INSTITUTO FEDERAL GOIANO - CAMPUS MORRINHOS
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS PARA INTERNET

IVAN DE ALMEIDA SANTOS

SEGURANÇA DA INFORMAÇÃO:
Um modelo de política para ambientes computacionais

MORRINHOS
2016

IVAN DE ALMEIDA SANTOS

SEGURANÇA DA INFORMAÇÃO:
Um modelo de política para ambientes computacionais

Trabalho de curso apresentado ao Curso Superior de Tecnologia em Sistemas para Internet do Instituto Federal Goiano-Campus Morrinhos, como requisito parcial para obtenção de título de Tecnólogo em Sistemas para Internet.

Área de concentração: Segurança da Informação.
Orientador: Antônio Neco de Oliveira

MORRINHOS
2016

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas – SIBI/IF Goiano Câmpus Morrinhos

S237s Santos, Ivan de Almeida.

Segurança da informação : um modelo de política para ambientes computacionais / Ivan de Almeida Santos. – Morrinhos, GO: IF Goiano, 2016.
62 f. : il : color.

Orientador: Msc. Antônio Neco de Oliveira.

Trabalho de conclusão de curso (graduação) – Instituto Federal Goiano Câmpus Morrinhos, Curso de Tecnologia em Sistemas para Internet, 2016.

1. Gestão de riscos. 2. Política de segurança. 3. Informação. I. Oliveira, Antônio Neco de. II. Instituto Federal Goiano. Curso de Tecnologia em Sistemas para Internet. III. Título

CDU 004.056(043)

IVAN DE ALMEIDA SANTOS

SEGURANÇA DA INFORMAÇÃO:
Um modelo de política para ambientes computacionais

Data da defesa: 28 de janeiro de 2016.

Resultado: _____

BANCA EXAMINADORA ASSINATURAS

Antônio Neco de Oliveira Prof. Msc_____
Instituto Federal Goiano Campus Morrinhos

José Pereira Alves Prof. Esp _____
Instituto Federal Goiano Campus Morrinhos

Odilon Fernandes Neto Prof. Esp_____
Instituto Federal Goiano Campus Morrinhos

MORRINHOS
2016

DEDICATÓRIA

Dedico este trabalho primeiramente aos meus pais Romeu e Vânia, que sempre em minhas fraquezas e preocupações, me deram forças para continuar e chegar até o final. E ainda pela educação e a importância do estudo que sempre pregaram.

À minha esposa Aline, que sempre esteve ao meu lado me alegrando com seus carinhos, amor, cuidados e que ainda me deu o maior presente que poderia ganhar, ser pai.

Dedico também a todos aqueles que torceram e rezaram por mim, para que conseguisse alcançar mais essa vitória em minha vida.

AGRADECIMENTOS

Agradeço, em primeiro lugar a DEUS pelo dom da vida. Por me permitir viver cada dia, por me dar forças e me abençoar nos momentos em que a dor e o desespero batem a nossa porta.

Agradeço a paciência de todos os meus colegas, amigos e companheiros, que nas minhas dificuldades sempre estenderam a mão e ofereçam a ajuda que eu precisava. E nos momentos mais obscuros do caminho, nos demos as mãos e caminhamos juntos em busca de um objetivo.

Agradeço a todos os funcionários da instituição por prestar os serviços dos quais precisávamos, em especial ao meu amigo/irmão Paulo Sebastião Vaz, que mesmo com suas obrigações sempre esteve disposto a me ajudar e incentivar.

Agradeço a todos os professores por sempre estarem dispostos a nos passar os seus conhecimentos, pela dedicação na arte de ensinar, e por mais que a profissão traga dificuldades, nunca deixaram a alegria que sempre nos contagiou.

E por fim, um agradecimento especial ao professor Antônio Neco de Oliveira, por ter aceitado ser meu orientador e ter a paciência e a vontade de me ajudar nessa etapa final de curso.

RESUMO

O presente trabalho apresenta o quanto a segurança da informação é importante e indispensável em uma organização, por se tratar de um conjunto normas capazes de proteger o seu principal patrimônio, a informação. Para que a segurança da informação seja concretizada de forma aceitável, os seus princípios Confiabilidade, Integridade e Disponibilidade devem sempre serem satisfeitos. Define, também, como a informação deve ser tratada e seu real valor nas regras do negócio, como é importante a sua classificação e o conhecimento do seu ciclo de vida, além de conhecer a quais riscos ela está exposta. É de extrema importância, que todos na organização sejam envolvidos no processo de implantação de segurança da informação, e que todos tenham o conhecimento das regras adotadas na política de segurança, visto que a vulnerabilidade da informação não é um problema somente da área de informática, mas sim de todos. Os ataques sempre buscaram o elo de segurança mais fraco para se concretizarem; portanto, a política de segurança implantada deve prever esses acontecimentos, apresentando as normas, regras e procedimentos para o uso da informação.
Porém, para que possa entender todo o universo da informação lógica, é importante apresentar o modo como ela é distribuída e acessada no universo da Internet, um mundo sem barreiras onde milhares de pessoas se encontram todos os dias, sempre em busca de mais informações. Para esse fim, os conceitos de redes são apresentados para dar uma ideia de como tudo funciona e da importância do assunto segurança da informação.

Palavras-Chaves: Segurança da Informação; Política de Segurança; Informação;

ABSTRACT

This paper will present how information security is important and essential in an organization, because it is a set of standards that protect their main asset, information. So that information security is implemented in an acceptable manner, the principles of Reliability, Integrity and Availability must always be satisfied. It also defines how the information should be treated and their actual value in the business rules, how important their rating and the knowledge of their life cycle, and know what risks it is exposed. It is of extreme importance that everyone in the organization are involved in information security implementation process, and you all have knowledge of the rules adopted in the security policy, since the vulnerability information is not a problem computer area only, but overall. The attacks have always sought the weakest security link vine materialize therefore deployed security policy should provide for these events, presenting the standards, rules and procedures for the use of information.

But so you understand the whole universe of logic information, it is important to present the way it is distributed and accessed in the Internet universe, a world without barriers where thousands of people meet every day, always looking for more information. For this purpose, the concepts of networks appear to have an idea of how everything works and the importance of the subject information security.

Key Words: Information Security; Security policy; Information;

LISTA DE FIGURAS

Figura 1 - Elemento da Comunicação de Dados 18
Figura 2 - Transmissão de Dados 19
Figura 3 - LAN (Local Area Network) 20
Figura 4 - MAN (Metropolitan Area Network) 21
Figura 5 - WAN (Wide Area Network) 22
Figura 6 - Rede Ponto a Ponto 23
Figura 7 - Rede Cliente/Servidor 24
Figura 8 - Estrutura do endereço IP 26
Figura 9 - Etapas para Análise de Riscos 40
Figura 10 - Estrutura de um modelo de política de segurança 45
Figura 11: Exemplo de rede em uma organização 47
Figura 12 - Script para Mapeamento da Pasta do Departamento 51
Figura 13 - Script para bloqueio e desbloqueio de portas USBs 53

LISTA DE SIGLAS

ABNT	Associação Brasileira De Normas Técnicas;
AD-DS	Active Directory - Domain Server;
BR	Brasil;
DDoS	Distributed Denial of Service;
DHCP	Dynamic Host Configuration Protocol;
DNS	Domain Name System;
DoS	Denial of Service;
EUA	Estados Unidos da América;
IDS	Intrusion Detection Systems;
IPS	Intrusion Prevention System;
LAN	Local Area Network;
MAN	Metropolitan Area Network;
NOS	Network Operating System;
PT	Português;
TCP	Transmission Control Protocol;
USB	Universal Serial Bus;
WAN	Wide Area Network;

SUMÁRIO

1. INTRODUÇÃO 12
1.1. JUSTIFICATIVA 13
1.2. OBJETIVOS 14
1.2.1. Objetivo Geral 14
1.2.2. Objetivos Específicos 14
1.3. METODOLOGIA 14
1.4. ORGANIZAÇÃO DO TRABALHO 15

2. A EVOLUÇÃO DAS REDES DE COMPUTADORES 16
2.1. CONHECENDO AS REDES DE COMPUTADORES 17

3. SEGURANÇA DA INFORMAÇÃO 28
3.1. A IMPORTÂNCIA DA INFORMAÇÃO 28
3.2. CLASSIFICAÇÃO DA INFORMAÇÃO 29
3.3. CICLO DE VIDA DA INFORMAÇÃO 30
3.4. CONCEITO DE SEGURANÇA DA INFORMAÇÃO 31
3.5. AMEAÇAS À INFORMAÇÃO 33
3.5.1. Ameaças fundamentais 33
3.5.2. Ameaças à segurança da informação 34
3.6. VULNERABILIDADES DA INFORMAÇÃO 37
3.7. GESTÃO DE RISCO 38

4. MODELO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 42
4.1. TIPOS DE POLÍTICAS DE SEGURANÇA 43
4.1.1. Política Regulatória 43
4.1.2. Política Consultiva 44
4.1.3. Política Informativa 44
4.2. UM MODELO ESTRUTURAL DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 45
4.3. POLÍTICA DE USO E ACESSO À REDE CORPORATIVO E À INTERNET 47
4.3.1. Objetivo 48
4.3.2. Definições 48

4.3.3. Escopo e Abrangência 48
4.3.4. Acesso à Internet 49
4.3.5. Atividades proibidas no uso da Internet 49
4.3.6. Acesso à rede 50
4.3.7. Política de senhas 51
4.3.8. Política de uso de computadores 52
4.3.9. Utilização de e-mail 53
4.3.10. Acesso físico 54
4.3.11. Política de backup 54
4.3.12. Responsabilidades 54
4.3.13. Cumprimentos das Normas 55
4.4. FERRAMENTAS E TÉCNICAS PARA A PROTEÇÃO DA INFORMAÇÃO 55
4.4.1. Antivírus 55
4.4.2. Criptografia de dados 56
4.4.3. Firewall 57
4.4.4. Sistema de detecção de intrusos (IDS) 57

5. CONSIDERAÇÕES FINAIS 59
5.1. TRABALHOS FUTUROS 60

REFERÊNCIAS 61

1. INTRODUÇÃO

Vivemos a era da tecnologia em que manchetes de novos casos de informações confidenciais que são roubadas e publicadas ou usadas para se obter vantagens sobre os concorrentes ou para se executar fraudes tornam-se comuns. Por conta de tantos transtornos e prejuízos causados por uma perda ou roubo de informações, vemos o quão valiosa uma informação pode ser.

Quando falamos de informação, é importante deixar claro que não estamos falando apenas de dados eletrônicos, de comunicação entre computadores ou de um ambiente centralizado na informática. Mas, também, das inúmeras informações escritas que são arquivadas em papel e cuja importância, muitas vezes, superam as informações digitais.

Vivemos em função de informações, sejam em papel ou virtual, que de alguma forma se localizam nos bancos de dados de uma empresa ou no próprio computador pessoal (Machado, 2014).

A segurança da informação abrange todos os tipos de informações, seja escrita, falada ou armazenada em formato eletrônico. Para cada tipo, é extremamente importante a adoção de políticas de segurança corretas que mantenham essas informações protegidas de eventuais ameaças. Neste trabalho aborda-se a proteção das informações eletronicamente armazenadas ou criadas, baseando-se em normas e em literaturas, que apresentam as medidas a serem adotadas e como as políticas de segurança da informação podem ser implantadas, acompanhada de ferramentas para auxiliar na manutenção de um ambiente seguro e com menor vulnerabilidades.

O setor que gera mais preocupação em relação à segurança da informação é o ambiente de redes de computadores. Portanto, abordar-se-ão conceitos de redes como: os principais tipos de redes, a comunicação de dados e como tudo evoluiu para os padrões que temos hoje.

O crescimento desacelerado das tecnologias de comunicação traz consigo um aumento incalculável de vulnerabilidades. A política de segurança da informação tem um papel importante em uma organização, devendo ser divulgada e estar de acordo com as expectativas da administração em relação à segurança de suas informações. O processo de criação pode ser considerado difícil e árduo, motivando

a apresentação de um modelo de política de segurança da informação, aplicando os conceitos e normas de segurança da informação. Juntamente ao modelo de política de segurança da informação apresentada, são descritas possíveis implementações de ferramentas e recursos para garantir que as regras sejam cumpridas.

1.1. JUSTIFICATIVA

Com o grande avanço tecnológico, cada vez mais torna-se necessário o investimento em segurança da informação. Assim como surgem novas ferramentas para facilitar e agilizar as atividades em uma organização, as técnicas de invasão e de violação da informação também evoluem, de forma rápida e eficiente. Com isso, pode-se afirmar que não existe ambiente 100% seguro, por esse motivo, as políticas de segurança devem ser bem elaboradas e atualizadas, juntamente aos recursos de segurança atuantes nas empresas.

Portanto, cada organização deve preparar-se para responder de maneira correta e mais eficaz possível, cada ameaça que venha ocorrer em seu ambiente computacional e ela deve ter o conhecimento de suas vulnerabilidades, monitorando-as de maneira especial. Deve-se ter um plano de contingência com especificações de ações a serem tomadas em caso de necessidade imediata.

O que influenciou este trabalho foi a dificuldade que a administração das empresas encontra no desenvolvimento de uma política de segurança eficaz, que reforce a importância da informação perante os usuários, para minimizar a ocorrência e o impacto gerado pelos ataques que venham a ocorrer.

