JOÃO LUCAS LAUBSTEIN BRANDÃO

A SEGURANÇA DA INFORMAÇÃO EM REDES DE COMPUTADORES

Rio Claro
2018

JOÃO LUCAS LAUBSTEIN BRANDÃO

A SEGURANÇA DA INFORMAÇÃO EM REDES DE COMPUTADORES

Trabalho de Conclusão de Curso apresentado à Instituição Anhanguera Educacional LTDA, como requisito parcial para a obtenção do título de graduado em Ciência da Computação.

Orientador: Jessica Lopes

Rio Claro
2018

JOÃO LUCAS LAUBSTEIN BRANDÃO

A SEGURANÇA DA INFORMAÇÃO EM REDES DE COMPUTADORES

Trabalho de Conclusão de Curso apresentado à Instituição Anhanguera Educacional LTDA, como requisito parcial para a obtenção do título de graduado em Ciência da Computação.

BANCA EXAMINADORA

Prof. LEANDRO JOSE DA SILVA DE PAIVA

Prof. THIAGO GIROTO MILANI

Rio Claro, 11 de dezembro de 2018

BRANDÃO, João Lucas Laubstein. **A Segurança da Informação em Redes de Computadores**. 2018. 31 p. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Anhanguera Educacional LTDA, Rio Claro, 2018.

RESUMO

A informação é um bem extremamente valioso e que sempre foi motivo de cobiça, não apenas para quem deseja crescer com ela de forma estratégica como principalmente para entidades maliciosas que almejam a quebra de seu sigilo para seu próprio benefício. Esses apresentam um perigo iminente aos proprietários das mesmas, uma vez que os danos a quem as possua podem ser extremamente impactantes. Dados esses, o objetivo deste trabalho é definir os conceitos de segurança da informação e de redes de computadores e, desta forma, compreender como a segurança da informação pode atuar em uma rede de computadores para diminuir ou zerar os riscos que podem ameaçar todas e quaisquer informações que transitem em uma rede. O presente trabalho trata-se de uma revisão literária baseada em livros escritos nos últimos oito anos de autores especializados no assunto e abrange as ferramentas utilizadas no processo de proteção de uma rede de computadores, concluindo que é imprescindível o bom uso da segurança da informação não apenas para organizações, mas também para usuários comuns, tendo como final resultado, o resguardo da integridade, confidencialidade e disponibilidade que uma informação possui.

Palavras-chave: Segurança da informação; Redes; Riscos; Ameaças; Crime virtual.

BRANDÃO, João Lucas Laubstein. ***The Information Security in Computer Networks***. 2018. 31 p. *Completion of Course Work* (*Graduation in Computer Science*) – Anhanguera Educacional LTDA, Rio Claro, 2018.

ABSTRACT

Information is an extremely valuable asset that has always been a source of greed, not only for those who wish to grow with it in a strategic way, but especially for malicious entities who seek to break their secrecy for their own benefit. These present an imminent danger to the owners of the same, since the damages to who owns them can be extremely impactantes. These data, the objective of this work is to define the concepts of information security and computer networks and, in this way, understand how information security can act in a computer network to reduce or eliminate risks that can threaten any and all information that passes through a network. The present work deals with a literary revision based on books written in the last eight years of authors specialized in the subject and covers the tools used in the process of protection of a computer network, concluding that it is indispensable the good use of information security not only for organizations, but also for ordinary users, having as final result, the protection of the integrity, confidentiality and availability that an information possesses.

Key-words: *Information security; Networks; Risks; Threats; Virtual Crime.*

LISTA DE ABREVIATURAS E SIGLAS

ACL	*Access Control Lists*
SI	Segurança da Informação
CID	Confidencialidade, Integridade e Disponibilidade
LAN	*Local Area Network*
WAN	*Wide Area Network*
VPN	*Virtual Private Network*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
OSI	*Open Systems Interconnection*

SUMÁRIO

1. INTRODUÇÃO

Desde antes da era digital, a informação sempre foi motivo de cobiça para entidades maliciosas, e com o aumento da facilidade ao seu acesso após a chegada da internet, tornou-se fundamental o uso de ferramentas que auxiliam na sua proteção. Com toda a evolução das redes em geral, os crimes virtuais se tornaram cada vez mais constantes. Os criminosos estão evoluindo juntamente às tecnologias usadas por eles, que por sua vez, são cada vez mais sofisticadas e precisas, tornando a caça por informações mais simples e eficaz. É nesse escopo em que a SI (Segurança da Informação) atua.

Com isso, conclui-se que a proteção dos dados é algo totalmente indispensável, visto que as informações possuem um valor inestimável, uma vez que todo dado é armazenado em sistemas computacionais, que por sua vez, podem conter falhas e/ou vulnerabilidades que podem ser exploradas, tendo a rede de computadores como principal meio. O aumento dos crimes virtuais, sustentados pela facilidade que o avanço tecnológico traz, é um perigo iminente em um mundo ao qual a dependência do meio virtual e das redes de computadores como principal ferramenta para manipulação dos dados, cresce constantemente. Dados esses, observa-se a importância da segurança da informação nas redes de computadores. Seu uso e o estudo de suas características, das formas de aplicação e de suas técnicas, é indispensável para sistemas que utilizam a rede como principal meio para a manipulação de suas informações.

