ROBERT CERQUEIRA DE OLIVEIRA

ADEQUADAS TÉCNICAS A GESTÃO DE SEGURANÇA DA INFORMAÇÃO NA INTERNET

ROBERT CERQUEIRA DE OLIVEIRA

ADEQUADAS TÉCNICAS A GESTÃO DE SEGURANÇA DA INFORMAÇÃO NA INTERNET.

Trabalho de Conclusão de Curso apresentado à Instituição Anhanguera como requisito parcial para a obtenção do título de graduado em Sistema de informação.

Orientador: Samuel Novais

Brasília - DF
2020

ROBERT CERQUEIRA DE OLIVEIRA

ADEQUADAS TÉCNICAS A GESTÃO DE SEGURANÇA DA INFORMAÇÃO NA INTERNET.

Trabalho de Conclusão de Curso apresentado à Instituição Anhanguera como requisito parcial para a obtenção do título de graduado em Sistema de informação

BANCA EXAMINADORA

Prof(a). Titulação Nome do Professor(a)

Prof(a). Titulação Nome do Professor(a)

Prof(a). Titulação Nome do Professor(a)

Brasília, 29 de Setembro de 2020

Dedico este trabalho a Deus, que é o verdadeiro guia dessa caminhada, sem sua infinita sabedoria, nunca teria sucesso.

ROBERT, Oliveira. **Adequadas técnicas a gestão de segurança da informação na internet**. 2020. Número total de folhas: 45. Trabalho de Conclusão de Curso de Graduação em Sistema de Informação – Instituição Anhanguera, Brasília-DF, 2020.

RESUMO

O presente trabalho de tcc exibe as normas de gerenciamento de segurança da informação, com o objetivo de resolver questões referentes a segurança de redes, seus conceitos, suas propriedades, visando ajudar a encontrar soluções para evitar danos significativos na utilização de ambientes em rede, impedindo assim ataques aparentemente invisíveis aos utilizadores de rede de computadores, com objetivo de furto de dados ou informações. A tecnologia se desenvolve rapidamente, a abundância de hardware e software conectado à world wide web jamais foi tão significativa, temos telefones, laptops, pulseiras inteligentes, todo tipo de hardware interligados à internet e com nossos dados, o que possibilitam inovação na configuração de intercâmbio entre humano-computador, através de algoritmos inteligentes, sendo o incremento dessas novas tecnologias através da utilização dos nossos dados, eles também são associados a um grande número de aplicativos conectados à internet, no mundo, o uso desse tipo de equipamento e de seu software já se tornou uma realidade, os nossos dados, são capturados através das redes de internet, esses dados viram informações, que são utilizadas, para diversas finalidades, no entanto não se questiona a questão da privacidade e a segurança da informação, sendo assim extremamente importante o estudo da base de gerenciamento de segurança em redes de computadores, garantindo aos usuários a confidencialidade, integridade, disponibilidade e privacidade.

Palavras-chave: Segurança; Gerenciamento; Internet; Hackers; Informação.

ROBERT, Oliveira. **Adequate techniques for managing information security on the internet**. 2020. Total number of pages: 45. Conclusion of the Graduation Course in Information System - Anhanguera Institution, Brasília-DF, 2020.

ABSTRACT

The present work of term paper shows the information security management standards, with the objective of solving issues related to network security, its concepts, its properties, aiming to help find solutions to avoid significant damages in the use of networked environments, preventing thus apparently invisible attacks on computer network users, with the objective of stealing data or information. Technology is developing rapidly, the abundance of hardware and software connected to the world wide web has never been more significant, we have phones, laptops, smart bracelets, all types of hardware connected to the internet and with our data, which enable innovation in the exchange configuration between human-computer, through intelligent algorithms, and the increase of these new technologies through the use of our data, they are also associated with a large number of applications connected to the internet, in the world, the use of this type of equipment and its software it has already become a reality, our data are captured through internet networks, these data become information, which are used for various purposes, however the question of privacy and information security is not questioned, being thus extremely important the study of the security management base in computer networks, guaranteeing users confidentiality and, integrity, availability and privacy.

Keywords: Security; Management; Internet; Hackers; Information.