1.2. OBJETIVOS

1.2.1. Objetivo Geral

O objetivo geral deste trabalho é apresentar os conceitos principais que englobam as teorias e normas de segurança da informação, para garantir o compartilhamento de informações nos ambientes computacionais.

1.2.2. Objetivos Específicos

Apresentar os conceitos de informação, segurança da informação, política de segurança da informação e redes de computadores.

Apresentar um modelo de Política de segurança da informação que facilite o desenvolvimento, implantação e manutenção das regras.

Descrever a utilização de ferramentas que possam ser usadas no cumprimento das regras adotadas na política de segurança.

Descrever os principais tipos de ameaças e as formas de ataques mais utilizadas e as medidas adotadas para garantir o acesso à informação com integridade e confidencialidade.

1.3. METODOLOGIA

A pesquisa exploratória será baseada na bibliografia levantada. Os dados serão coletados através de buscas em artigos acadêmicos, livros, normas de regulamentação, revistas e outros trabalhos relacionados.

Para demonstrar uma política de segurança, será elaborado um modelo com regras que podem ser implantadas em um ambiente computacional, criando a política de uso de equipamentos e descrevendo ferramentas que auxiliem na manutenção da segurança da informação.

1.4. ORGANIZAÇÃO DO TRABALHO

Para uma melhor abordagem, este trabalho está dividido nos seguintes capítulos:

O capítulo 2 apresenta um breve histórico de como as redes foram criadas, qual o seu objetivo, como foi desenvolvida e como funciona a comunicação de dados. São apresentados os conceitos básicos de redes de computadores, os tipos e a classificação.

No capítulo 3 define-se o que é informação, a sua importância para as organizações e o seu valor para a continuidade do negócio. São definidos os conceitos e as boas práticas de segurança da informação que garantem a Confiabilidade a Integridade e a Disponibilidade da informação.

O capítulo 4 apresenta um modelo de política de segurança da informação para ser aplicado em um ambiente computacional, os requisitos e regras da política de segurança. Descreve como podem ser implantados alguns controles para que as regras sejam cumpridas.

No capítulo 5 apresentam-se as considerações finais com indicações de trabalhos futuros.

2. A EVOLUÇÃO DAS REDES DE COMPUTADORES

No século XX tivemos como marco de evolução tecnológica, a capacidade de adquirir, processar e compartilhar a informação com o surgimento das linhas de telecomunicações mundiais, o rádio e a televisão, os satélites e principalmente o crescimento acentuado da indústria de informática. Com esse desenvolvimento, hoje é cada vez mais fácil e rápido executar todo o ciclo da informação, pois, as fronteiras foram rompidas, distâncias encurtadas. Uma empresa pode se comunicar e monitorar em tempo real todas as suas unidades, mesmo estando instaladas em regiões, países ou até mesmo em outros continentes (Tanenbaum, 2003).

Tanenbaum (2013), ainda explica que, anteriormente a esse grande avanço tecnológico, tínhamos um cenário completamente diferente. Os computadores eram de grande porte e ocupavam grandes áreas na empresa, além do processamento ser executado em *batch*[1] de forma *off-line*[2]. Hoje, com a junção dos computadores e da comunicação, percebemos um cenário muito diferente, onde o trabalho de processamento da informação é executado em tempo real por um grande número de computadores alocados separadamente, mas interconectados pelas redes de computadores.

Torres (2014), define que rede de computador é quando mais de um computador utilizando o mesmo protocolo de comunicação, compartilham informações e recursos, através de um tipo de conexão.

Com o rápido avanço de tecnologias voltadas para a comunicação de dados, a distância em que os computadores conseguiam se comunicar foram aumentando, com isso, houve o surgimento da Internet. A internet é uma rede de redes, interligando computadores pelo mundo inteiro.

A Internet é mais uma das inúmeras tecnologias produzidas em busca de vantagens e poder durante uma guerra. Sua criação se deu durante a *Guerra Fria*[3] e foi fruto de pesquisas de militares dos EUA, pois temiam um ataque às suas bases

---

[1] *Batch:* é um arquivo em lote usado para automatizar tarefas em um sistema.

[2] *Off-line:* sem conexão a um computador associado.

[3] *Guerra Fria:* é a designação atribuída ao período histórico de disputas estratégicas e conflitos indiretos entre os Estados Unidos e a União Soviética, disputando a hegemonia política, econômica e militar no mundo.

militares. Seu intuito era permitir a troca de mensagens para que as informações fossem descentralizadas, e se bases fossem atingidas as informações estariam replicadas em outras bases, fazendo com que os dados armazenados não se perdessem. Foi assim que, por volta de 1969, o Departamento de Defesa Americano desenvolveu a *ARPAnet*[4].

Com o surgimento da *ARPAnet*, o desenvolvimento de uma série de *protocolos de rede*[5] contribuiu para que sua comunicação melhorasse. No início da década de 80 outras redes se juntaram à *ARPAnet* que, por sua vez, passou a ser chamada de Internet.

Portanto, com o grande crescimento da Internet desde sua criação, muitas tecnologias de comunicação foram criadas e melhoradas para o processo de transmissão de informação ser mais rápido e seguro, e as redes de comunicações e a Internet tornaram-se cada vez mais indispensáveis.

2.1. CONHECENDO AS REDES DE COMPUTADORES

Apresenta-se de maneira geral, como uma rede de computadores funciona e como ocorre a transferência das informações, com conceitos suficientes para permitir a aplicação da segurança da informação em um ambiente computacional, seja ele empresarial ou doméstico.

Para que haja troca de informações entre os computadores, alguns elementos são fundamentais. A comunicação de dados corresponde aos agentes responsáveis pela troca de informações.

Segundo Forouzan (2006), comunicação de dados é a troca de informação entre dois dispositivos através de algum meio de comunicação. Em um sistema de comunicação de dados básico encontramos cinco elementos:

---

[4] *ARPAnet (Advanced Research Projects Agency):* primeira rede de computadores desenvolvida pelo Departamento de Defesa dos EUA, cujo objetivo era manter o sistema de comunicação mesmo com avarias locais (Simon, 1997).

[5] *Protocolos de rede:* são regras que governam e possibilitam uma conexão, comunicação ou transferência de dados entre dois sistemas.

Mensagem: é a informação a ser transmitida. Pode ser formada por letras, números, imagens, áudio e vídeo, ou qualquer conjunto destes elementos.

Transmissor: é o dispositivo que envia a mensagem. Pode ser um telefone, computador, *tablet*[6], entre outros.

Receptor: é o dispositivo que recebe a mensagem.

Meio: é o caminho físico por onde a mensagem trafega do transmissor ao receptor.

Protocolo: representa um padrão de comunicação estabelecido de forma a possibilitar a comunicação entre os dispositivos, sendo assim, é um conjunto de regras que possibilita a comunicação de dados.

A Figura 1 apresenta os elementos presentes na comunicação de dados.

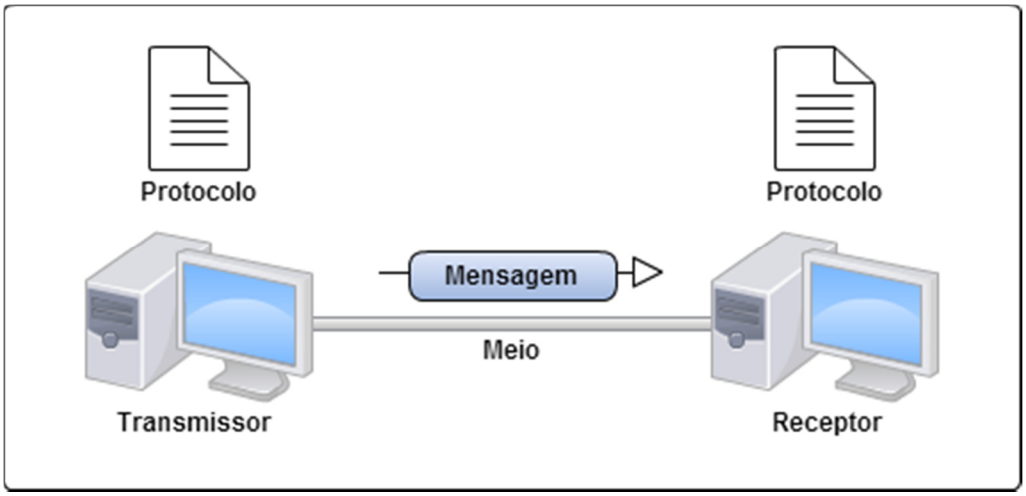

Figura 1 - Elemento da Comunicação de Dados
Fonte: (Alencar, 2010)

Portanto, para que haja uma comunicação de dados, é necessário que todos os elementos estejam presentes e em harmonia uns com os outros, desde a criação da mensagem passando pelo meio até chegar ao receptor de destino.

O meio de transmissão de dados pode operar de três formas diferentes: *simplex*, *half-duplex ou full-duplex*.

No modo de operação *simplex*, temos um transmissor e um receptor, mas a mensagem sempre trafegará em apenas um sentido. O transmissor nunca será um

---

[6] *Tablet:* tipo de computador portátil de tamanho reduzido de espessura fina e sensível ao toque.

receptor e o receptor nunca será um transmissor. Podemos citar como exemplo as transmissões de Televisão e Rádio que sempre trafegam no sentido do receptor, mas nunca recebem um retorno da mensagem.

O modo *Half-Duplex* tem agentes transmissores e receptores em cada lado, e ambos podem transmitir, mas nunca ao mesmo tempo. Nesse modo, o meio físico é liberado totalmente para o agente que está transmitindo. Um exemplo são os *Walkie-talkies*[7].

No modo de operação *Full-Duplex* temos o transmissor e o receptor transmitindo e recebendo mensagens ao mesmo tempo. O meio físico é compartilhado por ambos. Esse modo de operação pode ser feito de duas maneiras: no meio físico pode existir dois caminhos separados, onde, um envia e o outro recebe as mensagens, ou existe um meio físico compartilhado para transmissão e recepção. Um exemplo é o canal de voz de telefonia, onde duas pessoas podem falar e ouvir ao mesmo tempo.

A Figura 2 ilustra os tipos de transmissão de dados.

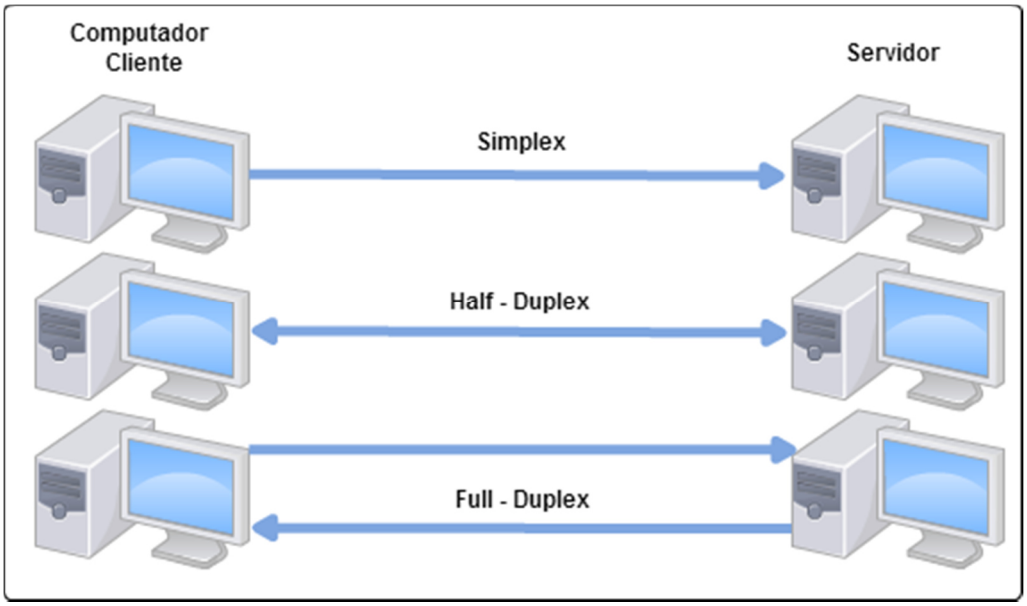

Figura 2 - Transmissão de Dados
Fonte: (http://www.twalves.com/img/tipos-transmissoes-dados.jpg)

[7] Walkie-talkies: pequeno aparelho de rádio emissor e receptor, usado para comunicações de curta distância.

Contudo, cada modo de operação possui características próprias, que podem ser utilizadas em diferentes soluções para o envio de informações entre dispositivos.

A transmissão de dados pode ser realizada entre grandes distâncias, dependendo do meio físico de transmissão utilizado. Levando em conta essa característica, podemos encontrar redes de vários tamanhos, com quantidades diferentes de computadores e usuários, e elas classificam-se como locais – *Local Area Networks* (*LANs)*, metropolitanas - *Metropolitan Area Networks (MANs)* e geograficamente distribuídas - *Wide Area Networks (WANs)*.

Segundo Tanenbaum (2003), as redes locais são redes privadas contidas em um único edifício ou campus universitário com até alguns quilômetros de extensão. Elas são amplamente utilizadas para conectar computadores pessoais e estações de trabalho em escritórios e instalações industriais, permitindo o compartilhamento de recursos e troca de informações.

A Figura 3 ilustra uma LAN, na qual os computadores estão interligados e se comunicam entre si, além de compartilharem recursos de hardware e software como impressoras, scanner entre outros.