Dado esses, a segurança da informação aplicada às redes de computadores, é a solução mais óbvia e eficiente para lidar com esses tipos de criminosos e os riscos que esses podem oferecem, não só no meio empresarial como à usuários comuns que também utilizam desse meio. Considerando o aumento desses ataques às redes de computadores, como a segurança da informação pode atuar para reduzir os riscos?

Para responder à essa pergunta, é necessário entender como a segurança da informação pode atuar para reduzir os riscos em uma rede de computadores. E, para entender como a SI expõe-se a solucionar o problema em questão, é importante conceituar a segurança da informação e suas características, conceituar uma rede de computadores e, por fim, compreender como a SI pode reduzir os impactos dos riscos em uma rede de computadores.

O tipo de pesquisa foi uma revisão de literatura que retratou diversas obras de diversos autores tais como DANTAS e LYRA, onde foram utilizadas obras científicas publicadas nos últimos oito anos, que trouxe uma maior precisão aos dados que foram apresentados. Foram usados como locais de buscas, livros e sites que possuíam uma grande confiabilidade e reputação para garantia da autenticação de cada referência citada.

2. A SEGURANÇA DA INFORMAÇÃO E SUAS CARACTERÍSTICAS

Para que haja total compreensão do termo “segurança da informação” e entender seu significado propriamente dito juntamente à sua importância nos meios informacionais, é muito importante conceituar as palavras chave que compõem a mesma. De uma forma clara e objetiva, o conceito de informação pode ser definido por um agrupamento de dados filtrados e ordenados de tal modo que tragam algum sentido ou acepção dentro de determinado contexto. (LYRA, 2015).

A informação pode conter diversas formas, tais como: via impressa, formato eletrônico, dita, via correio tradicional ou eletrônico etc. Independente do formato, meio de transição ou armazenamento, é necessário que ela seja zelada de forma adequada. Dado esses, é de comprometimento da segurança da informação preservá-las de todo e qualquer tipo de risco ou ameaça. (COELHO; ARAÚJO; BEZERRA, 2014).

Onde existe informação, existe também o interesse em proteger a mesma de entidades não autorizadas, que por sua vez, podem gerar grandes danos às instituições que as possuam. Para isso, é necessário garantir os três princípios básicos de sua segurança: a integridade, a disponibilidade e a confidencialidade. São esses os princípios base da segurança da informação. (DANTAS, 2011).

Para entender como a segurança da informação pode atuar nos meios onde existe um grande tráfego de dados, inicialmente, é necessário compreender o que é a segurança da informação e quais suas características. Segundo Dantas (2011), a segurança da informação é a preservação da informação quanto a diversas variedades de ameaças, garantindo a estabilidade do serviço, minimizando os riscos e maximizando o retorno investido nos meios de manipulação de informações.

Já Coelho, Araújo e Bezerra (2014), definem a segurança da informação como a preservação dos sistemas, informações, recursos entre outros ativos contra infortúnios, falhas (sejam intencionais ou não) e adulterações de entidades não autorizadas, tendo como principal objetivo a diminuição das probabilidades e de impactos causados por incidentes de segurança. Tais controles precisam ser constituídos, implementados, vigiados, analisados de forma crítica, e otimizados para que dessa forma garantam que as metas dos negócios e a segurança da informação de determinado meio sejam alcançadas. (COELHO; ARAÚJO; BEZERRA, 2014).

A proteção de um conjunto de dados, depende dos princípios base que a segurança da informação traz, como: A integridade, que consiste na ideia de que a informação deve chegar ao seu destinatário sem perdas durante seu caminho, de forma que a mesma enviada seja exatamente a mesma recebida; A disponibilidade, que consiste na garantia de que o usuário autorizado para o acesso dessa informação, poderá acessá-la a qualquer momento, sempre que solicitada a requisição; E, por fim, a confidencialidade, que consiste na garantia de que somente entidades autorizadas poderão ter acesso às informações solicitadas, onde ninguém que não seja autorizado possa ler e/ou sobrescrever esses dados. (DANTAS, 2011).

Aprofundando-se nos pilares que sustentam a SI, segundo Lyra (2015), pode-se definir que a confidencialidade é a certificação de que o alcance à determinada informação é exclusivo à usuários ao qual a mesma foi destinada. Em outras palavras, seu acesso é autorizado somente à determinados usuários, garantindo desta forma, que somente o remetente e o destinatário possam acessar todo o conteúdo da informação em questão.

Já a integridade, Lyra (2015) afirma que o termo consiste na ideia de que toda e qualquer informação que transite em um meio, deve ser conservada de forma que o mesmo estado em que foi fornecido pelo seu proprietário, deve ser entregue ao destinatário, tendo em vista conserva-las contra adulterações mal-intencionadas, acidentais ou intencionais, ou seja, informações íntegras são informações que não sofreram alterações em todo seu percurso, desde o remetente até o destinatário.

Concluindo a tríade CID, Lyra (2015) defende que a disponibilidade consiste em assegurar que a informação e os meios envolvidos fiquem acessíveis para todo e qualquer usuário autorizado, de forma tal que, a qualquer momento, o mesmo possa acessar as informações. Desta forma, independente do intuito, a informação deve estar sempre disponível ao usuário.