LISTAS DE FIGURAS

LISTAS DE TABELAS

ABREVIAÇOES

IBGE..... Instituto brasileiro de geografia

SUMÁRIO

1. INTRODUÇÃO

Como todos sabemos, a conveniência com a tecnologia, trouxe uma realidade em que as trocas de informações foram desenvolvidas por uma questão de necessidade. A internet tem uma velocidade cada vez mais rápida para o compartilhamento e desenvolvimento de informações necessárias para o continuo desenvolvimento humano, mas esta função na comunicação mundial causa um problema: Acesso incorreto as informações, confiabilidade de dados e privacidade dos usuários e companhias. Perante esses fatos, a segurança da informação passou a ser uma questão muito importante, sendo discutido e revisado presentemente e mais importante do que nunca sendo o principal utensílio para adoção de disposições ardilosas em vários aglomerados e departamentos da sociedade.

A importância desse trabalho se baseia, na questão do gerenciamento para que os dados sejam protegidos contra apropriações indevidas e utilizadas para prejudicar pessoas ou ambientes de projetos.

A internet deve oferecer aos seus usuários um ambiente seguro, essa deve ser a prioridade, a segurança da informação não é apenas uma ferramenta preventiva, ela garante que seus dados não deverão ser utilizados para fins indevidos ou não autorizados.

O termo gestão de segurança de dados indica as possibilidades de resguardar as informações criadas por usuários, companhias e seus ambientes de projetos através do gerenciamento das ferramentas de segurança.

Os dados e informações gerados são considerados um item valioso no mercado, eles são importantes para companhias que utilizam essas informações para direcionar consumo de pessoas, mostrar tendências de negócio, gerenciar estoques, oferecer e direcionar serviços e bens para consumo e produção.

Acontece que esses dados são colocados em um algoritmo que gera informações que apresentam por exemplo tendências de consumo, essa informação para uma companhia é importante pois garante competividade no mercado e ao mesmo tempo ajudam as empresas a se manter competidoras. os usuários desejam que suas informações sejam protegidas garantindo assim a privacidade das informações e as empresas desejam a mesma coisa pois seus negócios dependem dos usuários.

A questão é que progressivamente estamos conectados e enviando dados, em uma proporção cada vez maior, isso abre a possibilidade de crescentemente mais pessoas estão procurando formas de quebrar a segurança e capturar as informações tanto de usuários como de companhias, em contrapartida também temos ferramentas de gerenciamento de segurança para garantir a proteção desses sistemas.

O conhecimento é atributo intelectivo humano e o seu domínio é desejado por muitas pessoas e empresas, quando alguma informação é vazada, acidentalmente ou propositalmente, seja por desleixo ou a sagacidade podem prejudicar a pessoa ou causar prejuízo em participação da organização no mercado. Algumas etapas podem ser executadas para ajudar a controlar a utilização e segurança dos dados, e principalmente garantir a confiabilidade, privacidade e disponibilidade das informações

Averiguar os princípios básicos na área de gerenciamento de segurança da informação, suas dificuldades e aspectos.

Determinar os princípios básicos de gerenciamento de segurança da informação; examinar as dificuldades para a gestão da segurança de informação; distinguir aspectos futuros da aplicabilidade aprendida no gerenciamento de segurança da informação

Compreende-se que as informações são patrimônios importantes para qualquer empresa ou usuário, pois essas informações são utilizadas para manter a sobrevivência do negócio e aperfeiçoamento nas decisões de atitude. Diante disso é importante compreender como proteger as informações e evitar que esses dados sejam invadidos ou expostos, prejudicando a imagem das pessoas ou empresas

Os métodos utilizados no trabalho pesquisado podem ser apresentados como o procedimento de coleta e armazenamento de dados proeminentes e seguros sobre o tema que foi constituído como um assunto de pesquisa. Para que a análise alcance o desígnio de confirmar a necessidade de proteção através do gerenciamento das informações.

A metodologia de análise como processo de desenvolver de forma elegante e sistemática, com o desígnio de responder às questões colocadas. “A pesquisa é requerida quando não se dispõe de informação suficiente para responder ao problema [...]” (GIL, 2007, p. 17).