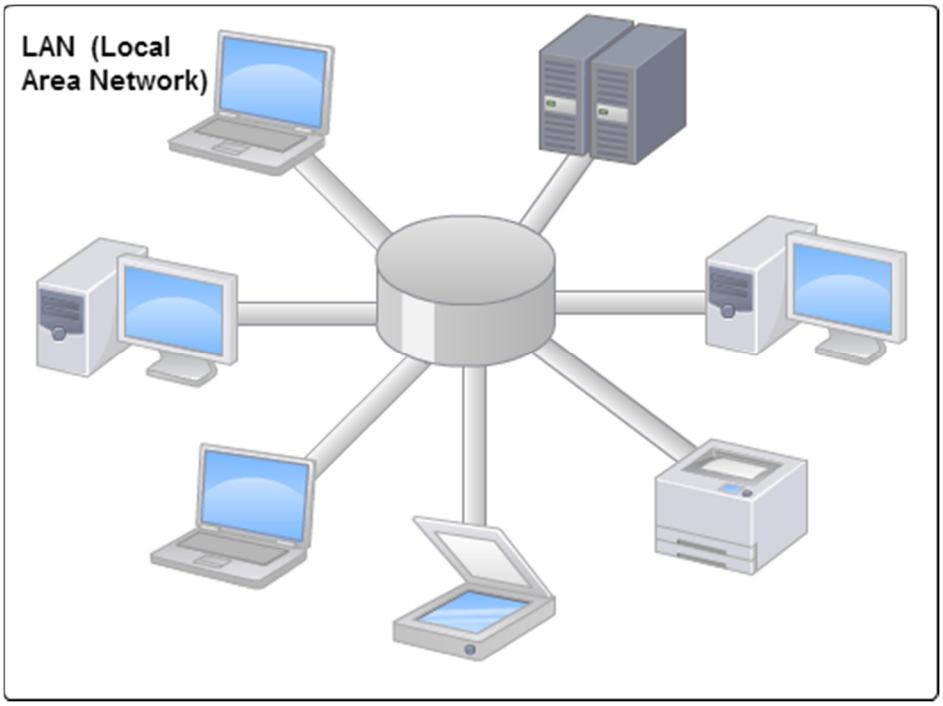

Figura 3 - LAN (Local Area Network)
Fonte: (http://eduscol.education.fr/sti/domaines/energie-et-information)

As *Metropolitan Area Networks (MANs),* podem ser caracterizadas por uma maior distância entre os pontos de conexão, podendo interligar várias *LANs* em uma mesma cidade. Portanto, um conjunto de *LANs* interconectadas formam uma MAN, como mostra a Figura 4.

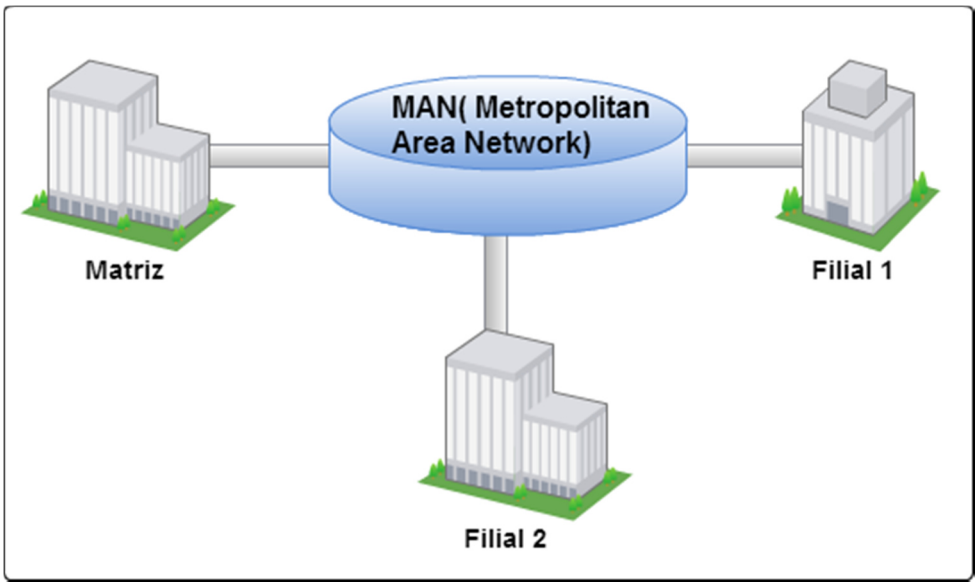

Figura 4 - MAN (Metropolitan Area Network)
Fonte: (http://fabrica.ms.senac.br/wp-content/uploads/2013/07/MAN.jpg)

Neste exemplo, cada prédio possui uma *LAN* interna, e as *LANs* estão conectadas entre si formando uma *MAN*. Neste modelo é possível que as informações de um computador em um dos prédios possam ser acessadas de qualquer prédio que esteja dentro da mesma *MAN*, facilitando o compartilhamento de recursos da rede. São muito utilizadas por empresas, hospitais e outros estabelecimentos que tenham várias unidades em uma mesma cidade.

Quando a distância entre as redes ultrapassa os limites de uma cidade, é utilizado o conceito de *WANs*, que podem interligar regiões e até mesmo, continentes. As *WANs* são redes de longa distância muito utilizadas por grandes corporações para interligarem suas unidades e terem acesso às informações de todas as unidades em qualquer lugar.

Na Figura 5 podemos observar várias *LANs*, que podem ser as várias unidades de uma empresa em uma cidade ou em uma região. As *MANs* fazem as interligações entre elas e a WAN que, estabelece a comunicação entre todos

utilizando-se de uma infraestrutura de longa distância. Podemos dizer que a Internet é uma grande WAN que interliga inúmeras redes, sejam elas públicas ou privadas.

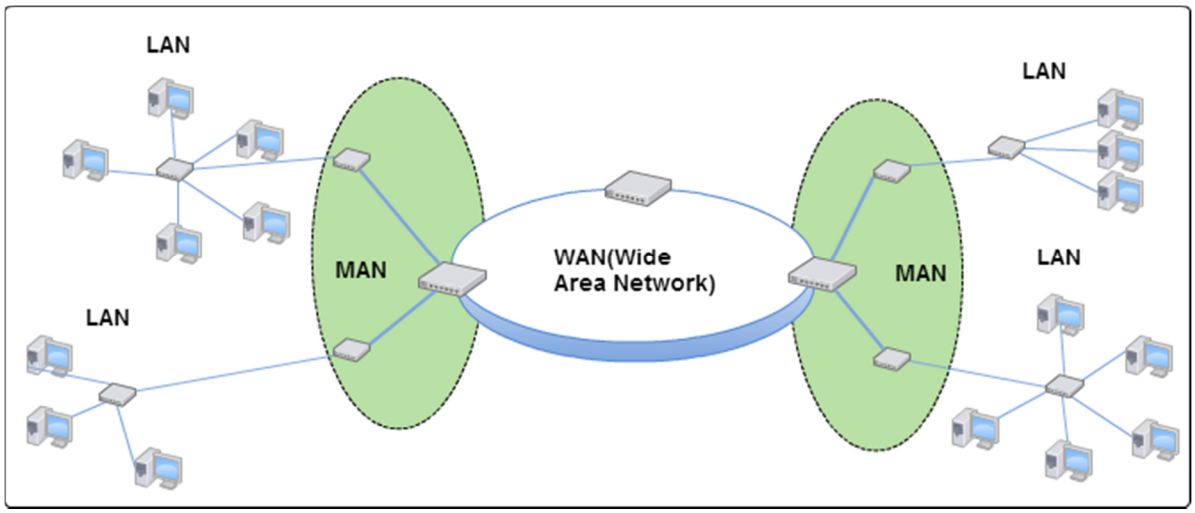

Figura 5 - WAN (Wide Area Network)
Fonte: (http://player.slideplayer.com.br/8/2331910/data/images/img16.jpg)

As redes de computadores também podem ser classificadas levando-se em consideração sua instalação lógica. Classificam-se em redes Ponto a Ponto e redes cliente/Servidor, ambas possuem vantagens e desvantagens.

> As redes Ponto a Ponto não possuem hierarquias, todos os computadores podem ser iguais não havendo um elemento controlador de recursos de forma centralizada, fazendo com que os usuários possam acessar qualquer arquivo ou informação que esteja em qualquer computador da rede sem pedir permissão. Neste tipo de rede o próprio sistema operacional possui mecanismos de compartilhamento e mapeamento de arquivos e impressoras, mecanismos de segurança menos eficientes, esta arquitetura é indicada para redes com poucos computadores (Costa, 2010 p.8).

A Figura 6 ilustra o modelo lógico de uma rede Ponto a Ponto, onde os computadores são interligados e cada terminal controla seus recursos utilizando-se das ferramentas que cada sistema operacional instalado possibilita.

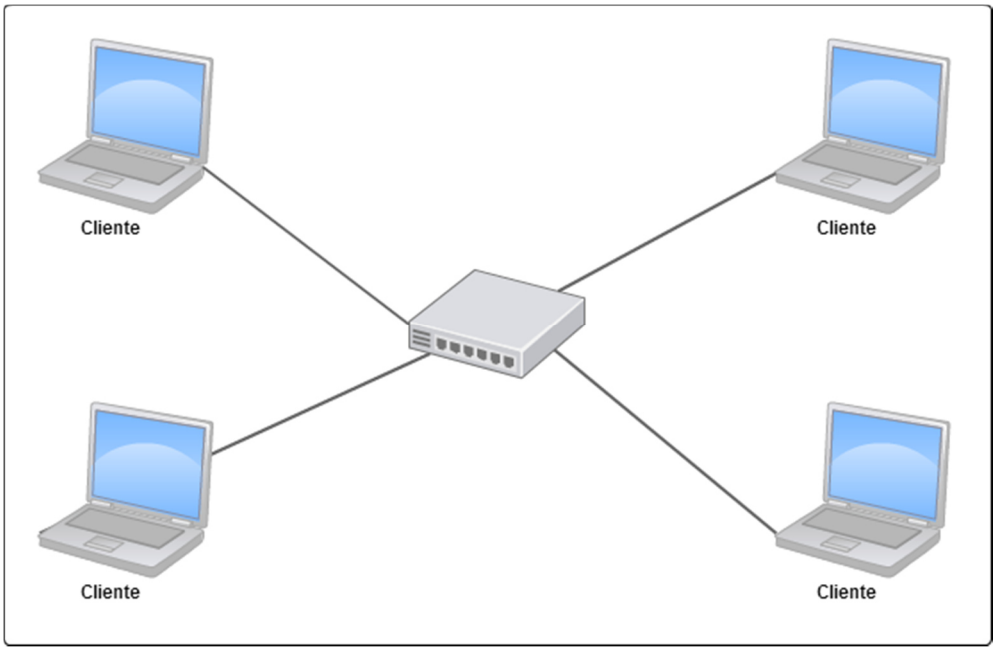

Figura 6 - Rede Ponto a Ponto
Fonte: (Costa, 2010)

Características Ponto a Ponto:

- Fácil instalação e configuração;
- O próprio usuário configura recursos;
- Não há necessidade de um administrador de rede;
- Sistema operacional local;
- Segurança limitada;
- Baixo custo, entre outras.

No Modelo Cliente/Servidor encontramos um computador que cumpre o papel de gerenciar todos os acessos e recursos disponibilizados na rede, centralizando a administração e melhorando a segurança e a organização da rede.

Nesse modelo, torna-se importante a figura do administrador da rede, pois será o responsável por acompanhar o desempenho, as configurações e o acesso dos usuários às informações contidas no *servidor*[8]. O computador cliente solicita o serviço ao computador servidor que, por sua vez, só libera para clientes autorizados.

[8] *Servidor* é um sistema computacional centralizado que fornece vários serviços a uma rede de computadores. Geralmente é o hardware de maior desempenho na rede.

> A arquitetura Cliente/Servidor é mais sofisticada, nesta arquitetura o usuário fica dependente do Servidor, uma máquina central, que retém todas as leis de utilização da rede em um software chamado Sistema Operacional de Rede (NOS) (Costa, 2010 p.8).

A Figura 7 apresenta um diagrama de uma rede cliente/servidor.

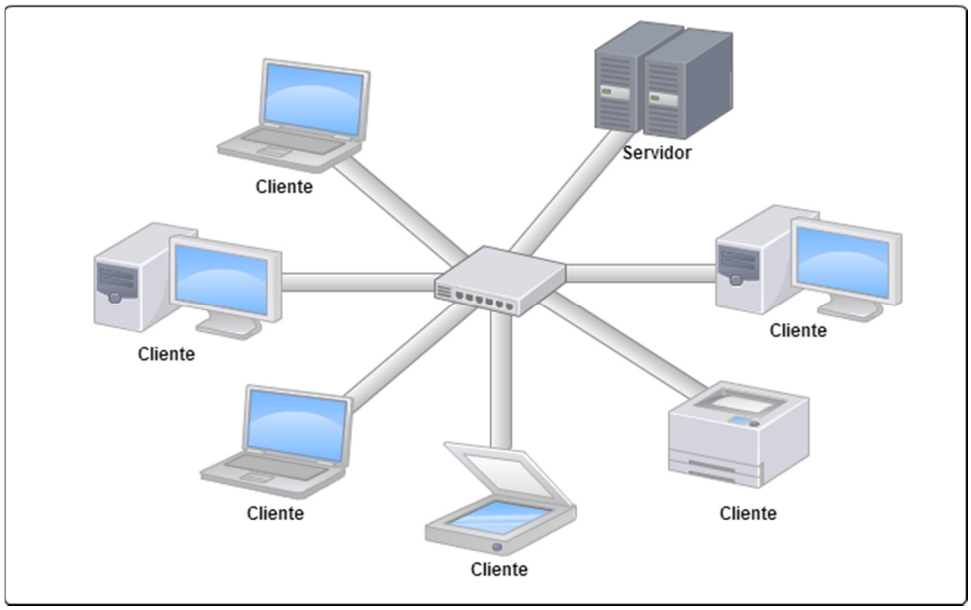

Figura 7 - Rede Cliente/Servidor
Fonte: (Costa, 2010)

Características Cliente/Servidor:

- Utiliza sistema operacional de rede;
- Gerência o acesso aos recursos;
- Segurança;
- Custo de implantação mais alto;
- Maior desempenho;
- Necessita de um administrador.