Em contrapartida, Nakamura (2016) define: A confidencialidade é a característica que consiste que a informação esteja indisponível ou seja exposta a indivíduos, entidades ou processos não autorizados, ou seja, permitir que apenas ativos autorizados tenham todo e qualquer tipo de acesso às informações. Sobre a integridade: As informações têm de continuar íntegras independente o percurso que as mesmas percorram, em outras palavras, elas não podem sofrer quaisquer tipos de adulteração, ou seja, a integridade é a característica de resguardo da consistência e completeza de ativos. E, por fim, sobre a disponibilidade, Nakamura (2016) explica: A

disponibilidade consiste de uma particularidade interessante em comparação com as demais, cuja está associada à percepção. Diferencialmente da dificuldade que existe de notar em que momento a confidencialidade ou a autenticidade é comprometida, a disponibilidade de imediato é percebida quando há uma falha na segurança. (NAKAMURA, 2016).

Tais pilares são conhecidos pela sigla CID (Confidencialidade, Integridade e Disponibilidade), também chamadas de tríade CID, essas são fundamentais para a aplicação da segurança da informação seja em qualquer ambiente, tal como em uma rede de computadores. “Tais elementos não são uma mera coincidência, mas sim, os três pilares principais (ou princípios básicos) da Segurança da Informação. ” (LYRA, 2015, p. 10).

Além da tríade CID, existem também outros importantes fundamentos que estão relacionados aos riscos: a vulnerabilidade, as ameaças, os riscos, os ataques e os impactos. Quando o assunto é segurança da informação, é indispensável a presença desses termos, pois são estes elementos que os criminosos exploram como base para ferir os pilares da segurança da informação: a confidencialidade, a integridade e a disponibilidade.

Uma vulnerabilidade pode ser definida como uma brecha em todo e qualquer tipo de sistema ou infraestrutura que, uma vez explorada pelos criminosos, pode resultar em vários danos e transtornos, ferindo alguns ou todos os pilares da tríade CID, transpassando toda a proteção das informações, aos quais define como incidentes de segurança. (NAKAMURA, 2016).

Como complemento, pode-se afirmar que as vulnerabilidades são fraquezas que podem causar danificações consequentes do uso de dados em qualquer quadrante do ciclo de vida da informação. Essas brechas, se bem exploradas por indivíduos mal-intencionados, podem resultar em uma perda parcial ou até geral das informações. Em outras palavras, as vulnerabilidades são os pontos fracos que ativos maliciosos podem explorar à fundo e se beneficiar dos resultados coletados de uma rede ou sistema, provocando um enorme transtorno em um meio informacional de alguma forma. (DANTAS, 2011).

Com o esclarecimento das características de uma vulnerabilidade, as definições dos outros termos citados anteriormente se tornam mais claros e concisos. Após a vulnerabilidade, pode-se definir uma ameaça como toda e qualquer ocorrência que possa explorar uma vulnerabilidade. Circunstância potencial de um indesejado

incidente de segurança, que por sua vez, pode resultar em grandes prejuízos para um sistema ou uma organização em geral. Além das ameaças, também nesse escopo, existem os riscos, que podem ser definidos como a junção da probabilidade (chance de uma ameaça se concretizar) de algo acontecer e dos efeitos negativos que podem prejudicar um sistema ou uma corporação. Em outras palavras, é algo que pode acontecer e causar graves consequências nos objetivos de um usuário ou uma organização. (COELHO; ARAÚJO; BEZERRA, 2014).

Tendo em vista os riscos e as ameaças que uma informação sofre ao decorrer de seu ciclo de vida, também é muito importante definir o conceito de ataque. Coelho, Araújo e Bezerra (2014), defendem que o termo ataque pode ser definido como todas e quaisquer tipos de atividades que violem a proteção das informações de um usuário ou uma organização. Em outras palavras, pode-se definir um ataque como uma ação dirigida contra um ativo em específico ou diretamente à uma rede, afetando um ou todos os *hosts* que pertençam a mesma causando, desta forma, um grande transtorno às vítimas com roubos de informações ou qualquer outra violação que infrinjam um ou todos os pilares da tríade CID.

Em sequência da definição de ataque, os autores complementam defendendo que o conceito de impacto são consequências geradas por um ataque em específico, seja eles efetuados por ativos humanos ou artificiais, como softwares de exploração (*exploits*) ou *malwares*, em outras palavras, pode-se definir que os impactos são resultados de uma ação adversa que conseguiu com êxito infringir a tríade CID causando, consequentemente, danos, perdas, violações e /ou roubos das informações alvejadas pelos criminosos. A importância de se conhecer os impactos que os ataques podem causar e as probabilidades deles se concretizarem, consiste na possibilidade de calcular os riscos usando a fórmula: Risco = Impacto * Probabilidade. (COELHO; ARAÚJO; BEZERRA, 2014).

