneira segura. Para municiar as organizações contra estes ataques devem criadas e divulgadas políticas, normas e procedimentos de segurança da informação através de programas de treinamento e conscientização constantes.

6.2 CRIANDO PROGRAMAS DE TREINAMENTO E CONSCIENTIZAÇÃO

É imprescindível conscientizar as pessoas sobre o valor da informação que elas trabalha no seu dia a dia, independentemente se ela for corporativa ou íntima. Também vale orientar sobre como age um engenheiro social sendo este um dos maiores vilão quando o assunto trata-se de segurança.

A preocupação em apenas em divulgar com panfletos ou encaminhado a política da segurança da informação em página da intranet não diminuirá os riscos de ataques a organização. O objetivo da política é criar uma rotina de segurança que seja aplicada nas atividades dos colaboradores afim de cumprir todos os itens contidos nesta política. Assim, garantido que sejam entendidos os motivo da política, diminuirá drasticamente as chances de alguém cometer algum deslize. Consequentemente diminuirá as chances de sucesso de um engenheiro social.

A vantagem de conscientizar os colaboradores sobre segurança está em adestrar as pessoas gerando mudança de comportamento e costumes facilitando a obediência aos itens da política protegendo os ativos de informações da organização. Criar alguma motivação também ajuda no processo, fazendo o funcionário acreditar que sua desatenção as políticas não prejudicará não só a organização como também todos os outros colaboradores, uma vez que a empresa guarda informações pessoais dos seu empregados.

É necessário envolver e motivar os colaboradores de forma que eles se sintam envolvidos e integrados na política de segurança da informação. A organização pode considerar que o programa de treinamento e conscientização está no sentido do êxito se todos os colaboradores, após participarem do treinamento, estejam motivados e convencidos [49]. Não se pode deixar de lado a conscientização por parte de todos os colaboradores, para ao menos, mitigar as ameaças de engenharia social [50].

Para completar o treinamento nada mais natural conhecer as tática de um engenheiro social além de saber se defender dos seus ataques. Sendo assim é imprescindível que a organização tenha um engenheiro social a seu favor. O papel dele é localizar vulnerabilidades existente na empresa com a finalidade de propor soluções que melhorem a segurança no ponto vulnerável.

Além do função vista no parágrafo anterior, ele pode aplicar algumas atividades para melhorar a segurança da informação [51].

- Seminários de sensibilização;
- Curso de capacitação;
- Campanhas de divulgação da política;
- Crachás de identificação;
- Termo de responsabilidade;
- Termo de confidencialidade;
- Softwares de auditoria de acessos;
- Softwares de monitoramento e filtragem de conteúdos.

A rotina de trabalho dos colaboradores já é bastante estressante e exaustiva, transformando a conscientização e o treinamento em segurança das informações em algo interessante é uma da metas para tornar a política de segurança eficiente e eficaz. Para se chegar a este patamar faz-se necessário trazer introduzir estas informação de maneira mais prazerosa aos colaboradores através de vídeos educacionais.

7 CONCLUSÃO

A informação está sujeita a inúmeras formas de ataques, os diferentes meios são: físicos, lógicos ou humanos, sendo o último o meio de maior vulnerabilidade como vimos no decorrer do trabalho. As organizações desprendem vultuosas quantias financeiras em tecnologias de última geração para a proteção de seus seus sistemas computacionais que processam e armazenam informações contra acessos não-autorizados, porém só tecnologia não garante a segurança da informação, é necessário considerar o fator humano nesta questão. Sabendo do elo mais fraco da corrente quando o assunto é segurança, o engenheiro social atuará nesta fraqueza para invadir sistemas das organizações e obter informações para uso próprio ou de alguém que tenha contratado seus serviços.

Dentro deste contexto, foram criadas as políticas de segurança da informação com o intuito de educar e conscientizar os colaboradores sobre do que se trata a segurança da informação, que tipos de informações são consideradas sigilosa e de conhecimento público, como se deve proceder e a quem solicitar auxílio em dúvidas sobre alguma situação que possa comprometer a segurança, em outras palavras, é uma ferramenta que visa reduzir as chances de sucesso de um ataque realizado por alguém mal intencionado que sempre buscará o elo mais fraco da corrente, o fator humano.