Alguns serviços executados em um servidor de rede:

- Serviço Controlador de Domínio;
- Serviço de *Firewall*[9] (Segurança);

[9] *Firewall* é uma solução de hardware ou software, que analisa um conjunto de regras para filtrar o trafego de rede para determinar quais transações podem ser executadas.

- Serviço de Arquivos;
- Serviço de *FTP*[10] (*File Transfer Protocol*);
- Serviço Web;
- Serviço de Impressão;
- Serviço de Banco de Dados, entre outros.

Portanto, a arquitetura cliente/servidor dispõe de soluções importantes para manter os serviços de rede mais seguros e mais estáveis, visto que a velocidade e o desempenho da rede são maiores se comparados com a Ponto a Ponto.

Foram apresentadas as definições e estruturas como uma rede pode se comportar, porém, de nada adiantaria se não existissem os protocolos de rede para intermediar e estabelecer a comunicação entre os computadores. Protocolos são, basicamente, a parte do sistema operacional da rede encarregada de ditar as normas para a comunicação entre os dispositivos (Costa, 2010 p.63).

Os protocolos são responsáveis por definir a estrutura da mensagem, os métodos de compartilhamento de informações de rotas entre os dispositivos, como e quando informações de erro ou de sistemas serão repassadas entre os dispositivos, controlar e fechar seções ao término das transferências de informações. Os protocolos controlam todas as etapas do processo de transmissão de dados.

A arquitetura de protocolos mais utilizados para gerenciar a comunicação entre os computadores de uma rede é o Protocolo de Controle de Transmissão *TCP/IP* (*Transmission Control Protocol*) e Protocolo de Interconexão *IP (Internet Protocol)*, que juntamente a outros protocolos formam a arquitetura TCP/IP.

O protocolo IP tem como função identificar de forma única todos os dispositivos conectados em uma rede TCP/IP e permitir o roteamento das informações. Essa identificação é feita pelo endereço IP. O endereço IPv4 é formado por 32 bits que são agrupados em quatro grupos de 8 bits chamado de *octeto*. A Figura 8 apresenta um exemplo de endereço IP onde podemos notar os octetos referente a cada um dos grupos que formam o endereço IP.

---

[10] *FTP (File Transfer Protocol)* é um protocolo para transferência de arquivos vai internet utilizado para enviar e receber arquivos de um servidor FTP.

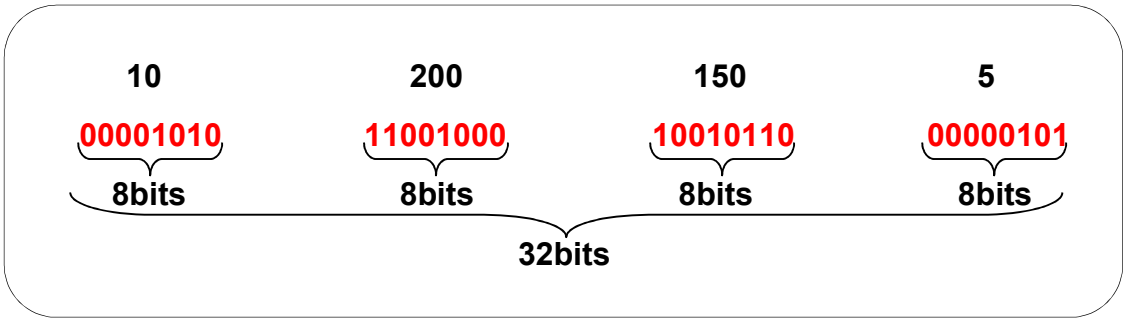

Figura 8 - Estrutura do endereço IP

Um endereço IP pode ser configurado de maneira estática ou dinâmica, ou seja, ele pode ser fixado manualmente nas configurações do dispositivo de rede ou de forma dinâmica através de um servidor *DHCP (Dynamic Host Configuration Protocol)*, que é responsável por controlar o endereçamento da rede para dispositivo.

O protocolo TCP (*Transmission Control Protocol*) foi criado para garantir um fluxo de dados confiável. O TCP tem como principal característica a robustez diante de várias falhas se adaptando aos tipos de rede encontrados. Basicamente ele fornece a garantia da entrega da informação, checando cada pacote entregue e solicitando a retransmissão quando necessário. Também é papel do TCP organizar os pacotes recebidos, uma vez que eles não são transmitidos na ordem correta. O TCP deve fornecer a confiabilidade que a maioria dos usuários deseja, mas que o IP não oferece (Tanenbaum, 2003).

Afinal, os protocolos da família *TCP/IP* formam a estrutura de comunicação da Internet, permitindo o compartilhamento de informações, pois, cada protocolo, desenvolve atividades específicas.

Na Internet, quando se navega em sites, observa-se uma outra funcionalidade muito importante quanto ao endereçamento, são os chamados servidores de *DNS (Domain Name Service),* Sistema de Nomes de Domínio. O *DNS* é responsável por associar o nome de um domínio em endereço *IP*, facilitando a navegação, por ser bem mais fácil decorar um nome do que um número. Por exemplo, é bem fácil decorar o nome www.uol.com.br do que 200.221.2.45 que é o *IP* associado a ele.

Apresentados os conceitos básicos da comunicação de dados e de redes de computadores, já é possível entender como a informação transmitida percorre grandes distâncias para chegar a seu destino. O principal papel da segurança da informação é encontrar e minimizar as falhas existentes no ambiente computacional através de normas e boas práticas, assegurando um ambiente seguro para o compartilhamento de informação.

3. SEGURANÇA DA INFORMAÇÃO

Para que o assunto Segurança da Informação seja abordado, é fundamental que se entenda os conceitos de informação, qual a sua importância e valor para uma organização, como ela pode ser classificada e qual o seu ciclo de vida dentro da organização. Com esses conceitos podemos aplicar os princípios da segurança da informação para que se garanta a continuidade do negócio.

3.1. A IMPORTÂNCIA DA INFORMAÇÃO

O conceito de informação é de difícil compreensão, uma ideia de difícil entendimento. Na busca por uma definição, a informação é uma parte fundamental de nossa existência, tem uma importância e um poder imenso, e quem as detém é capaz de tomar decisões importantes e precisas em meio a sérios problemas, onde a informação pode ser usada para criar ordem e uma nova estrutura. Segundo o Dicionário AURÉLIO (1999), informação é um dado acerca de alguém ou algo; o conhecimento; segundo a teoria da informação, a medida da redução da incerteza.

De acordo com DIAS (2000), a informação é o principal patrimônio da empresa e está sob constante risco. As empresas se deram conta que o uso da tecnologia para a manipulação da informação é vital para o seu crescimento. O controle da informação é um fator de sucesso crítico para os negócios e sempre teve fundamental importância para as corporações do ponto de vista estratégico e empresarial (MARTINS, 1991).

Segundo o código de prática de gestão da segurança da informação, a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectados. Como resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ABNT, 2005).

A informação desempenha um papel tão importante que é através dela que se toma uma decisão, tanto na definição, como também na execução de uma

estratégia. A informação e o conhecimento são os diferenciais para quem pretende se destacar no mercado e ser mais competitivo. A informação representa a inteligência competitiva dos negócios, e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa (SÊMOLA, 2003).

Portanto, a informação é o ativo mais importante de uma organização. Seu poder é tão grande que na corrida comercial, qualquer detalhe e qualquer informação sobre um concorrente pode fazer a diferença, ela se torna um fator relevante para a saúde da empresa e por isso deve ser protegida. Esse ativo pode se classificar de acordo com sua característica e importância. Essa classificação é de fundamental importância para a manutenção da informação segura, de forma que não haja influências não autorizadas sobre ela.

3.2. CLASSIFICAÇÃO DA INFORMAÇÃO

O processo de classificação da informação se caracteriza principalmente por identificar o grau de importância da informação. Com essa classificação podem ser definidos os níveis de segurança e de proteção de cada tipo de informação.

Não existe um padrão definido de classes da informação. Isso vai depender da política de segurança da empresa e com quais tipos de informações ela trabalha (SILVA & OCULATI, 2007).

As quatro classes a seguir são as mais utilizadas:

Pública: são informações que o público de maneira geral pode ter conhecimento.

Interna: são informações mais específicas que fazem parte do interesse apenas da empresa e do tipo de negócio.

Particular: trata-se de uma informação com âmbito mais pessoal. São aquelas informações que se violadas, podem trazer prejuízos a empresa e também ao próprio funcionário.

Confidencial: diz-se que se trata da informação mais valiosa de uma empresa. Apenas alguns membros devem saber e ter acesso a tal informação. São

as informações de operação da empresa, como resultados de campanhas de *marketing*[11], valores e negociações, segredos comerciais, entre outras.

Com a informação classificada de acordo com sua importância, é possível evitar cenários com informações sensíveis ou críticas sem o nível de proteção adequado, podendo causar incidentes de segurança, onde, causariam prejuízos e comprometeria a eficácia das operações ou, em contrapartida, uma informação que não necessita de proteção pode estar sendo protegida desnecessariamente consumindo recursos e orçamentos de segurança.

Após a classificação e o entendimento dos níveis de importância de cada tipo de informação, também se torna necessário compreender os caminhos e o ciclo que a informação percorrerá desde a sua criação até o seu descarte ou arquivamento.

3.3. CICLO DE VIDA DA INFORMAÇÃO

O Ciclo de vida da informação se vivencia em todo momento que um *ativo*[12] da empresa manipula a informação para que os processos sejam mantidos (Sêmola, 2003). O ciclo de vida apresenta-se em quatro fases: manipulação, armazenamento, transporte e descarte.

Manipulação: é a fase inicial do ciclo de vida, onde a informação é originada e manuseada, podendo ser no processo de escrita, digitação, folheando papéis ou até mesmo quando informamos usuário e senha para um acesso.

Armazenamento: é a continuação após o manuseio e criação, ou seja, a informação deve seguir um caminho para que a mesma seja armazenada para futuros acessos. Podemos citar gravação dos dados em alguma mídia, banco de dados, papéis guardados em gavetas ou em arquivos adequados.

---

[11] *Marketing*: conjunto de atividades que envolvem o processo de criação, planejamento e desenvolvimento de produtos ou serviços que satisfaçam as necessidades do consumidor, e de estratégias de comunicação e vendas que superem a concorrência.

[12] *Ativo:* valor, bem, crédito ou instrumento, onde seu conjunto forma o patrimônio de uma empresa. Ex.: Computadores, moveis, funcionários, capital financeiro, entre outros.

Transporte: seguindo a fase do armazenamento, a fase de transporte representa o instante em que a informação está em trânsito, podendo ser através de um e-mail, telefone, mensagem de texto, serviços postais, entre outros.

Descarte: esta é a fase final do ciclo de vida da informação, de igual importância às demais. É o destino final da informação quando ela não é mais útil, podendo ser para a lixeira, no caso de informações impressas, um arquivo deletado, entre outros.

Para garantir que a informação percorra todas as fases de modo coerente sem interferências, é que a política de segurança da informação elabora técnicas e boas práticas para que não haja influência de pessoas não autorizadas em nenhuma fase do ciclo de vida. É de suma importância que a organização tenha bem definido os processos de segurança em cada fase do ciclo, pois, em cada uma das fases são necessárias abordagens específicas de segurança.

3.4. CONCEITO DE SEGURANÇA DA INFORMAÇÃO

A informação é um ativo importante e essencial para uma organização e seus negócios, portanto, a segurança da informação nada mais é que a proteção da informação de vários tipos de ameaças, para que se possa garantir a continuidade dos negócios, minimizando os riscos e maximizando o retorno desses negócios.

A segurança da informação é consolidada com a implantação de controles, incluindo políticas de segurança, processos, procedimentos, estruturas e funções de *software*[13] e *hardware*[14]. Todos esses controles de nada adiantarão se não forem bem estabelecidos, implantados, monitorados e analisados, pois, somente desta forma poderão ser melhorados a fim de garantir os objetivos do negócio e de segurança (ABNT, 2005).

Baseando-se na norma NBR ISO/IEC 17799:2001, a segurança da informação se caracteriza quando se há a manutenção da confidencialidade,

---

[13] *Software:* é toda a parte lógica da informática, aplicativos, sistema operacional, banco de dados, entre outros.

[14] *Hardware:* é a parte física da informática, teclado, mouse, monitor, computador, entre outros.

integridade e disponibilidade da informação. Porém, na norma NBR ISO/IEC 27002:2005 se mantém os conceitos acima, sendo acrescentados outras propriedades que também podem ser envolvidas: autenticidade, responsabilidade, o não repúdio e a confiabilidade (DANTAS, 2011).