Concluindo os conceitos de segurança da informação e suas principais características, antes de entender como sua aplicação em uma rede de computadores pode proteger todas e quaisquer informações que trafeguem por ela, é fundamental conceituar, apresentar as propriedades e particularidades que uma rede de computadores possui e entender como a mesma trabalha, não apenas em nível teórico, mas também em nível operacional, uma vez que existem diversas formas e meios de se implementar a segurança da informação em uma rede de computadores, desde a condução de instruções básicas ao ativo, que são geralmente usuários leigos,

até o uso de antivírus, *firewalls* e *softwares* em geral, fortemente equipados das melhores e mais atuais tecnologias que possam lutar de forma igualitária contra entidades maliciosas que utilizam de recursos extremamente poderosos, explorando como principal caminho até as informações, uma rede de computadores que permita por falhas ou vulnerabilidades, o acesso às mesmas comprometendo sua confidencialidade, integridade e/ou disponibilidade. (COELHO; ARAÚJO; BEZERRA, 2014).

3. REDES DE COMPUTADORES E SUAS CARACTERÍSTICAS

Após a abordagem das definições e características da segurança da informação propriamente dita, antes de estudar sua aplicação em uma rede de computadores, é fundamental abordar um conteúdo completo e rico sobre as propriedades que compõem uma rede e dos atributos que a mesma possui no âmbito computacional, uma vez que ela é utilizada como principal meio de tráfego de informações responsável pela comunicação entre os dispositivos em todo e qualquer lugar do mundo.

Segundo Mosharraf (2013), é possível definir uma rede como sendo a reunião de vários dispositivos conectados entre si, capazes de se comunicarem uns com os outros. Nesse escopo, um dispositivo pode ser chamado de *host*, tais como *desktops*, *laptops* ou *smartphones*. Nesta definição, existem também dispositivos chamados de dispositivos de conexão, que podem ser roteadores, responsáveis por ligar uma rede a outras redes, um *switch* que liga dispositivos entre si, um modem, responsável pela alteração da forma dos dados e assim sucessivamente. Tais dispositivos são conectados em uma rede usando meios para transmissão dos dados com ou sem fio, como cabo ou o ar. Conectando-se dois computadores usando um roteador, cria-se uma pequena rede, por exemplo. (FOROUZAN; MOSHARRAF, 2013).

Pode-se obter diversos tipos de rede, dependendo da forma em que são utilizadas entre si, tendo como exemplo, uma rede LAN (*Local Area Network*), que geralmente é uma propriedade privada e que conecta alguns *hosts* em um único ambiente, pode ser combinada com uma WAN (*Wide Area Network*), que consiste na mesma ideia de uma LAN, capaz de conectar diversos dispositivos entre si, no entanto, ao contrário de uma LAN que possui seu tamanho limitado, a WAN pode ser estendida em uma área geográfica muito maior, podendo interligar dispositivos atravessando cidades ou até mesmo países, e seus *hosts* são geralmente *switches*, roteadores ou modems. Com a junção desses dois tipos de rede, pode-se obter uma *internetwork* ou *internet*, capaz de fazer com que dispositivos como *desktops* ou *smartphones* se comuniquem de qualquer lugar do mundo. (FOROUZAN; MOSHARRAF, 2013).

Com os dispositivos interligados em uma rede, é necessário viabilizar um meio de forma que eles possam efetuar comunicações entre si, possibilitando-os realizar transferências de dados e troca de informações. Para isso, é necessário que haja uma

estrutura que permita tal comunicação entre os *hosts* de uma rede, como o modelo OSI (*Open Systems Interconnection*).

O modelo OSI é uma arquitetura com sua estrutura baseada em camadas para projetos de sistemas em uma rede, que proporciona a conversação entre todo e quaisquer tipos de sistemas computacionais. Esse modelo fundamenta-se em sete camadas distintas, porém, ao mesmo tempo, inter-relacionadas, cada uma caracterizando uma fração do processo de transferência da informação por meio de uma rede. A compreensão do modelo OSI disponibiliza uma base concreta para o estudo da transmissão e interligação de dados. (FOROUZAN, 2010).

São sete as camadas que a estrutura desse modelo disponibiliza, que consistem nas camadas: Física, Enlace de Dados, Rede, Transporte, Sessão, Apresentação e Aplicação, as quais permitem compreender todo o processo em que as informações são submetidas e os caminhos que as mesmas percorrem para possibilitar a comunicação dentre os *hosts* de uma rede. Forouzan (2010), respectivamente define-as: A camada física executa os comandos requeridos para realizar o transporte de um fluxo de bits utilizando-se de um meio físico para realizar tal tarefa. Ela opera com os fatores tanto mecânicos como elétricos da interface e da via de transmissão. A camada Física define, também, os processos e as atividades que os *hosts* (dispositivos físicos interligados em uma rede) e as interfaces de rede precisam realizar para que a transmissão dos dados ocorra. A camada Física se responsabiliza por tratar as características físicas do campo de interação de uma rede e dos meios, representar os bits em uma transmissão de dados, comandar a velocidade que esses dados serão transmitidos, sincronizar os bits de uma transmissão, configurar a linha em um meio, administrar toda a topologia física e modos de transmissão.

Já a camada chamada Enlace de Dados, transforma a camada Física (uma ferramenta de transmissão bruta), em um link preciso e seguro. Ela permite à camada Física afigurar-se livre de falhas para a camada seguinte, que é a camada de Rede. O Enlace de Dados fica responsável pela formação dos frames, pelo endereçamento físico, pelo controle do fluxo de bits, pelo controle de erros e falhas e pelo controle de acesso. (FOROUZAN, 2010).