Levando em consideração que os colaboradores integram engrenagens da segurança, e estes estão suscetíveis a falhas corrobora que as políticas da informação não garantirá um ambiente totalmente seguro. Sendo assim é necessário investir pesado em treinamentos para que os colaboradores saibam o que fazer em caso de ataque, e assim, diminuir as probabilidades de sucesso do atacante.

REFERÊNCIAS BIBLIOGRÁFICAS

1. WIKIVERSITY. Desenvolvido pela Wikiversity Foundation. Apresenta conteúdo enciclopédico. Disponível em: https://pt.wikiversity.org/wiki/Hist%C3%B3ria_da_Administra%C3%A7%C3%A3o_III. Acesso em: 12/12/2017.
2. SÊMOLA, Marcos, Gestão da segurança da Informação: visão executiva da segurança da informação. Editora Elsevier Rio de Janeiro, 2003 1
3. MÓDULO SECURITY SOLUTIONS. 9ª Pesquisa Nacional de Segurança da Informação. Rio de Janeiro, 2003. 2
4. REZENDE, Denis Alcides e ABREU, Aline França. Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais. Editora Atlas. São Paulo, 2000. 4
5. CARVALHO, G. M. R. de; TAVARES, M. da S. Informação & conhecimento: uma abordagem organizacional. 1. ed. Rio de Janeiro: Qualitymark, 2001. 5
6. FERREIRA, Aurélio Buarque de Holanda. Novo Aurélio Século XXI: o dicionário da língua portuguesa. 3 ed. totalmente rev. e ampl. Rio de Janeiro: Nova Fronteira, 1999. 6
7. HOUAISS, A. e Villar, M. de S. Dicionário Houaiss da Língua Portuguesa. Rio de Janeiro: Objetiva, 2001. 7
8. CHIAVENATO, Idalberto. Administração nos novos tempos. 2ª Edição. Rio de Janeiro: Campus, 1999. 8
9. RABAÇA, Carlos Alberto, BARBOSA, Gustavo. Dicionário de Comunicação.São Paulo: Ática, 1995. 9
10. SILVA, Heide Miranda da. Sociedade da Informação. Disponível em: < http://www.profcordella.com.br/unisanta/textos/tgs21_dados_info_conhec.htm >. Acesso em: 12/12/2017
11. DAVENPORT, Thomas H.; PRUSAK, Laurence. Working Knowledge: How Organizations Manage What They Know. Harvard Business Press, 2000. 10
12. PADOVEZE, Clóvis Luís. Sistemas de Informações Contábeis: fundamentos e análise. 2. ed.,São Paulo:Atlas,2000. 11

13. MORESI, Eduardo Amadeu Dutra. Delineando o valor do sistema de informação de uma organização. Ci. Inf. [online]. 2000. 12
14. CRONIN, Blaise. Esquemas conceituais e estratégicos para a gerência da informação. Revista da Escola de Biblioteconomia da UFMG, 1990. 13
15. WETHERBE, J. C. Análise de sistemas para sistemas de informação por computadores. São Paulo: Campus, 1987. 14
16. BIO, S. R. Sistemas de Informação: um enfoque gerencial. São Paulo: Atlas, 2004.
17. OLIVEIRA, Djalma de Pinho Rebouças de. Sistemas de informações gerenciais. 2. ed.. São Paulo: Atlas, 1993.
18. LAUDON.K.C;LAUDON, J.P. Sistemas de informação com internet. 4. ed. Rio de Janeiro: LTC, 1998.
19. CASSARRO, A . Sistema de informações para tomada de decisões. São Paulo: Pioneira, 1994
20. OLIVEIRA, Djalma de Pinho Rebouças de. Sistemas de Informações Gerenciais: Estratégicas Táticas Operacionais. 12ª Ed. São Paulo: Editora Atlas, 2008. 15
21. LAUREANO, Marcos Aurelio Pchek. Gestão de Segurança da Informação.01/06/2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf . 16
22. LAUDON, Kenneth C.; LAUDON, Jane P. Sistemas de Informação Gerencial: administrando a empresa digital. 5 ed. São Paulo: Prentice Hall, 2004. 17
23. STAIR, Ralph M. Princípios de sistemas de informação: uma abordagem gerencia. Rio de Janeiro: LTC, 2002.
24. SÊMOLA, Marcos, Gestão da segurança da Informação: visão executiva da segurança da informação. Editora Elsevier Rio de Janeiro, 2003. 18
25. Associação Brasileira de Normas Técnicas - ABNT. Norma NBR 27002. 19
26. SALVADOR, Gustavo. 2013. Entendendo os fundamentos da segurança da informação. Disponível em http://www.profissionaisti.com.br/2013/10/entendendo-os-fundamentos-daseguranca-da-informacao. 20
27. LATTARO, Alex. Uma breve viagem ao desenvolvimento da Segurança da Informação - Passado, presente e futuro. Disponível em: < https://imas-