Confidencialidade: tem o objetivo de limitar o acesso às informações, permitindo o acesso apenas de pessoas autorizadas. Deve ser garantida em todas as fases do ciclo de vida da informação, desde a sua criação ou manipulação, sua passagem pelos meios de transmissão, chagando ao seu destino para serem armazenadas ou descartadas de forma correta, sendo destruídas de forma que seja impossível a sua recuperação. Nessa etapa, existe a possibilidade de utilização de processos de criptografias, controles de acessos, entre outros, para garantir a proteção da informação de modo que, quanto mais importante for a informação mais ela deve ser protegida.

Integridade: é garantir que a informação só vai ser alterada por pessoas autorizadas. É garantir que a informação não pode ser modificada em seu conteúdo por pessoas sem autoridade ou de maneira acidental, até chegar ao seu destinatário.

Disponibilidade: seu objetivo é garantir que informação sempre esteja acessível quando necessário. Pode ser conseguido com rotinas de backup bem elaboradas, redundância de serviços, controle de acesso entre outros, pois, não adianta uma informação integra e confiável se a mesma não estiver disponível quando necessário.

A segurança da informação é essencial e vital para uma organização, pois, suas normas e diretrizes, são responsáveis por classificar os riscos e estabelecer padrões de comunicação e transferência das informações geradas em suas várias formas, sejam elas impressas, escritas, armazenadas eletronicamente, enviadas por correio ou e-mail, apresentadas ou até mesmo faladas. Independente da forma que é apresentada, do meio de compartilhamento ou armazenamento, a informação deve ser protegida adequadamente conforme sua importância. Outro ponto importante para a garantia da segurança da informação é conhecer as vulnerabilidades e as ameaças em potencial, as quais o ambiente computacional está exposto. Conhecendo-as, as ferramentas podem ser utilizadas de forma correta para garantir as propriedades de um ambiente seguro.

3.5. AMEAÇAS À INFORMAÇÃO

Ameaças na segurança da informação é qualquer condição ou elemento que caso se concretize, cause um incidente de segurança, que viole a informação e seus ativos explorando vulnerabilidades, causando prejuízos no negócio.

As ameaças são qualquer causa potencial de um incidente indesejado, que possa resultar em danos aos dados de um computador (Machado, 2014).

O objetivo de uma ameaça, é sempre explorar uma vulnerabilidade do sistema computacional buscando causar um impacto negativo, que pode ser desde um roubo de informações sigilosas até um ataque de negação de serviço, ou seja, um serviço essencial deixa de estar disponível para os usuários. A intenção de uma ameaça, portanto, é sempre causar um prejuízo e afetar o negócio.

3.5.1. Ameaças fundamentais

Ameaças fundamentais são aquelas que, de uma maneira ou de outra, afetam diretamente os princípios que são defendidos pela segurança da informação. Podem ser classificadas em vazamento de informações, violação de integridade, indisponibilidade de serviços ou ainda o acesso não autorizado (Machado, 2014).

O vazamento de informações pode ocorrer de maneira involuntária quando ocorre a falha de um equipamento, quando mensagens são enviadas a um endereço incorreto, falta de esclarecimento de procedimentos que causa erros de usuários ou até mesmo por falha de programação em alguma aplicação utilizada pela empresa, ou seja, quando não se tem a intenção de disponibilizar a informação ao ambiente externo. Um vazamento voluntário normalmente ocorre quando pessoas mal-intencionadas tem o acesso às informações e de forma deliberada roubam os dados, fraudam informações adulterando dados importantes, invadem sites, ou por qualquer outro meio em que a pessoa tem a total intenção de roubar informações.

A violação de integridade consiste em modificar a consistência dos dados ou de um sistema, de maneira não autorizada voluntariamente ou involuntariamente. Pode-se considerar como violação de integridade, um acesso não autorizado ao

sistema, onde poderia ser alterado o salário de vários funcionários ou até mesmo uma modificação do site de uma organização.

Outra ameaça funcional trata-se da indisponibilidade de serviços computacionais, que consiste na paralisação de acesso ou do próprio recurso impedindo a utilização dos mesmos. Esse tipo de ameaça consiste em aumentar o número de requisições a um determinado servidor, fazendo com que seus recursos sejam utilizados por completo até ocasionar a parada dos sistemas. É muito comum ocorrer esse tipo de ataque em servidores web deixando sites indisponíveis.

O acesso não autorizado por sua vez, trata-se da utilização de recursos computacionais por pessoas não autorizadas. Ocorre, por exemplo, quando um usuário tem sua senha roubada e terceiros passam a ter acesso às informações que não poderia acessar. Essa ameaça pode se concretizar de maneira voluntária ou involuntária, pois, um usuário pode ter sua senha roubada, mas nada impede que ele seda essa informação de maneira intencional.

Percebe-se que todas as ameaças fundamentais podem ocorrer de maneira voluntária ou involuntária. Todas as ameaças também buscam o acesso e a alteração de informações e vão ao encontro das vulnerabilidades do sistema computacional e da segurança da informação.

3.5.2. Ameaças à segurança da informação

Como ameaça é a possibilidade da exploração de uma vulnerabilidade provocar um incidente, algumas ameaça merecem um destaque especial por serem comuns no ambiente computacional e causarem perdas de dados e violações de privacidade em ambientes vulneráveis. Estas ameaças se concretizam tanto em ambientes corporativos, quanto em ambientes domésticos.

3.5.2.1. Vírus

Vírus é o termo mais conhecido entre usuários de computadores. Mas o que são e como eles funcionam?

Vírus é um programa desenvolvido com o intuito de alterar a forma como o computador trabalha sem o conhecimento ou permissão do usuário (Machado,2014).

Os vírus caracterizam-se por serem auto executáveis, ou seja, não precisam de nenhuma intervenção explicita do usuário para se instalar no computador. Geralmente utilizam o caminho de outros programas para serem executados. Outra característica importante é que eles podem se duplicar e, desta forma, vão substituindo outros arquivos do computador.

As ações que um vírus pode executar são variadas. Eles podem danificar o computador corrompendo arquivos ou programas, removendo arquivos ou até mesmo formatando o disco rígido, causando a perda de todo o conteúdo do computador. Outros vírus são desenvolvidos para apenas se multiplicar, afetando o desempenho na execução de programas do computador, pois, consomem os recursos de processamento e podem causar o travamento total do computador.

Para se proteger dos vírus, um dos passos mais importantes é entender o que eles podem causar em um computador. Outro passo importante é manter sempre um software antivírus instalado e atualizado. Atualizações são importantes não apenas para o antivírus, mas também para todos os programas utilizados, pois, na maioria dos casos, os vírus se utilizam de falhas nesses programas para executar os ataques. Mesmo a falha sendo encontrada e corrigida, de nada adiantará se a nova versão não for instalada no computador.

Várias outras recomendações são importantes. Estar sempre atentos ao abrir e-mails não esperados ou de destinatários desconhecidos, acessar sites e baixar arquivos não confiáveis e principalmente conscientizar todos os usuários a terem os hábitos corretos e boas práticas na utilização dos recursos computacionais da empresa.

3.5.2.2. Hacker e Cracker

Segundo Machado (2014), hacker é uma pessoa que estuda profundamente como modificar os aspectos internos de dispositivos de tecnologia da informação, programas e redes de computadores.

Com esse conhecimento adquirido e com o treinamento e aperfeiçoamento de técnicas, um hacker é capaz de invadir uma rede ou um sistema e causar danos às empresas e pessoas. Seu conhecimento é tão amplo que em muitos casos, as barreiras criadas por especialistas em segurança são incapazes impedir os acessos não autorizados.

O conceito hacker, muitas vezes, é confundido com outro elemento que também detém do mesmo nível de conhecimento, porém suas atitudes e intenções são bem diferentes. Enquanto o hacker se preocupa em utilizar de seus conhecimentos para detectar e corrigir falhas, o cracker com seu conhecimento e nenhuma preocupação em causar prejuízos, atacam sistemas apenas para deixar a sua “marca”, roubar informações ou apenas destruí-las completamente.

Portanto, o termo cracker pode ser relacionado como o indivíduo que prática a invasão ou a quebra de sistemas de informação e segurança sem ética e de forma ilegal, causando prejuízos e perdas de informação. Já o hacker é aquele que utiliza de seus conhecimentos e técnicas para identificar vulnerabilidades e corrigi-las.

3.5.2.3. Negação de Serviço

Os ataques de negação de serviço *(DoS - Denial of Service)*, são caracterizados por fazerem com que os servidores ou computadores sejam impedidos de realizarem suas tarefas e indisponibilizar os serviços. Baseiam-se em fazer com que o servidor receba um número tão grande de requisições, que não seja capaz de atende-las e com isso podem vir a negar algum tipo de serviço.

Temos ainda o termo *DDoS (Distributed Denial of Service)*, que é uma variação do *DoS*, só que em grandes proporções, pois, utiliza vários computadores para atacar um sistema. É a forma de ataque de negação de serviço mais comentada e vista em noticiários, por se tratarem de ataques geralmente de grandes proporções.

Para esse tipo de ataque são utilizados, geralmente, *malwares*[15] que infectam computadores do mundo todo com programas de ataque *DoS*. Os

[15] *Malwares:* Software malicioso destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações

computadores infectados passam a serem controlados remotamente executando solicitações a um determinado alvo até que seus recursos sejam esgotados e o serviço esteja indisponível.

3.6. VULNERABILIDADES DA INFORMAÇÃO

Marcos Sêmola define o termo vulnerabilidade da informação como:

> Fragilidades presentes ou associadas a ativos que manipulam e/ou processam informações que, ao serem exploradas por um ataque, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade (Sêmola, 2014, p. 44).

Quando o esperado é garantir a segurança da informação em uma empresa, é importante que os processos vulneráveis sejam identificados para que sua importância seja conhecida e as medidas e controles de segurança sejam aplicadas adequadamente. Essas medidas devem estar configuradas adequadamente para não se torarem vulnerabilidades, pois, uma medida de segurança implantada de forma incorreta, torna-se um ponto de vulnerabilidade a ser explorado.

Segundo PEIXOTO (2006), as vulnerabilidades também podem ser classificadas como físicas, naturais, hardware, software, mídias, comunicação e humanas.

Físicas: são instalações físicas que não levam em consideração as normas ou boas práticas de segurança vigentes, onde podem ocorrer falta de equipamentos contra incêndio e falta de controle de acesso aos locais de armazenamento de informações.

Naturais: instalação de equipamentos eletrônicos em locais com fortes ocorrências de desastres naturais, como enchentes, terremotos, falta de energia, poeira, alta umidade e temperatura.

Hardware: computadores sofrem com o acumulo de poeira, alta temperatura e umidade além de estarem sujeitos a acessos indevidos a recursos não protegidos e ainda sofrem com a influência de componentes defeituosos ou mal configurados ou que sofrem com a falha de energia.

Software: erros de código, instalação de software inadequados que proporcionam acesso indevido, vazamento de informações, perda de informações e até mesmo indisponibilidade de recursos.

Mídias: impressos e relatórios podem ser perdidos e danificados juntamente a discos rígidos, fitas de backup entre outros, que podem se danificar com falhas elétricas, vida útil dos equipamentos, interferência eletromagnética, entre outros.

Comunicação: vulnerável às escutas telefônicas e aos problemas de infraestrutura ou de configuração de equipamentos que podem impedir o estabelecimento da comunicação.

Humanas: treinamento inadequado ou inexistente, avaliação de consulta a antecedentes, má fé ou descontentamento de funcionários, falta da execução de uma rotina de segurança já estabelecida, omissão, entre outros. São fatores que levam a um possível compartilhamento de informações confidenciais.

Vulnerabilidade da informação, portanto, trata-se dos elos fracos que possam existir em uma organização, possibilitando que um incidente ocorra. É de suma importância que todas as vulnerabilidades sejam detectadas e aplicadas a elas suas medidas de segurança adequadas. As vulnerabilidades são as mais importantes causas de incidentes de segurança e esses incidentes afetam o negócio e todos os envolvidos.

O estudo e à identificação das vulnerabilidades de uma organização se assemelha ao conceito da gestão de riscos que se trata do estudo que analisa a probabilidade da ameaça explorar vulnerabilidades, causando perdas de impactos negativos no negócio.

3.7. GESTÃO DE RISCO

A gestão de risco engloba a segurança da informação em seu processo e é fundamental para manter em perfeito funcionamento toda a instalação tecnológica de uma empresa, visto que o número de riscos comprometedores para a empresa não para de crescer. Acompanhada da segurança da informação, a gestão de risco tem um papel fundamental para a proteção da informação, reputação e da marca de uma

empresa, uma vez que, a partir de uma gestão de risco bem elaborada é possível implementar e gerir os controles que focam no objetivo e na manutenção do negócio, na eficiência das ações de prevenção e de correção, na garantia do cumprimento dos regulamentos e na definição correta da gestão da segurança da informação.

Uma das grandes vantagens da gestão de risco voltada para a segurança da informação está na prioridade das ações de acordo com as necessidades e objetivos além de ser possível a adoção de números e indicadores para os resultados (Dantas M. L., 2011).