Deste modo a pesquisa irá desenvolver os seguintes itens:

- classificação da análise
- proposito de recolhimento de dados

2. GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO

De um modo geral, a segurança da informação é responsável por cuidar das informações e dados coletados e compartilhados, os responsáveis por isso são os usuários ou banco de dados que anotam, arrecadam e gravam esses elementos. A principal função dessa tarefa é a proteção permanente, no entanto os usuários não tem essa visão, se colocando as vezes em riscos (SILVA; STEIN, 2007).

O gerenciamento de dados tem como objetivo garantir que as atividades e dados gerados pelos seus usuários estejam protegidos de possíveis coletas não autorizadas, por vezes os próprios usuários acabam se colocando em risco de compartilhar informações privadas com terceiros sem autorização. Perante isso o trabalho de gerenciar a segurança se torna cada vez mais importante e a várias formas de proteger esses dados (OLIVEIRA; MOURA; ARAÚJO, 2012).

Muitos usuários e companhias discutem a respeito da segurança de dados, com o objetivo de chegar a um patamar de proteção cada vez maior, esses discursos surgem no momento em que a tecnologia evolui crescentemente alcançando todos os âmbitos do desenvolvimento humano, diante dessa realidade é necessário investimentos na questão da segurança para a garantia de confiança e privacidade para gerar um ambiente com mais interações de desenvolvimento(RIGON; WESTPHALL, 2011).

Partindo desse seguimento, numerosas dificuldades permanecem, a principal delas é o usuário, pois é esse que produz os dados e todos os desafios estão conexos a criar e desenvolver técnicas e ferramentas para aprimorar a segurança da informação. Deve-se focar nas ferramentas de gerenciamento para que as informações não sejam utilizadas de forma que não ocasionem riscos ou perdas aos usuários e companhias (SILVA; STEIN, 2007).

Contudo, as previsões futuras nessa disciplina de segurança é que tenhamos uma evolução para o desenvolvimento de tecnologias, com esforços crescentes e mundiais para que se crie mais ferramentas capazes de melhorar o gerenciamento da segurança em redes de internet (OLIVEIRA; MOURA; ARAÚJO, 2012).

Proteger os utilizadores de internet ou trabalhadores de tecnologia é uma forma de proteger as instituições em todo o mundo, garantindo segurança e privacidade para o desenvolvimento de projetos em todos os âmbitos (OLIVEIRA; MOURA; ARAÚJO, 2012).

2.1 CONCEPÇÃO DE DADOS

Apesar da conotação de dados e informação serem parecidas, existe conceitos diferentes em relação aos termos utilizados, o que gera confusão em questão do uso, sendo assim os dados são avulsos, como se fossem características separadas dentro de um plano maior, ao juntar vários dados temos uma característica completa sobre o tema abordado(SILVA; STEIN, 2007).

Podemos dizer que os dados estão espalhados e desconectados, portanto, não se pode tirar terminações específicas sobre um assunto. Todo algarismo sendo ele o nome e a data no código são determinados como os dados, mas só podemos saber o real significado quando agrupamos e organizamos, para que os usuários possam encontrar significado logico, como também identificar características mais complexas (RIGON; WESTPHALL, 2011).

A importância dos dados é grande por que de maneira correta e agrupada eles geram informações para um processo maior, seja em um banco de dados ou em um sistema de analise, gerando assim relatórios para tomada de decisões que garantam uma estratégia de sucesso (OLIVEIRA; MOURA; ARAÚJO, 2012).

Muitas companhias utilizam desse meio para alcançar objetivos empresariais, realizando assim Investimentos na captura e processamento de dados, isso garante o investimento no empreendimento, o caminho correto, se analisando essas dados para auxiliar em tomadas de decisões, nem sempre é necessário a captura de maneira ilegal desses dados pois muitos dados ficam disponíveis para a extração, por exemplo, em uma simples pesquisa no IBGE você consegue descobrir quantos habitantes tem em determinado pais, quais são seus costumes e assim realizar um cruzamento da dados para encontrar um nicho de mercado para investimento(RIGON; WESTPHALL, 2011).

Os usuários também podem utilizar esses dados para benefício próprio, pois isso garante disposições astutas, maior confiabilidade adotadas nas decisões para atingimento de metas pessoais, só é necessário dar sentido aos dados, transformando-os em informações (SILVA; STEIN, 2007).