Após essa camada, os dados passam pela camada de Rede, a qual é responsável por transportar um pacote, desde sua origem até seu destino, muito provavelmente passando por um ou vários *links* (redes). Ao passo que a camada de

Enlace de Dados controla o envio do pacote entre dois sistemas ou interfaces de uma mesma rede (*link*), a camada de Rede é responsável por assegurar que cada pacote, partindo de seu ponto de origem, chegue ao seu devido destino. Se dois sistemas ou duas interfaces de rede estão conectadas em um link ao mesmo tempo, geralmente eles não necessitariam de uma camada de Rede. Não obstante, se ambos os sistemas estiverem conectados a redes (*links*) distintas com dispositivos de conexão entre elas, geralmente há necessidade da presença da camada de Rede para efetuar o envio da origem ao destino. A camada de Rede é responsável também pelo endereçamento lógico e pelo roteamento das redes para o controle do fluxo de dados. (FOROUZAN, 2010).

A camada seguinte é a camada de Transporte, que tem como principal objetivo realizar o envio de processo a processo de todo um conjunto de dados (mensagem a ser enviada) de forma completa e inteiriça. Processos são aplicações/*softwares* executados em um dispositivo (*host*). Apesar da camada de Rede supervisionar a rotina de envio de origem/destino de pacotes de forma individual, ela não efetua nenhum tipo de correlação entre eles. Ela lida individualmente com cada um de forma distinta, de modo que cada parte pertença a uma mensagem seja ela separada ou não. A camada de Transporte, em contrapartida, assegura que a mensagem inteira chegue ilesa, realizando o controle de erros e falhas, controlando o fluxo de dados em nível de origem/destino e garantindo a integridade da mensagem. É de encargo da camada de Transporte, o endereçamento de ponto de serviço, a segmentação e remontagem e o controle de conexões, fluxos e erros. (FOROUZAN, 2010).

A quinta camada da estrutura OSI, é chamada de camada de Sessão; nela, os serviços que as três primeiras camadas (Física, Enlace de Dados e Rede) disponibilizam, são insuficientes para alguns processos. A camada de Sessão é o manipulador da conversação da rede. Ela determina, conserva e coordena a interação entre sistemas e interfaces que se comunicam. São especialidades dessa camada: o controle de diálogo entre os dispositivos e a sincronização dos bits em um fluxo de dados. (FOROUZAN, 2010).

A camada de Apresentação refere-se à sintaxe e à semântica contidas nas informações que são trocadas entre dois sistemas ou interfaces de rede. Essa camada realiza a tradução da sequência de caracteres que compõem uma informação na conversação entre dois sistemas para que a mensagem enviada possa ser interpretada pelo sistema receptor. Ela é responsável também pela criptografia dos

dados e pela compactação dos mesmos em meio essa troca de informações entre os sistemas. (FOROUZAN, 2010).

A sétima e última camada é chamada de camada de Aplicação. Essa camada disponibiliza ao usuário final, seja ele um ativo humano ou artificial, o acesso propriamente dito à uma rede. Ela oferece interfaces de usuário e suporte à serviços de gerenciamento de banco de dados embarcados, e-mails, acessos remotos, transferências de arquivos entre outros tipos de serviços de compartilhamento/troca de informações. Em outras palavras, essa camada é responsável por exibir toda informação já traduzida e processada nas camadas anteriores para o usuário final, para que o mesmo possa acessar e interagir com a mesma, assim como os terminais virtuais de rede ou as transferências, acessos e gerenciamentos em geral de arquivos. (FOROUZAN, 2010).

Antes do modelo OSI, foi criado e desenvolvido os protocolos TCP/IP. Logo, as camadas que o montante de protocolos TCP/IP possui, não equivalem necessariamente às que constituem o modelo OSI. A coleção de protocolos TCP/IP é formado por cinco camadas: a camada física, camada de enlace de dados, camada de rede, camada de transporte e camada de aplicação. As primeiras quatro camadas concedem, respectivamente: padrões físicos, interfaces de redes, interconexão entre redes e funções/regas de transporte que compõe as primeiras quatro camadas do modelo OSI. Contudo, as três últimas camadas que formam o topo do modelo OSI, são caracterizadas na composição dos protocolos TCP/IP por uma única camada, denominada camada de aplicação. (FOROUZAN, 2010).

Mas para que os *hosts* se comuniquem entre si em uma rede, sejam elas uma LAN ou uma WAN, tendo como fundamento o modelo OSI, é fundamental a utilização de protocolos de conversação para que os mesmos se comuniquem na mesma “língua”, fazendo com que as informações sejam enviadas, receptadas e interpretadas com Êxito. Dentre os protocolos mais conhecidos na área da tecnologia da informação com o foco em redes, pode-se destacar o protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*), ao qual foi inicialmente desenvolvido para suprir as necessidades e solucionar os problemas de endereçamento e de interconexão das redes heterogêneas, tanto locais quanto também remotas. Pode-se considerar o protocolo TCP/IP uma estrutura composta por um agrupamento de diversos protocolos de comunicação utilizados nas redes locais (LAN) ou redes externas (WAN). (SOUSA, 2013).