Obter sucesso na avaliação dos riscos não livrará a organização dos prejuízos, mas ela será capaz de enumerar os riscos e ter a noção clara de quais riscos estão ocorrendo. Portanto, gestão de risco é conhecer todo o cenário da informação na empresa, conhecer todos os riscos aos quais está exposta para um planejamento antecipado das ações necessárias em eventuais ataques.

Mas o que pode ser considerado um risco? Risco em segurança da informação é tudo que cria ou aumenta o potencial de perdas e danos explorando-se as vulnerabilidades de recursos ou processos.

Para se analisar um risco, algumas etapas devem ser consideradas:

- Identificação de recursos críticos que são essenciais para a sobrevivência da empresa podem ser valorizados pela facilidade de substituição ou pelo custo, quando há necessidade de substituição;
- Identificar as vulnerabilidades a ameaças dos recursos críticos, bem como a probabilidade de ocorrência de perdas e os impactos que causariam;
- Determinar as perdas e danos de maneira realista que estão associados à realidade da ameaça de um recurso de modo a gerar o nível do risco ao qual este recurso está exposto;
- Classificar o nível do risco quanto à sua aceitação ou necessidade de reduzir as consequências de acordo com o grau esperados pela organização.

A Figura 9 apresenta as etapas a serem seguidas para se fazer a análise de risco em uma organização.

Figura 9 - Etapas para Análise de Riscos
Fonte: (http://www.optrasecurity.com.br/site/file/2015/08/grmmetaframework.png)

Após o processo de identificação de recursos críticos, das vulnerabilidades, das possíveis perdas referentes a cada recurso e da classificação do risco, a organização pode decidir as suas ações perante cada tipo de risco, podendo até mesmo aceitar um nível de risco existente que não afete as atividades do negócio.

Outros dois pontos importantes que devem ser levados em consideração é a origem e como os riscos podem ser classificados. Isso facilitaria a compreensão e a tomada de decisões. Os riscos podem se originarem de um evento da natureza, de um problema técnico ou até mesmo de ação proposital de um funcionário ou de uma pessoa terceira.

As classificações dos riscos podem se categorizar com base na origem das ameaças e vulnerabilidades. Dessa forma, eles podem ser naturais, involuntários e intencionais.

Os riscos naturais são aqueles que surgem de fenômenos da natureza, como terremotos, alagamentos, furacões entre outros; os riscos involuntários surgem

de ações que não são intencionais, que estão relacionados a vulnerabilidades humanas, físicas, dos meios computacionais e de comunicação, como um funcionário sem treinamento ou conhecimento que realiza uma tarefa errada e causa um incidente, um sistema não responde entre outros; já os intencionais são aqueles resultantes de ações humanas, que são realizados intencionalmente visando prejudicar e causar danos.

Após a classificação, é possível verificar e detectar os fatores que venham a motivar os riscos. Desta forma é importante que medidas sejam adotadas em cada categoria para que os eventuais riscos não ocorram. Na sequência, são apresentados alguns fatores importantes na prevenção dos riscos:

- Ter conhecimento se a região onde a empresa está instalada é susceptível a eventos da natureza como ventos, chuvas, descargas elétricas, alagamentos entre outros;
- Equipamentos de prevenção de sinistros instalados e inspecionados;
- Ter um plano eficiente de recuperação de dados em caso de desastres, para garantir a continuidade do negócio;
- Treinamento para as ações de contingência;
- Material de qualidade na construção;
- Ter equipamentos de prevenção, detecção e de controles internos;
- Ter controle do acesso físico e do acesso às informações da empresa.

Gestão de risco, portanto, é o processo de identificação e análise dos impactos que a exploração de cada vulnerabilidade encontrada no negócio pode causar, com o intuito de gerenciar, aplicar e melhorar as prevenções necessárias em cada segmento da empresa, controlando o risco desde sua origem até o tratamento dos prejuízos causados.

Após os processos de gestão de riscos, após as vulnerabilidades serem identificadas e as ameaças detectadas, pode-se ter uma base dos aspectos que a segurança e a política de segurança da informação devem abordar e proteger na organização.

4. MODELO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Política de segurança da informação é um conjunto de normas, procedimentos e diretrizes que visam a proteção, tanto da organização quanto dos empregados, do ambiente computacional. Seu objetivo principal é garantir a correta utilização, gerenciamento e proteção do principal patrimônio da empresa, a informação.

Uma política de segurança da informação visa prover orientação e apoio à direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes (ABNT NBR ISSO/IEC 17799:2005).

Sêmola (2014), chega a comparar, guardando as devidas proporções, a importância da política de segurança da informação com a Constituição Federal de um país, visto que fornece orientação e apoio para as ações de segurança e seu papel e comprimento é fundamental na manutenção de um cenário seguro.

Sua função é estabelecer responsabilidades, critérios e padrões durante o ciclo de vida da informação, assegurando o nível de segurança estabelecido pela organização. Para que isso ocorra é importante que suas diretrizes sejam claras e expresse a estratégia e a importância da informação para a empresa e, além de tudo, mantenha os funcionários cientes desse valor, de forma que se comprometam na implantação da segurança na cultura organizacional de trabalho.

> O conjunto da política de segurança da informação e dos demais regulamentos deve ter uma arquitetura que facilite a estruturação desses regulamentos. Não existe uma estrutura rígida de separação dos tipos de orientações (Fontes, 2012, p. 94).

O autor define que não existe um padrão de arquitetura para estruturação da política de segurança da informação, mas recomenda os seguintes níveis para as regras estabelecidas pelos regulamentos:

Política: nesse nível apresenta-se as diretrizes que devem ser seguidas. Essas diretrizes são as orientações básicas que apresentam o que se quer com a política. Ela não define como ser implantada e nem como deve ser feita, apenas apresenta a intenção do que se quer proteger.

Norma: apresenta regras básicas da implantação do controle definido pela política da organização ou por algum regulamento que deve estar em conformidade. Este documento caracteriza-se por além de ter as definições presentes no nível anterior, também explica como atender os controles.

Procedimento: neste nível encontramos as atividades detalhadas de como deve ser implantado o controle. Caracteriza-se por detalhar como as atividades devem ser executadas.

Fontes (2012), cita o exemplo da autenticação de usuários. A política declara que todo usuário deverá se identificar e autenticar de forma individual. A norma indica como será feita a autenticação do usuário, se vai ser utilizado a biometria ou uma senha. Quando for utilizado a senha a norma define que ela dever ser secreta e deve ser criada de forma a evitar senhas frágeis que podem ser quebradas com facilidade. O procedimento define a regra de criação da senha, que pode seguir um padrão diferente para cada ambiente da organização.

Portanto, cada nível apresenta suas características e facilita o entendimento por parte do gestor de segurança da informação, pois, mantém documentados todo o escopo do que se quer proteger e quais medidas tomar para execução das atividades computacionais de uma organização.

4.1. TIPOS DE POLÍTICAS DE SEGURANÇA

Assim como o documento e a arquitetura de uma política de segurança da informação, também é importante o entendimento dos tipos de políticas de segurança que podem ser implementados. Existem três tipos de políticas: regulatória, consultiva e informativa.

4.1.1. Política Regulatória

Ferreira (2003), afirma que políticas regulatórias são implementadas devido às necessidades legais impostas a uma empresa. Normalmente são específicas para um tipo de atividade.

Política regulatória se define por uma série de especificações legais. É descrito com detalhes tudo que se deve fazer, quem deve fazer ou fornecer um parecer relatando qual ação é importante. Deve-se assegurar que a organização esteja seguindo os procedimentos e normas apresentadas ao seu ramo de atividade provendo conforto e segurança em suas execuções.

4.1.2. Política Consultiva

A política consultiva sugere quais ações e métodos devem ser adotados nas realizações de tarefas. O objetivo é esclarecer as atividades cotidianas da organização de forma direta. Não são obrigatórias, mas recomentadas.

É importante que os usuários conheçam essas ações para a realização de tarefas e que possam ser evitados riscos pelo não cumprimento das mesmas, tais como:

- Haver a omissão de informações cruciais na tomada de decisão crítica aos negócios;
- Falha de comunicação com a alta administração;
- Compromissos e prazos importantes perdidos.

Contudo, se torna importante e indispensável que a organização torne essa política obrigatória e os usuários se conscientizem para que os riscos não possam causar prejuízos e perdas ao negócio. Devem ser consultadas sempre que houver dúvidas sobre a atividade que será executada.

4.1.3. Política Informativa

Como a denominação diz, tem caráter informativo e nenhuma ação é desejada e riscos não existem com o seu não cumprimento. Pode conter diversas observações importantes e também advertências pelo não cumprimento.

Se a política descrever que apenas um usuário pode acessar um sistema, em caso de qualquer outro usuário violar o acesso, este será penalizado. Na política

não são informados os usuários que podem acessar o sistema, mas é determinado as punições para que as descumprir.

4.2. UM MODELO ESTRUTURAL DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Para facilitar o entendimento da política de segurança, é de fundamental importância que seu conteúdo seja claro e organizado. Fontes (2012), apresenta uma estrutura de documento que facilita esse processo, onde o desenvolvimento da política é dividido em blocos de informações. A Figura 10 exemplifica os blocos a serem utilizados.

Figura 10 - Estrutura de um modelo de política de segurança
Fonte: (Fontes, 2012)

No primeiro bloco é detalhado o objetivo do documento, do que se trata e o que a empresa quer repassar com o documento. Quando se iniciar a leitura deve estar claro ao usuário o assunto e o detalhamento. No documento não deve ser apresentado uma aula sobre segurança da informação, o objetivo é deixar os usuários cientes de como a organização deseja que suas informações sejam tratadas, as proibições, as permissões e o que se deseja ser feito. O assunto segurança da

informação pode ser tratado com mais detalhe nos treinamentos e em cartilhas educativas fornecidas aos usuários.

No escopo do documento, segundo bloco, são definidos os limites de aplicação do documento, ou seja, os ambientes físicos, lógicos, tipos de usuários, validade do documento, entre outros. Define os ambientes e às pessoas as quais se aplicarão as regras.

No terceiro bloco é descrito as definições ou glossário. Nesta parte do documento deverão ser apresentados os termos mais específicos, como abreviaturas, termos técnicos, siglas e palavras não comuns para o usuário.

No bloco seguinte são apresentadas as regras, ou seja, tudo que a organização quer que seja cumprido pelos usuários. Portanto, este bloco torna-se essencial no documento. Ela indicará aos usuários tudo o que deve ser feito, que é obrigatório, o que não fazer e os princípios a se seguir. As regras devem ser bem explicadas para que não fiquem dúvidas para o usuário, visto que, um mal entendimento de uma regra pode se tornar um ponto de vulnerabilidade.

No bloco cinco são descritas as responsabilidades referentes ao documento. Devem ser indicados os responsáveis por manter o texto do regulamento, o responsável pelo treinamento dos usuários, pela divulgação perante os usuários e qualquer outra ação necessária para manter em bom funcionamento e fazer ser cumprido as regras do documento.

No último bloco são definidas as penalidades pelo não cumprimento. Trata-se das penalidades caso alguma regra não seja cumprida por algum usuário. Deve conter o que é inaceitável pela organização, além de abranger como o usuário deve se comportar em caso de dúvidas, erros ou alguma outra situação que não esteja no documento.

Levando em consideração a divisão em blocos, será apresentado um modelo de política de segurança da informação que pode ser aplicado em uma organização de pequeno porte, onde será definido uma política de acesso às informações, buscando garantir a segurança em seus aspectos principais: Confidencialidade, Integridade e Disponibilidade.

4.3. POLÍTICA DE USO E ACESSO À REDE CORPORATIVO E À INTERNET

Uma das influências na realização deste trabalho foi a dificuldade que uma empresa encontra no processo de escrita e de implantação de uma política de segurança da informação. Serão propostas as regras básicas de uma política e como podem ser feitos os controles para auxiliar no cumprimento dessas regras. O cenário utilizado na criação desta política será como o apresentado na Figura 11.

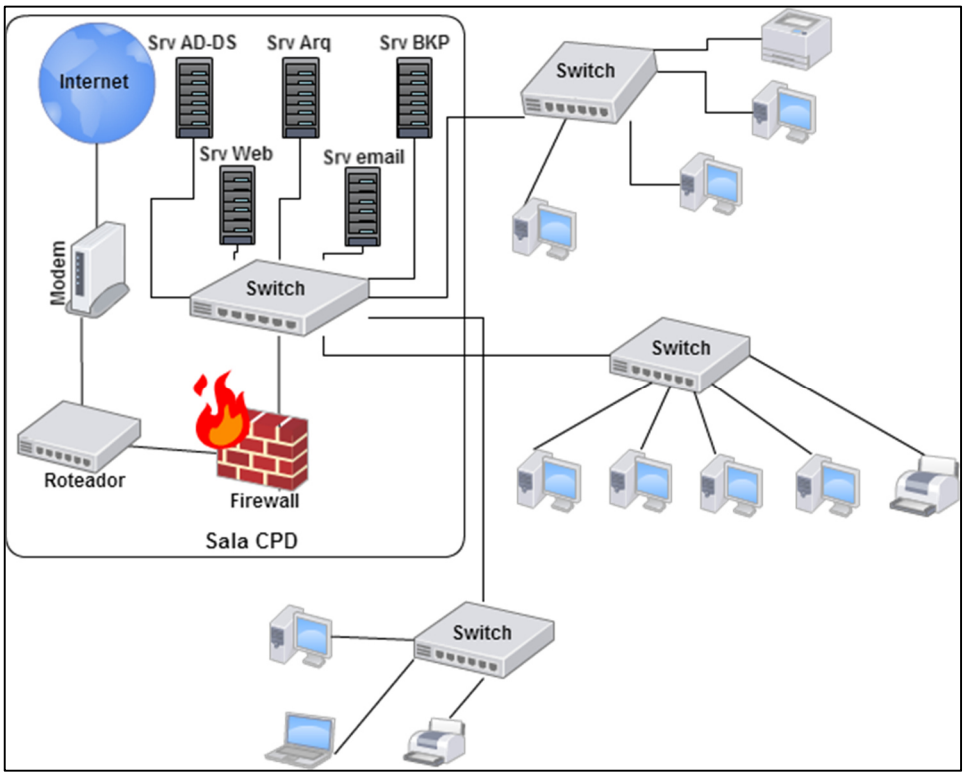

Figura 11: Exemplo de rede em uma organização

O modelo da Figura 11 apresenta a estrutura de uma rede em uma organização. Basicamente, este é o cenário mais comum e que mais se enquadra na necessidade de uma política de segurança da informação.