2.2 CONCEPÇÃO DE INFORMAÇÃO

A compreensão do assunto sobre segurança e gerenciamento da informação está conectada a ideia de informação. A informação é o resultado de vários dados relacionados, ganhando sentido ou seja os dados relacionados geram informações que podem ser utilizadas, por exemplo conjunto de dados do usuário, ou da companhia, isso pode gerar estratégias para que se alcance o objetivo proposto para na tomada de decisão(RIGON; WESTPHALL, 2011).

É importante as informações, pois a civilização do modo que conhecemos necessita disso para realizar várias agilidades e planejamentos, qualquer setor seja na área de bem-estar, capitalização, instrução, politicas necessitam disso para existir. Toda informação obtida gera uma função dentro do contexto, as companhias apreciam isso devido a sua importância nas atividades desenvolvidas, por mais que a informação gerada não seja útil no momento, ela pode ser aplicada futuramente em outra ocasião, isso se aplica tanto a empresas como para os usuários(RIGON; WESTPHALL, 2011).

As informações podem ser divididas em tipos e suas aplicabilidades podem ser variadas, dependendo de quem as adquire, o foco pode ser verificar tendências de mercado por exemplo, então a várias entidades em busca de informações para tomadas de decisões, gerando uma rede de informações constante(SILVA; STEIN, 2007).

As informações estão em todos os lugares, desde quando você passa seu cartão bancário para comprar uma agua, até o momento que o usuário utiliza o celular para realizar uma tarefa de lazer, tudo é recolhido, processado e gerado informações que serão utilizadas em determinado momento para garantir esse movimento cíclico dentro das sociedades, a grande questão é quando essas informações são utilizadas para o bem-estar social ou para outras finalidades(SILVA; STEIN, 2007).

Além disso, com o recolhimento desses dados e gerados essas informações sobre usuários e empresas, qual a aplicabilidade pode ser realizada sem causar danos aos emissores de dados, como compreendemos se aquela informação será utilizada de maneira correta, e a pior parte é será que isso terá um aproveitamento real para o crescimento e desenvolvimento humano de forma saudável, sem causar efeitos colaterais indesejados(OLIVEIRA; MOURA; ARAÚJO, 2012).

Tantos usuários como empresas necessitam de utilizar as informações para agregar valor em seus empreendimentos, sem deixar de lado a questão da segurança e privacidade sobre as informações emitidas através dos dados (SILVA; STEIN, 2007).

2.3 SEGURANÇA DA INFORMAÇÃO

A aplicabilidade dos meios tecnológicos é variada e as diversas maneiras diferentes de utilização dos mesmos dentro de uma sociedade, e a cada momento essas aplicações se mostram inovadoras para resolução de problemas enfrentado pela humanidade, no entanto essa utilização dos meios tecnológicos trazem riscos para seus usuários, como por exemplo a invasão da privacidade das informações sem consentimento ou até mesmo o compartilhamento de informações falsas para levar os usuários a um entendimento errado, conhecido como fake News(SILVA; STEIN, 2007).

Tanto organizações como pessoas devem adquirir informações que garantam confiança de conteúdo, e garantia que seus dados não sejam colocados a disposições de risco. Esse ambiente de internet ou redes devem garantir informações completas e ter disponibilidade para utilização para gerar resultados satisfatórios (SILVA; STEIN, 2007).

Acontece no entanto que as informações podem ser hackeadas e expostas de forma que prejudica seus usuários, as empresas ainda não possuem toda a disposição de proteção das informações , seja por falta de ciência ou imissão na área de segurança, assentando assim em ímpeto não apenas as informações de seus usuários como também da própria empresa(OLIVEIRA; MOURA; ARAÚJO, 2012).

As informações são por essência confidenciais, isso significa que somente usuários previamente autorizados, podem ter acesso a informação emitida, no momento que acontece uma captura indevida, ou seja sem autorização, isso gera danos aos indivíduos, seja ele empresa ou pessoas, além é claro de uma perda de confiança(RIGON; WESTPHALL, 2011).

Outro problema conhecido na área de segurança é a falta de integridade da informação que basicamente é quando a informação prestada aos usuários está incompleta ou com adulterações, e portanto, insegura, pois se a informação está incompleta ou maquiada, logo isso abre margem para decisões incorretas, o que pode

ocasionar perdas significativas na confiança da prestadora de informações, é necessário assim garantir a informação correta(RIGON; WESTPHALL, 2011).