ters.com.br/infra/seguranca/uma-breve-viagem-ao-desenvolvimento-da-seguranca-da-informacao-passado-presente-e-futuro/?trace=1519021197&source=single>. Acesso em:12/12/2017.

28. CAMPOS, André L. N. Sistema de segurança da informação: controlando os riscos. Florianópolis: Visual Books, 2007. 21
29. DANTAS, M. Segurança da Informação: Uma abordagem focada em gestão de riscos. 1 ed. Olinda: Livro rápido, 2011. 22
30. MAGALHÃES, Wanderson Fernandes. Segurança da Informação em Redes Corporativas. Barbacena: UNIPAC/FACICS, 2004. 23
31. ABREU, Dimitri. Política de Segurança - Definir para implementar. Módulo Security Magazine, 2002. 24
32. DIAS, Cláudia. Segurança e Auditoria da Tecnologia da Informação. Axcel Books. Rio de Janeiro, 2000. 25
33. WADLOW, Thomas. Segurança de Redes. Editora Campus. Rio de Janeiro, 2000. 26
34. FERREIRA, F N; ARAUJO, M. Política de Segurança da Informação. Ciência Moderna, 2006. 27
35. CASTRO, Vander de. Internet nas empresas: bloquear ou liberar o uso para atividades pessoais? 2012. 28
36. WILES, JACK; ROGERS, RUSS. Techno Security's Guide to Managing Risks for IT Managers, Auditors, and Investigators. USA: Syngress Publishing, 2007. 29
37. Sveen, F.O., Torres, J.M. and Sarriegi, J.M. Blind Information Security Strategy. International Journal of Critical infrastructure Protection, v.2, 2009. 30
38. Colwill, C. R. Human factors in information security: The insider threat & Who can you trust these days? Information Security Technical Report, 2010. 31
39. KUROSE, J. F. e ROSS, K. W. Computer Networking: A top down approach featuring the Internet, Addison Wesley, 2001. 32
40. FITZGERALD, Jerry; DENNIS, Alan. Comunicação de dados empresariais e redes. RJ: LTC, 2005. 33
41. STAMP, MARK. Information Security: Principles and Practice. Indianapolis, USA: Wiley Publishing, 2008. 34

42. STEWART, JAMES MICHAEL; TITTEL, ED; CHAPPLE, MIKE. Certified Information Systems Security Professional Study Guide. New Jersey, USA: John Wiley & Sons Publication, 2008. 35
43. FRAHIM, JAZIB; HUANG, QIANG. SSL Remote Access VPNs. Indianapolis, USA: CISCO Press, 2008. 36
44. CHIN, Liou Kuo. Redes Privada Virtual – VPN Boletim trimestral sobre tecnologia de redes. 37
45. BRANDS, STEFAN A. Rethinking Public Key Infrastructures and Digital Certificates. London, England: MIT Press, 2000. 38
46. KLOSTERBOER, LARRY. Implementing ITIL Configuration Management. Massachusetts, USA: IBM Press, 2008. 39
47. BEAL, Adriana. Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos da Informação nas Orgnizações. São Paulo: Editora Atlas, 2008. 40
48. PEIXOTO, Mário C. P. P. Engenharia Social e Segurança da Informação na Gestão Corporativa. Rio de Janeiro: Brasport, 2006. 41
49. FONSECA, Paula Fernanda. Gestão de Segurança da Informação: O Fator Humano. 2009. Artigo (Pós Graduação em Redes e Segurança de Computadores) – Pontifícia Universidade Católica do Paraná, Curitiba, 2009. 42
50. ARAUJO, Eduardo. A Vulnerabilidade Humana na Segurança da Informação. 2005. 43
51. SÊMOLA, Marcos. Gestão da Segurança da Informática: Uma Visão Executiva. 10ªed. Rio de Janeiro: Elsevier, 2003. 44