Graças à sua formação de endereçamentos e sua inteligente estruturação, o protocolo TCP/IP tem a capacidade de efetuar o roteamento e transporte das informações entre as redes locais e as redes externas, tais como envio e recepção de e-mails, emulações remotas de terminais, transferências de arquivos, gerenciamentos de modo geral entre outras funções, possibilitando a interoperabilidade dentre variados tipos de redes. Diversos ambientes têm compatibilidade e suporte para esse protocolo, como os sistemas Windows, DOS, Linux, UNIX e etc., possibilitando a agregação dentre diversas plataformas. (SOUSA, 2013).

Comer (2016) complementa dizendo que nos protocolos TCP/IP, o chamado (de forma isolada) TCP (*Transmission Control Protocol*), concede um serviço de transporte preciso e seguro. Ele possui grande reconhecimento pois soluciona de forma eficaz, problemas de difíceis resoluções. Apesar da criação de outros tios de protocolos, nenhum tipo de protocolo de transporte com seu uso de maneira genérica, funcionou melhor do que no protocolo TCP. Com isso, a maior parte das aplicações, interfaces e sistemas que consistem em uma rede, são desenvolvidas com foco no suporte para o protocolo TCP. (COMER, 2016).

4. A APLICAÇÃO DA SEGURANÇA DA INFORMAÇÃO EM UMA REDE DE COMPUTADORES

Após a apresentação e definição de uma rede de computadores, dos protocolos e de suas camadas, é aberto uma grande perspectiva com uma visão extremamente ampla, de forma a garantir uma melhor compreensão dentro da abordagem da aplicação da segurança da informação em uma rede de computadores, assegurando uma maior fluidez em suas definições e facilitando o entendimento na fusão entre dois assuntos aparentemente distintos. Com isso, é fundamental apresentar a correlação entre os temas citados dentro do escopo em questão.

Quando se fala em uma rede de computadores de forma geral, seja ela desde uma LAN ou até uma *internetwork*, a segurança da informação tem como principal dever e objetivo de proteger todas e quaisquer informações que passem pelos meios de comunicação entre os *hosts*. Dados esses, a segurança da informação possui de diversas ferramentas para reduzir ou zerar os impactos que os riscos possam causar em uma rede de computadores exposta. (MORAES, 2010).

Dentre essas ferramentas, Moraes (2010) destaca recursos como a autenticação, a criptografia, as redes VPN, os protocolos de rede e os *firewalls*. Respectivamente, Moraes define: A autenticação consiste no processo de identificar se algo ou alguém é realmente quem afirma ser. Os métodos de autenticação são muito usados em redes de domínio público, como a Internet e em redes privadas como LAN’s residenciais ou corporativas. A autenticação se baseia nas três linhas básicas: A autenticação por algo que se saiba, a autenticação por algo que se tenha ou a autenticação por algo que se seja. (MORAES, 2010).

Fontes (2010), enriquece e complementa a definição de Moraes (2010) dizendo que a autenticação consiste em garantir que o usuário relatado na identificação é realmente quem diz ser. Em outras palavras, a autenticação busca provar que a pessoa que quer acessar determinada informação pessoal é a mesma de quem a informação pertence. Geralmente, o reconhecimento é um dado público e de fácil compreensão, diferente da autenticação, ao qual o dado deve possuir total sigilo.

No âmbito computacional, o indivíduo é autenticado por alguma informação que ele saiba (senha), possua (cartão, *token*) ou seja (característica física-biometria). Também é possível possuir uma conciliação entre dois tipos de autenticação,

aumentando assim, o nível de segurança. Como por exemplo, um cartão com senha, ao qual exige algo que se tem e que se sabe. (FONTES, 2010).

Em seguida, Moraes (2010) diz que, sobre a criptografia, pode-se definir como a ciência que usa de algoritmos matemáticos para encriptar dados legíveis, transformando-os em dados ilegíveis, de modo que somente quem possuir a chave para quebrar os algoritmos consiga total acesso a esses dados, tornando a informação algo mais concreto e de difícil acesso para entidades não autorizadas. (MORAES, 2010).

Como complemento, pode-se dizer que a criptografia é uma concepção estrutural aplicado na segurança da informação em uma rede de computadores para fornecer integridade, confidencialidade e autenticidade às informações. A criptografia propriamente dita, é uma ciência extremamente complexa, com fundamentos baseados em conhecimentos matemáticos, cuja é utilizada pelo ser humano desde muitos séculos atrás.

O uso da criptografia garante a confidencialidade de uma informação, que pode ser dividia em três fundamentos básicos, sem contar a própria informação: a chave e os métodos de encriptação e decriptação. Os métodos usados para realizar a encriptação e a decriptação, são usualmente chamados de algoritmos de cifragem e decifração. Os dados de entrada que os algoritmos de cifragem recebem, são chaves de cifragem e informações em sua condição natural e compreensível para que venham passar pela criptografia e conceda, como saída, a informação criptografada. Já o algoritmo de decifração, por sua vez, realiza a operação inversa, recebendo como dados de entrada as chaves de decifração e a informação criptografada, proporcionando, após os processos, os dados de saída que contém a informação original. (MORAES, 2010).