Por fim temos a disponibilidade que é a utilização da informação quando seus usuários acessam independente do momento ou quando se faz necessário a sua consulta, caso a consulta não retorne em tempo hábil, isso também gera problemas as entidades que realizam a consulta do conteúdo(OLIVEIRA; MOURA; ARAÚJO, 2012).

2.4 GERENCIAMENTO DA SEGURANÇA

Devido a importância de armazenar informações na área tecnológica, surge a carência de ter recursos para proteger as informações de utilização imprópria, criando desse modo o campo de gerenciamento da segurança da informação, que são ferramentas e protocolos para impedir incursões e diversos episódios que conseguiriam ser excessivamente prejudiciais para usuários e empresas(RIGON; WESTPHALL, 2011).

Portanto, parece que o gerenciamento da segurança da informação não é somente uma tarefa, mas toda uma metodologia com pleno cuidado, atuações e providências que submergiu para evitar o uso impróprio destas informações sem autorização (RIGON; WESTPHALL, 2011).

Apresenta-se a figura para melhor compreensão:

Figura 1: estrutura de gestão.

Fonte: https://webinsider.com.br/itil-e-a-seguranca-da-informacao-parte-i/

Diga-se que o gerenciamento de sistema de informação é um melhoramento continuo das melhores práticas, sendo que é necessário avaliar e melhorar os procedimentos, dentro do ambiente corporativo, essa técnica é aplicada através de auditorias internas e externas com a finalidade de corrigir eventuais problemas e melhorar os procedimentos(SILVA; STEIN, 2007).

A gerencia de segurança representa um papel de cuidadora das informações, e para administrar foi desenvolvido métodos para garantir segurança aos processos, sendo uma área que se desenvolve a todo instante, contando hoje com vários recursos focados na proteção, no entanto vários setores ainda não consideram a gerencia de segurança importante para suas empresas ou informações, é necessário um amadurecimento dessa mentalidade para a preservação dos ativos como dados e informações estejam realmente protegidos(SILVA; STEIN, 2007).

Para aprimorar a compreensão sobre tipos de segurança da informação, apresenta-se a figura, que acompanha:

Figura 2 :Tipo de segurança da informação

Fonte: http://www.teleco.com.br

A segurança humana foca na proteção dos usuários que fazem uso das ferramentas e protocolos de segurança da empresa (OLIVEIRA; MOURA; ARAÚJO, 2012).

A segurança lógica prioriza o desenho do emprego dos recursos de aplicativos e software nas diferentes agilidades habituais da instituição que se depara de detenção deles (JORGE, 2011).

A proteção física dar ênfase especial no local onde as Informações são encontradas. Refere-se à necessidade de proteção, dos equipamentos e procedimentos (JORGE, 2011).

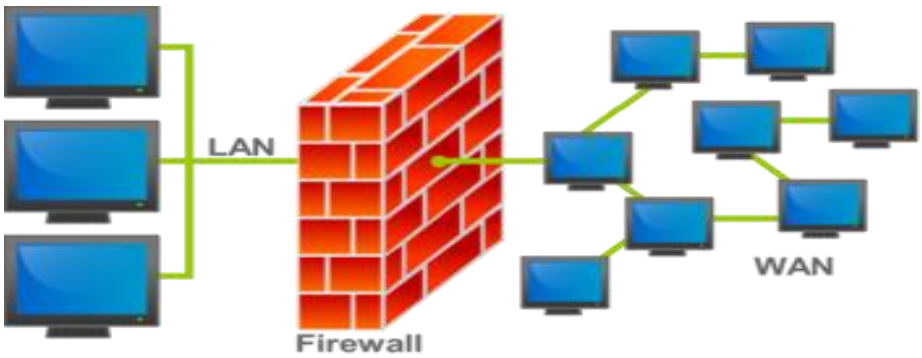
2.5 FERRAMENTA DE SEGURANÇA

Um dos principais instrumento de gerenciamento de segurança é um firewall, que é um aglomerado de elementos distribuídos em um ponto da rede de uma companhia ou instituição, ele transmite os dados organizados para fora, seu desígnio é fornece segurança, controle, autenticação, apontamentos de tráfego e monitoramento, identificando ameaças potenciais a segurança do usuário ou rede, além disso ele controla informações e gerencia hardware e software, possuindo características de controlar a navegação dos dados de entrada e saída, sendo uma ponte entre o ambiente interno e externo, tornando-se um bloqueador caso o conteúdo não seja autorizado, como um filtro(OLIVEIRA; MOURA; ARAÚJO, 2012).