A direção da empresa deve participar da elaboração e estar de acordo com todas as regras contida na política de segurança, estabelecer a responsabilidade de atualizações e publicações a um departamento e, dentro deste departamento, nomear o responsável por monitorar os logs do sistema e coordenar as ações para o cumprimento da política. Geralmente este trabalho é designado ao gerente de TI.

4.3.1. Objetivo

A política de segurança tem por objetivo estabelecer regras para o correto uso das tecnologias da informação disponíveis aos funcionários e pessoas externas, previamente autorizadas, e garantir a segurança da informação que é de propriedade da empresa.

4.3.2. Definições

USUÁRIO: é o colaborador que tem autorização para utilizar a informação da empresa através da Internet ou da rede corporativa da empresa.

COLABORADOR: é a pessoa que foi contratada como colaborador ou estagiário da empresa, que presta serviço ou que trabalha com algum vínculo de contrato para a empresa.

ACESSO A INTERNET: inclui o acesso à web sites, o envio e recebimento de e-mails, transmissão e recebimento de arquivos e a execução de aplicativos de Internet através de computadores da rede corporativa.

ACESSO A REDE LOCAL: inclui o acesso para manipulação de Informações armazenadas em rede com suas devidas permissões.

EQUIPE DE TI: equipe responsável pela manutenção, liberação, bloqueio e demais atividades que sejam necessárias na utilização dos serviços de tecnologia disponibilizados pela empresa.

GERENTE DE TI: funcionário responsável pelas ações referentes à política de segurança da informação e responsável por gerenciar e monitorar os recursos utilizados para o bom funcionamento da rede.

4.3.3. Escopo e Abrangência

A política de segurança abrange todos os funcionários que tenham ou venham a obter acesso às informações da empresa através da Internet ou da rede corporativa da empresa. Os fornecedores e prestadores de serviços também deverão estar cientes das regras impostas pela política de segurança da empresa.

4.3.4. Acesso à Internet

O acesso à Internet concedido pela empresa aos seus funcionários tem como objetivo auxiliar na realização das atividades diárias da empresa para se obter vantagens na competitividade do negócio, sendo que, os acessos serão controlados pelo nível de acordo com as necessidades de cada departamento.

A política de segurança estabelece a necessidade de monitorar os tipos de acessos ou a quantidade de acessos negados, para identificar possíveis tentativas de burlar a autenticação ou permissão dos usuários.

O controle de acesso à Internet pode ser realizado por meio de um servidor de firewall proxy, que interliga a rede interna da empresa com a Internet. Os pacotes oriundos da Internet são filtrados através de regras pré-definidas, e o pacote poder ser liberado, ou descartados. Outra função do servidor é, utilizando-se do firewall definir quais portas de acesso estarão disponíveis para programas dos usuários.

Associado as funcionalidades do firewall, o proxy pode trabalhar como um “cache”. Ele armazena as páginas requisitadas recentemente para repassa-las a uma nova requisição de usuário sem uma nova requisição ao servidor do site. O proxy evita conexões diretas entre o usuário e os servidores na Internet. A conexão é interceptada pelo proxy que é o responsável por fazer a requisição ao servidor do site, porém, armazena o endereço da máquina interna que fez a solicitação. A autenticação dos usuários, pode ser feita através do servidor *Active Directory - Domain Server (AD-DS)*, através de autenticação transparente, de forma a liberar os acessos de acordo com os seus grupos.

4.3.5. Atividades proibidas no uso da Internet

Realizar qualquer tipo de negócio privado para obtenção de lucros ou ganhos pessoais.

Realizar qualquer atividade ilegal, como jogos de azar e acessos não autorizados a sites.

Interferir de maneira intencional no funcionamento de equipamentos de rede da empresa ou interferir no funcionamento de sites da Internet.

Acessar conteúdo sem referência com os negócios da empresa, como sites de rádios, sites de imagens, áudio ou programas gratuitos.

Envolver-se em atividades que interfiram na política de segurança de outras empresas.

Revelar informações confidenciais ou de propriedade da empresa para pessoas não autorizadas, através de qualquer meio.

4.3.6. Acesso à rede

Para acessar a rede da empresa será disponibilizado ao usuário *login*[16] e senha exclusivos, que serão solicitados pelo supervisor do departamento junto a equipe de TI da empresa. Ao efetuar *login*, o usuário já estará apto a acessar a Internet, em seu respectivo nível de acesso, e também as pastas de seu departamento, e/ou de outro departamento caso disponibilizado, através da rede corporativa da empresa.

As regras de segurança serão controladas pelo servidor de *AD-DS*, que será o responsável pelo controle das políticas de acesso às pastas dos departamentos, as contas de usuários, grupos e gerenciar os computadores do domínio. Com a utilização do *AD-DS*, os recursos da rede só serão liberados perante autenticação do usuário. As liberações serão feitas na criação do usuário, onde serão definidos quais grupos ele fara parte. Cada departamento terá seu grupo específico e as pastas serão compartilhadas respeitando a relação grupo/departamento. As liberações de acesso à Internet, também, serão feitas através dos grupos. Os grupos serão criados com níveis de acessos, onde, cada nível terá as suas liberações. O nível “0” terá o total bloqueio de acesso à Internet; O nível “1” terá acesso aos sites bancários e sites governamentais; O nível “2” não terá acesso as redes sociais e nem permissão para downloads; O nível “3” possuirá acesso liberado aos sites, mas não pode fazer downloads; O nível “4” terá acesso liberado sem nenhuma restrição.

[16] *Login:* entrar, logar-se, acessar uma conta.

Ao efetuar *login* no computador, o usuário terá mapeado automaticamente à pasta de seu departamento, através de um script localizado na pasta *SYSVOL*[17]do servidor de *AD-DS* que será executado quando a autenticação for feita, conforme apresentado na Figura 12.

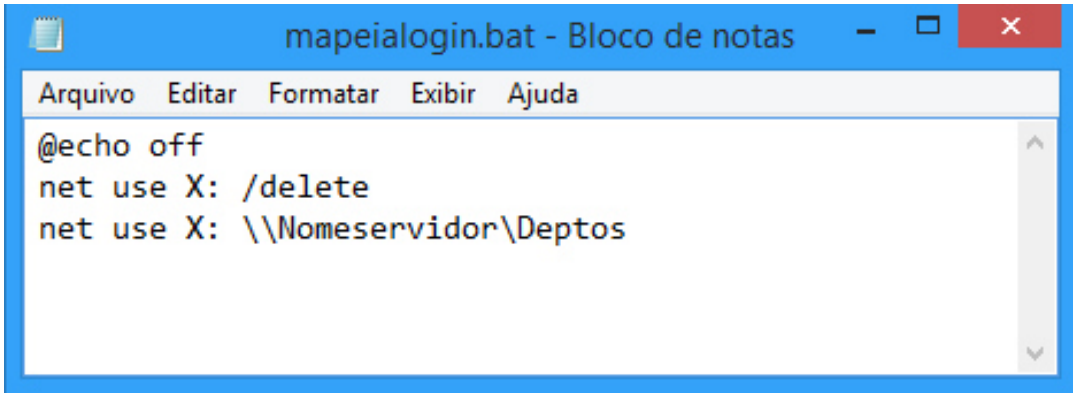

Figura 12 - Script para Mapeamento da Pasta do Departamento

A Figura 12 mostra como pode ser configurado o mapeamento da pasta Deptos atribuindo a ela a letra de unidade X:, que estará disponível no menu “Meu Computador” do usuário.

4.3.7. Política de senhas

A política de segurança deve definir regras para criação de senhas. As senhas utilizadas terão validade de 45 dias e devem conter, ao menos, seis caracteres, incluindo letras e números, respeitando as diretivas de senhas do servidor de *AD-DS*. É de responsabilidade do usuário cuidar de sua senha, não divulgando a terceiros.

Na diretiva de senhas do *AD-DS* é possível delimitar várias regras para a utilização de senhas. A complexidade da senha determina os requisitos mínimos para aceite da senha. Alguns requisitos de são:

1. Não conter partes significativas do nome da conta do usuário ou o nome todo;

[17] *Sysvol:* é um diretório compartilhado que armazena a cópia do servidor de arquivos de domínio público que deve ser compartilhado para acesso à replicação em todo o domínio comum.

2. Ter pelo menos seis caracteres de comprimento;
3. Conter caracteres de três das quatro categorias a seguir:
    - Caracteres maiúsculos do inglês (A-Z);
    - Caracteres minúsculos do inglês (a-z);
    - 10 dígitos básicos (0-9);
    - Caracteres não-alfabéticos (por exemplo, !, $, #, %).

Também é possível definir um bloqueio por tempo determinado quando a senha é digitada por várias vezes de forma incorreta. Isso impede que outros usuários garimpem senhas uns dos outros para obterem acesso não autorizado. O período em que senha será válida é definido nesta política de senha do *AD*. No caso em questão, ela será válida por 45 dias e antes de terminar esse período ela deverá ser trocada, respeitando as regras de senhas utilizadas anteriormente, que pode ser definida alterando a política de senha do domínio. Por padrão o *AD* define que não sejam utilizadas as últimas 24 senhas anteriores.

4.3.8. Política de uso de computadores

Os computadores são de propriedade da empresa e é responsabilidade do usuário cuidar e zelar dos equipamentos que utiliza, sendo proibida a instalação de software, salvo os autorizados e solicitados pelo supervisor da TI. O uso de periféricos é controlado de acordo com solicitação do supervisor do departamento, onde, os drivers de mídias serão desligados e as portas *USBs* desativadas. O bloqueio de acesso às portas *USBs*, será feito com a utilização de scripts, que serão adicionados ao perfil do usuário no servidor de *AD*.

Um arquivo com o nome bloqueiaUSB.reg pode ser criado e armazenado na pasta *sysvol*, juntamente ao arquivo bloqueioUSB.cmd, que é o responsável por executar a chamada do arquivo bloqueiaUSB.reg, para bloqueio das portas *USBs* pelo registro do sistema operacional, conforme ilustrado na Figura 13.

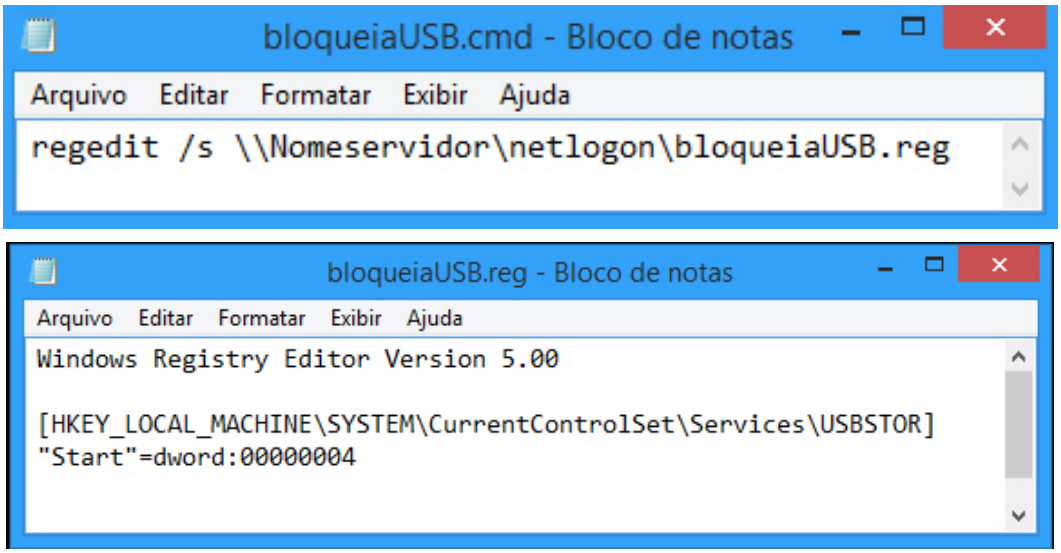

Figura 13 - Script para bloqueio e desbloqueio de portas USBs

Na Figuras 13 temos os arquivos de scripts que bloqueiam o acesso às portas *USBs*. O arquivo bloqueiaUSB.reg faz referência ao registro do sistema operacional que inicializa as *USBs*. Quando o registro corresponde a "Start"=dword:00000004, as portas estarão bloqueadas. Para desbloquear é preciso carregar um script idêntico, apenas alterando para o valor "Start"=dword:00000003.