Na realidade, os algoritmos de cifragem e de decifração são acessíveis a nível público. O seguro da confidencialidade de um dado está na consistência da chave a qual passará pelos métodos de cifragem e decifração, em outras palavras, todo o conhecimento que essas chaves possuem, contém o segredo que necessita de proteção. É precisamente de acordo com a chave de cifragem que os processos são divididos em dois gêneros: a chave simétrica e a chave assimétrica. Outro fator relevante é a função/algoritmo aplicado na criptação do texto a ser codificado. (CARISSIMI; ROCHOL; GRANVILLE, 2010).

Logo após, Moraes (2010) prossegue definindo as redes VPN (*Virtual Private Network*) como redes de circuitos virtuais que transmitem tráfego privado. Uma VPN é uma conexão que se baseia em criptografias para manipular informações através de uma rede insegura, como a Internet, por exemplo. As VPNs consistem em tecnologias de criptografia, autenticação e tunelamento. É útil para interligar pontos de conexão entre dispositivos de qualquer lugar do mundo através da Internet de uma forma extremamente segura.

Como citados anteriormente, outro fator muito importante na segurança da informação aplicada à uma rede de computadores, são os protocolos de rede, que, por sua vez, consistem em normas e sistemas de comunicação que tem como objetivo organizar as formas de conversação entre os dispositivos em pontos distintos de uma rede. Sousa (2013), complementa dizendo que os protocolos atuam na capacidade de efetuar o roteamento das informações entre redes locais e externas, realizar o transporte de dados e arquivos, emular remotamente terminais, realizar o envio e recebimento de e-mails, gerenciamentos gerais entre outras funções, possibilitando a comunicação operacional entre diferentes tipos de rede, de forma que não haja perda de dado por meio comunicativo, aumentando a integridade das informações, um dos pilares base da segurança da informação.

Como último fator citado por Moraes (2010), o *firewall*, é uma tecnologia indispensável para que uma rede tenha o mínimo de segurança em seu tráfego de dados. Ele é a base e o fundamento de toda a segurança da informação aplicada em uma rede de computadores, fazendo dele, a ferramenta mais importante para que uma rede e suas informações estejam seguras. O *firewall* consiste em um sistema que age com o foco em um único ponto de defesa entre redes privadas e redes públicas. Ele possui ainda a capacidade de monitorar o trânsito de informações em sub-redes de uma rede privada. Em outras palavras, praticamente toda a movimentação de entrada e saída de uma rede, deve necessariamente passar antes pelo *firewall*. Ele controla a autorização e negação das informações que tentam entrar ou sair da rede, além de armazenar tudo o que passar por ele.

O *firewall*, ou “parede de fogo”, auxilia na proteção do perímetro de uma rede. Entende-se por perímetro de rede, uma linha fictícia entre uma rede interna, que se deve total atenção em sua proteção, e uma rede externa, que geralmente é exposta quando se fala em Internet.

Dessa forma, pode-se definir um perímetro como o ponto de acesso de uma rede externa até uma rede interna, ou vice-versa. Desde que se iniciou a migração dos amplos sistemas de computadores para os sistemas de baixa plataforma, de forma tal havendo a criação das redes locais existentes, manifestou-se a carência de se determinar um perímetro de rede, logo, o *firewall* possui uma função indispensável, pois é ele que irá distinguir a rede assegurada (interna) da rede desprotegida (externa). Desta forma, o *firewall* é o alicerce de toda a proteção em um perímetro de rede.

O *firewall* é responsável por realizar e administrar todo o controle de acesso, o qual ocorre através da aplicação das listas de controle de acesso, ou ACLs (*Access Control Lists*). ACL são tabelas que possuem definições e instruções, através do controle de origem e destino de cada pacote que trafegue na rede, determinando se os mesmos são bloqueados, permitidos ou monitorados pelo *firewall*. Desta forma, o *firewall* se torna um portão, isto é, ele é o responsável pelo controle de interconexões de rede que saiam e/ou passem por ele. (MORAES, 2015).

Em suas configurações *default*, os *firewalls* impedem todos e quaisquer tráfego de dados que possam passar por ele. Desta forma, o “admin”, responsável pela segurança da rede, a partir da adoção de uma política de segurança e suas definições, deve ajustar as regras de tráfego no *firewall,* de forma tal que os tráfegos de dados autorizados, sejam liberados e declarados como permitidos. O *firewall* pode também ser utilizado para proteger as redes internas de um mesmo âmbito, tendo como exemplo, um banco que queira isolar o setor financeiro do resto de toda a rede dos setores do banco, possibilitando desta forma, com o auxílio do *firewall*, um nível de segurança extremamente superior aos usuários desse setor, pois essa medida impede que haja um ataque direto à rede do setor financeiro, forçando o possível ataque a passar por outros setores sem ter acesso ao setor alvo. (MORAES, 2015).

A resolução desse problema permite constituir e complementar o conhecimento dos perímetros de segurança e compreender como é possível isolar uma rede interna, de maneira tal que permita o controle dos acessos, aplicando as políticas de segurança em uma rede. Um *firewall* pode ter a simplicidade de um roteador que controla os pacotes se baseando em um ACL, mas pode ser complexo de maneira tal como um *firewall* de aplicação, que nesse nível, monitora todos e quaisquer pacotes até a camada de aplicação do protocolo utilizado, antes de decidir bloquear ou liberar o pacote que esteja passando por ele. (MORAES, 2015).