O firewall filtra tudo que trafega entre a empresa e o ambiente externo, esse filtro é configurado pelo administrador da rede, no qual controla o conteúdo de dados de entrada e saída, fazendo uso de alguns filtros como: proxy e bastion hosts, zona em outra linguagem o Firewall é um bloqueador de conteúdo que possa causar algum dano à rede, para melhor compreensão(JORGE, 2011).

apresenta-se a imagem a seguir.

Figura 3: Ferramenta de segurança



Fonte: https://pt.wikipedia.org/wiki/Firewall

Os filtros são gerados pelo roteamento de critério de pacotes de dados, acolhendo ou rejeitando as informações contidas em seus requisitos. As normas de filtragem são realizadas pela companhia, cabendo a ela definir seus parâmetros (JORGE, 2011).

por exemplo:

- O filtro de proxies são servidores com capacidade de atuar como sistema mediador em meio a internet e a rede interna das companhias, interpondo os requerimentos de usufrutuários e o ambiente exterior.

- Os bastions hosts, a sua parte, identifica-se como servidores nos quais se abrigam tarefas oferecido aos usufrutuários externos da companhia. A cargo de seu contato com ambiente externos, eles necessitam ser resguardados ao mais elevado para que adimpla exclusivamente tarefas e aproveitamentos para as afins de que as destinadas, feita para resistir ataques.

O instrumento de firewall é muito extraordinário para a artifício de segurança de informações de uma companhia, um aglomerado de entradas que orientam o gerenciamento de segurança das informações de uma companhia, necessitando ser advertido pelos usufrutuários internos e externos. O artifício de segurança decide os requisitos a serem acompanhadas pela empresa apontando garantir as soluções computacionais e elementos ali às ordens (SILVA; STEIN, 2007).

3 ADVERSIDADES PARA O GERENCIAMENTO DE SEGURANÇA DA INFORMAÇÃO

3.1 ADVERSIDADES DE GESTÃO

A grande adversidade atual é o combate a invasão, proteção e segurança dos dados armazenamento, evitando assim crimes relacionados a tecnologia de dados.
O meio mais utilizados para obter informações e dados é a internet, pois essa é uma ferramenta quase que universal para navegação em redes, por ser um ambiente consideravelmente novo, e que cresce constantemente, apresenta-se como uma adversidade a utilização, de maneira que os usuários podem cometer crimes e ainda é difícil de controlar e gerenciar o seu uso(STALLINGS,2008).

Com o desenvolvimento e diversificação do meio ambiente de internet, e a abonação de host para host se tornou mais abstrusa e o uso de padrões de garantia continua a crescer na Internet. Usando o exemplar de segurança de rede, a autoridade de elevação está ensimesmada em seus múltiplos hosts e os aparelhos que fornecem, em vez de fazê-los um por um, através de métodos de segurança de rede, que incluem firewalls para resguardar códigos interiores e redes, use autenticação intensa e sistema de criptografia para proteger os dados especialmente extraordinário na web. Portanto, os sítios podem obter o uso de um modelo de segurança de rede aumenta garantindo assim uma segurança maior (STALLINGS,2008).

No quesito de crimes cibernéticos, temos um histórico desde o início da criação da internet e dos meios tecnológicos que a sociedade está inserida, pode-se avaliar que quando cria-se um ambiente novo, é apresentado do mesmo modo, adversidades para a utilização desses recursos, sendo o vírus um dos problemas que mais afetam os sistemas de internet e meios de comunicação, basicamente tudo que utiliza um S.O, ou esta interligado a ele, pode ser hackeado (MARCIANO, 2006).