Todos os equipamentos devem ser desligados ao finalizar as tarefas diárias e, em hipótese nenhuma, o usuário está autorizado a desmontar ou realizar qualquer tipo de reparo nos equipamentos de informática. Qualquer problema apresentado deve se comunicado imediatamente à equipe de TI.

4.3.9. Utilização de e-mail

O e-mail é criado a partir de solicitação feita pelo supervisor do departamento junto à equipe de TI da empresa. Os e-mails devem ser utilizados exclusivamente para assuntos da empresa. Os e-mails serão verificados à procura de vírus e os e-mails suspeitos serão bloqueados e encaminhados à quarentena onde serão liberados após avaliação da equipe de TI. E-mail que contenham anexos com extensões .exe, .pif, .com, .zip, .bat não serão permitidos.

Para a obtenção da segurança na troca de e-mail é usada uma ferramenta que funcionará como um proxy de e-mail. Ela desviará todo o tráfego de e-mail

verificando a presença de vírus e spam. Os e-mails que não satisfazerem as regras de segurança serão destinados ao repositório de spam, onde poderão ser avaliados e, se possível, liberados pela equipe de TI aos destinatários. Os e-mails que não caírem neste repositório serão recebidos normalmente.

4.3.10. Acesso físico

A política deve apresentar regras para acesso físico aos equipamentos do datacenter. O Livre acesso físico ao datacenter só será permitido para a equipe de TI da empresa. Em caso de acesso de pessoas de outros departamentos ou de prestadores de serviço, os mesmos devem ser acompanhados por um funcionário da equipe de TI.

Para garantia de acesso apenas de pessoas autorizadas, podem ser utilizados equipamentos que exijam a autenticação para liberação. A autenticação pode ser feita por uma senha, por biometria, cartão de identificação, entre outros. É importante que esses acessos sejam registrados para possíveis auditorias.

4.3.11. Política de backup

Os backups serão realizados diariamente por sistemas automatizados. Serão executados em horários não comerciais, que o fluxo de informações transitando nos servidores é menor. A gestão de backup será de responsabilidade da equipe de TI e os dados serão salvos em discos rígidos específicos para esta finalidade.

4.3.12. Responsabilidades

A equipe de TI, junto a administração geral da empresa, são os responsáveis por manter este documento atualizado, bem como divulgado entre os usuários da empresa. O processo de treinamento para os usuários, se necessário, será de inteira responsabilidade da equipe de TI.

4.3.13. Cumprimentos das Normas

Usuário que, comprovadamente, violar a política de segurança estará sujeito, dependendo da gravidade da violação, à:

- Ter seu acesso à Internet restringido ou até mesmo cancelado;
- Arcar com despesas de equipamentos danificados por mau uso ou utilização indevida;
- Ter rescindido o contrato de trabalho ou de prestação de serviço;
- Responder a processo criminal.

4.4. FERRAMENTAS E TÉCNICAS PARA A PROTEÇÃO DA INFORMAÇÃO

4.4.1. Antivírus

Antivírus são programas que tem por objetivo procurar, detectar e excluir as ameaças. Com o crescimento das ameaças, as empresas de antivírus estão cada vez mais agregando funções aos programas. Eles são capazes de remover cavalos de Tróia, códigos maliciosos, verificar e-mails além da proteção de navegação na Internet e módulos de proteção de acesso à rede bancária.

Para que um antivírus seja considerado satisfatório, deve encontrar a maior quantidade de vírus possíveis, analisar os arquivos que estão sendo recebidos pelas Internet, monitorar os discos rígidos constantemente, monitorar os arquivos recebidos por e-mail de forma a excluir os infectados e, principalmente, ter uma assinatura de vírus eficientes e que seja atualizada diariamente.

Porém, não é possível se resguardar de outras ferramentas e de buscar informações sobre o assunto, pois, em alguns casos o antivírus sozinho não será capaz de impedir as ameaças e, a prevenção, se torna a principal ferramenta para impedir que os vírus contaminem computadores.

4.4.2. Criptografia de dados

Criptografia é um conjunto de técnicas que visa embaralhar, cifrar, codificar ou até mesmo modificar uma mensagem de forma a deixá-la incompreensível àqueles que não tem acesso as convenções combinadas ou não conhecem seus caracteres ou códigos. Dessa forma, a informação só poderá ser interpretada ou conhecida por seu destinatário detentor da “chave secreta”, tornando-a difícil de ser lida por alguém não autorizado.

Nos dias atuais, criptografar uma mensagem corresponde à utilização de um ou mais algoritmos para codificar ou decodificar uma mensagem ou texto. Neste processo é comum a utilização de uma chave pública para codificar e uma chave privada para decodificar.

Chave criptográfica é um parâmetro secreto utilizado por algoritmos para embaralhar ou codificar uma mensagem tornando-a compreensível apenas ao destinatário o qual tem a chave para decodificar.

Os objetivos principais da criptografia são garantir:

- **Confidencialidade:** apenas o destinatário portador da chave criptográfica poderá decodificar e ler a mensagem;
- **Integridade:** determinar se a mensagem foi alterada durante a transmissão;
- **Autenticação:** identificar o remetente e verificar se foi ele quem enviou a mensagem;
- **Não-repúdio ou irretratabilidade:** impossibilitar o emissor de negar a autoria da mensagem.

Uma utilização de criptografia é a assinatura digital que gera um código através de uma chave privada, onde a pessoa ou entidade receptora possa identificar e confirmar a integridade do documento.

4.4.3. Firewall

O firewall tem a função de isolar o acesso entre a rede interna e a externa, permitindo que sejam recebidos somente os pacotes que estejam configurados em sua lista de permissões. É a ferramenta de segurança mais importante em uma rede podendo ser utilizada tanto em ambientes domiciliares ou empresariais, protegendo a integridade e a confidencialidade das informações. Pode ser encontrado na forma de software ou na forma de hardware.

Os firewalls baseados em softwares são aplicações integradas ao sistema operacional, ou instaladas em computadores específicos para a ferramenta, garantindo a segurança desde o primeiro momento em que ele é carregado. Trabalham usando regras preestabelecidas para a análise dos pacotes de dados, se estiverem dentro das regras são aprovados, senão, são impedidos de chegarem a seu destino. Outro ponto importante é a utilização de filtros por portas de aplicativos. Esses filtros determinam exatamente os programas que podem ter acesso à Internet. As portas de comunicação também podem ser controladas de forma a bloquear as portas mais utilizadas por ameaças.

Os firewalls baseados em hardwares são equipamentos específicos e mais utilizados em ambientes empresariais. Sua vantagem é utilizar um hardware dedicado que não compartilha recursos com outros aplicativos, fazendo com que posa tratar as requisições e aplicar os filtros mais rapidamente.

4.4.4. Sistema de detecção de intrusos (IDS)

IDS (Intrusion Detection Systems) é um Sistema de Detecção de Intrusões. O mesmo possibilita identificar, através de análise dos dados, as tentativas de ataques e invasões, sejam elas concretizadas ou não. Normalmente, esse sistema trabalha no modo passivo apenas analisando os dados, em sua forma *Inline*[18] também conhecida por *IPS* (*Intrusion Prevention System*). É possível realizar a detecção de invasões em

[18] *Inline:* avaliação de desempenho do processo produtivo ao englobar procedimentos de gestão tática e operacional.

tempo real ajudando na prevenção de ataques mais complexos ou ataques em massa, além de possibilitar uma análise e correção das vulnerabilidades.

Em outras palavras, o *IDS* utiliza-se de um sistema de configurações e regras com a finalidade de gerar alertas toda vez que for detectado pacotes que se enquadre dentro dos parâmetros de um possível ataque, seja ele detectado através da comparação de assinaturas de ataques ou anomalias conhecidas. Uma vez implementado corretamente poderá evitar danos às informações, causadas por ataques à rede ou ao computador.

Em um ambiente corporativo, essa ferramenta é importante por alertar o administrador da rede sobre qualquer anomalia referente a tráfegos e requisições suspeitos. Com essas informações, as medidas de prevenção poderão ser tomadas de forma ágil e com mais eficiência.

5. CONSIDERAÇÕES FINAIS

Um ambiente de rede onde a informação é disponibilizada e transportada, exige que cuidados sejam tomados para garantir o completo ciclo de vida da informação na organização. A informação, por tratar-se do maior patrimônio de uma empresa, deve ser atendida por uma política de segurança bem elaborada, onde todos os funcionários sejam envolvidos para garantir que todas as áreas da empresa sejam atendidas e que eles estejam sempre atualizados sobre a importância de segui-las, pois, muitos incidentes podem ser causados por descuido e vulnerabilidades.

Independentemente do tipo de organização em que se trabalhe, seja um hospital, um banco, uma universidade, a busca por clientes estará sempre presente. A Maioria das organizações está ciente de que a qualidade é importante. Fica evidente que todo o processo de implantação de uma política de segurança da informação precisa ser baseado em análise. Por esse motivo, se torna indispensável levantar as informações, conhecer as vulnerabilidades da informação, as ameaças e gerir os riscos.

As ameaças à informação serão constantes e cada vez mais presentes. Para evitar que a política de segurança se torne obsoleta, é necessário que ela esteja sempre atualizada. A administração geral deve estar sempre ciente de tudo que está sendo abordado na política e garantir, junto com os responsáveis, que as punições estejam de acordo com a legislação vigente, para que possíveis punições não se tornem problemas ainda maiores para o empregador.

Este trabalho apresenta, uma proposta e um modelo de implantação e gestão de segurança da informação, visando garantir os princípios de confidencialidade, integridade e disponibilidade da informação nas organizações. A política de segurança apresentada contém os detalhes dos objetivos do documento, do que ele trata e o que a empresa quer repassar. Detalha o escopo, que trata dos limites de aplicação do documento. Estabelece uma descrição de termos utilizados no decorrer do documento para garantir o entendimento de todos os envolvidos. Posteriormente, encontram-se as regras que é tudo aquilo que a organização quer que seja cumprido pelos usuários. E, finalizando, são descritas as responsabilidades,

e estabelece as punições ou ações que serão tomadas caso as regras sejam descumpridas.

5.1. TRABALHOS FUTUROS

Propomos para trabalhos futuros, uma implantação completa da política de segurança da informação apresentada neste trabalho, utilizando ferramentas e aplicando conceitos da segurança da informação de forma prática, onde logs do sistema possam ser verificados para auxiliarem nas tomadas de decisões de formas eficazes e adequadas.

REFERÊNCIAS

ALECRIM, E. **Ataques DoS (Denial of Service) e DDoS (Distributed DoS)**. Disponível em: <http://www.infowester.com/ddos.php>. Acesso em: 10 jan. 2016.

ALENCAR, M. A. **Fundamentos de Redes de Computadores**. Manaus: CETAM, 2010.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Tecnologia da Informação:** Código de Prática para Gestão da Segurança da Informação: NBR ISO/IEC 17799:2001. Rio de Janeiro: ABNT,2005.

COSTA, J. **Apostila de Redes de Computadores**. São Paulo, SP. Disponivel em: <http://www.jeffersoncosta.com.br/redes.pdf> Acesso em: 15 nov. 2015.

DANTAS, M. **Tecnologias de Redes de Comunicaçao e Computadores.** Rio de Janeiro: AXCEL BOOKS, 2002.

DANTAS, M. L. **Segurança da informação:** uma abordagem focada em gestão de riscos. Olinda, LIVRO RÁPIDO, 2011.

FERREIRA, F. N. **Segurança da Informação.** Rio de Janeiro: CIÊNCIA MODERNA, 2003.

FONTES, E. **Políticas e Normas para a Segurança da Informação:** Como desenvolver, implementar e manter regulamentos para a proteção da informação nas organizações. São Paulo: BRASPORT, 2012.

MACHADO, F. N. **Segurança da Informação:** Princípios e controle de ameaças. 1. ed. São Paulo: ÉRICA, 2014.

NIEDERAUER, J. **Guerra Fria.** Disponível em: <http://www.sohistoria.com.br/ef2/guerrafria/>. Acesso em: 22 de out. 2015.

PEIXOTO, M. C. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: BRASPORT, 2006.

SÊMOLA, M. **Gestão de Segurança da Informação:** Uma visão executiva. 2. ed. Rio de Janeiro: ELSEVIER, 2014.

SILVA, G.F; OCULATI, T.R. **A Informação:** O maior patrimônio de uma organização. Artigo Faculdade de Informática de Presidente Prudente, Universidade do Oeste Paulista, 2007 11p.

SIMON, I. **A ARPANET.** Disponível em: <https://www.ime.usp.br/~is/abc/abc/node20.html>. Acesso em: 22 set. 2015.

SOUSA, A. R. **Redes de Computadores:** Tipos de classificação das redes de acordo com sua topologias. Disponivel em: <http://www.lanwan.com.br/Aulas_Senac/Tecnico_Redes_Noturno/Aula%2010052010%20-%20Topologias%20de%20rede.pdf>

TANENBAUM, A. S. **Redes de Computadores.** 4. ed. Rio de Janeiro: CAMPOS, 2003.

TORRES, G. **Redes de Computadores.** 2.ed. NOVA TERRA, 2014.

ULBRICH, H. C.; VALLE, J. D. **universidade H4CK3R.** 4. ed. DIGERATI BOOKS, s.d.

WADLOW, T. A. **Segurança de Redes - Projeto de Gerenciamento de Redes Seguras.** CAMPUS, s.d.