Em uma WAN, os *firewalls* são designados à administração do acesso à Internet, logo, pode-se referir à essa rede como a Internet propriamente dita. É importante ressaltar que os endereçamentos dessas redes possuem grande relevância, dado esses, a parte externa da área compartilhada do *firewall* obrigatoriamente tem de conter um endereço legítimo na rede. (MORAES, 2015).

Para conclusão do assunto retratando o *firewall*, em uma LAN, o mesmo possui a responsabilidade de proteger a rede interna. De forma generalizada, os *hosts* de uma rede podem trabalhar com endereçamentos não registrados ou não válidos, designando ao *firewall* o dever de administrar todas as funções que gerenciam os IPs e os endereçamentos. Todo tráfego dessa LAN, que não passe por uma rede externa (Internet), fica impossibilitado de receber os tratamentos adequados do *firewall* justamente por não transitarem por ele. (MORAES, 2015).

5. CONSIDERAÇÕES FINAIS

A segurança da informação possui diversas variáveis que, se utilizadas corretamente, podem blindar toda e qualquer informação que a seja aplicada, fazendo com que entidades maliciosas não tenham uma solução viável para a quebra de seu sigilo. O estudo de seus conceitos e aplicações é fundamental para proteger as informações propriamente ditas e/ou um meio como um todo, como uma rede de computadores, resultando em um tráfego seguro para as mesmas, uma vez que o caminho por onde elas passarem será controlado por ferramentas da S.I. Dados esses, pode-se concluir que a abordagem dos conceitos da segurança da informação foi esclarecido com sucesso, pois permite compreender como e quais serão as aplicações da mesma para garantir o sigilo dos dados assegurados.

Para a aplicação da S.I., são indispensáveis o estudo e a abordagem dos conceitos de uma rede de computadores, a qual possui um grande horizonte de ferramentas, que tornam a aplicação da S.I., possível em um conjunto de *hosts* interligados entre si. Como base de uma rede computacional, é necessário abordar o escopo de protocolos de rede, como o protocolo TCP/IP, permitindo concluir que: para a aplicação da segurança da informação em uma rede de computadores, é imprescindível que os protocolos sejam a ponte entre a aplicação da segurança da informação e uma rede de *hosts* interligados propriamente dita.

Finalizando o produto da fusão entre os dois assuntos abordados, pode-se concluir que o objetivo primário foi atingido com êxito, tal como os objetivos secundários, dado que o estudo permitiu compreender onde e como a aplicação da segurança da informação em uma rede de computadores pode proteger as informações que trafeguem por esse meio, garantindo que os pilares da tríade C.I.D. (Confidencialidade, Integridade e Disponibilidade) permaneçam intactas, sem que haja qualquer tipo de violação da mesma.

Há de se desenvolver um estudo que demonstre ainda mais a importância da segurança da informação, fornecendo detalhadamente, conteúdos mais aprofundados de sua aplicação não apenas em uma rede de computadores, como também em *hosts* e *hardwares* individuais, sempre enfatizando o grande poder que informações privilegiadas podem trazer para entidades que saibam utiliza-las tanto para o bem, quanto para o mal.

REFERÊNCIAS

CARISSIMI, Alexandre da Silva; ROCHOL, Juergen; GRANVILLE, Lisandro Zambenedetti. **Redes de Computadores**. Porto Alegre: Bookman, 2010. 390 p.

COELHO, Flávia Estélia Silva; ARAÚJO, Luiz Geraldo Segadas de; BEZERRA, Edson Kowask. **Gestão da Segurança da Informação**. Rio de Janeiro: RNP/ESR, 2014. 198 p.

COMER, Douglas E. **Redes de Computadores e Internet**. Porto Alegre: Bookman, 2016. 556 p.

DANTAS, Marcus. **Segurança da Informação: Uma Abordagem Focada em Gestão de Riscos**. Olinda: Livro Rápido, 2011. 150 p.

FONTES, Edison Luiz Gonçalves. **Segurança da Informação: O Usuário faz a Diferença**. São Paulo: Saraiva, 2010. 172 p.

FOROUZAN, Behrouz A.; MOSHARRAF, Firouz. **Redes de Computadores: Uma Abordagem Top-Down**. Porto Alegre: AMGH, 2013. 928 p.

FOROUZAN, Behrouz A. **Protocolo TCP/IP**. Porto Alegre: AMGH, 2010. 879 p.

LYRA, Maurício. **Governança da Segurança da Informação**. Brasília: Edição do Autor, 2015. 160 p.

MORAES, Alexandre Fernandes de. **Segurança em Redes: Fundamentos**. São Paulo: Érica, 2010. 262 p.

MORAES, Alexandre Fernandes de. **Firewalls: Segurança no Controle de Acesso**. São Paulo: Érica, 2015. 120 p.

NAKAMURA, Emílio Tissato. **Segurança da Informação e de Redes**. Londrina: Editora e Distribuidora Educacional S.A., 2016. 224 p.

SOUSA, Lindeberg Barros de. **Rede de Computadores: Guia Total**. São Paulo: Érica, 2013. 334 p.