Os vírus são programas desenvolvidos com a finalidade de prejudicar de algum modo o funcionamento adequado de algum sistema, tendo como característica similar a fácil propagação dentro de um equipamento que utiliza S.O e de difícil extermínio, assim como a internet se expande, os softwares maliciosos crescem da mesma

maneira, se aproveitando de falhas no gerenciamento de gestão de segurança da rede ou do mal uso pelos usuários, acarretando assim perdas significativas de funcionamento adequado das maquinas e até perdas financeiras, e o modo mais comum de ser contaminado por um vírus é a utilização desse ambiente de internet sem os devidos cuidados(SILVA; STEIN, 2007).

3.2 TIPOS DE VIRUS

Malwares são softwares de computador projetado para invadir ilegalmente o sistema de computador de outra pessoa para ocasionar determinado detrimento, adulteração ou saque de informação. Ele pode surgir na configuração de algoritmo executável, scripts e diferentes programas (RIGON; 2011).

Spywares são softwares desenvolvidos como espiões, tendo sua principal função furtar dados sobre as atividades de uma máquina, ele coleta dados de forma ilegal, no entanto nem todos os spywares são utilizados para prejudicar, muitas empresas utilizam esse software para coletar de maneira legal dados de seus clientes para posteriormente oferecer serviços mais adequados a necessidade do usuário (RIGON; 2011).

Backdoors significa porta dos fundos, são estruturas usual por vários softwares maliciosos para facilitar o acesso remoto a softwares ou redes infectadas. O programa foi projetado para usar falhas instaladas, desatualizadas e problemáticas que não são documentadas em aplicativos de firewall para acessar as portas do roteador, escapando assim de autenticidade ou criptografias do SO. (RIGON; 2011).

3.3 CONFIANÇA NO AMBIENTE DE INTERNET

A utilização de navegação na internet é importante como uma ferramenta de crescimento, a absolvição de dados e geração de informação, isso significa que é um fator de sobrevivência, na internet é compartilhado todo o conhecimento adquirido na história da humanidade, é não param de ser gerado dados nesse ambiente, a empresa ou usuário que deseja alcançar um nível de competividade

necessita dessa ferramenta para tomada de decisão, além disso a internet é um meio do qual estamos inseridos desde o momento que nascemos, os nossos dados são colocados em rede assim que nascemos, e eles são armazenados, processados e enviados para armazenamento. Diante disso a importância na proteção desses dados é de suma importância social, é necessário garantir um ambiente seguro, com informações autenticas, e disponível quando necessário (OLIVEIRA; 2012).

Uma empresa ou um governo que não protege a base de dados desse ambiente cai em falta de credibilidade, perdendo assim a confiança de seus usuários, além é claro de perdas com o comercio, na área de vendas e tomadas de decisões, pois seus usuário irão utilizar outros meios de armazenamento e proteção de dados, então é essencial que o foco seja continuo contra os crimes cibernéticos (OLIVEIRA; 2012).

A ocorrência de fato e que existem várias adversidades envolvendo a proteção de dados, principalmente quando ela envolve o cotidiano dos usuários que utilizam meios de tecnologia, suas celeridades com trabalho e o relacionamento com outros usuários e empresas tanto nacionais quanto internacionais, o uso frequente da redes proporciona uma vida melhor, com mais informações para encarar as dificuldades diárias, quando informações de algum usuário acaba sendo furtada, isso coloca em risco a vida privada, ocasionando em crimes contra a honra e o direito de privacidade, sendo necessário a confiabilidade, confidencialidade e proteção. (SILVA, OLIVEIRA; 2012).

3.4 DESAFIOS COTIDIANOS

Os crimes virtuais estão se tornando corriqueiros em diferentes aspectos da vida social, são vários os tipos de crimes cometidos utilizando as redes de internet, e o impacto dessa modalidade criminosa, coloca em questionamento a questão de segurança da informação, para que se possa compreender melhor o assunto, é necessário realizar um levantamento das possíveis adversidades que ocorrem dentro desse ambiente chamado internet, segue a tabela para compreensão dos principais meios de crimes vinculados ao uso de redes de internet:

Tabela 1: Adversidade no gerenciamento de segurança

ADVERSIDADES DO COTIDIANO	
Crime cibernéticos	Crime cometido por hackers ou organizações com a finalidade de furtar dados de pessoas ou empresas com a finalidade de ganhar alguma vantagem. Podemos citar por exemplo: fraudes, roubos de dados, extorsão, espionagem, o maior desafio nesse crime é identificar o causador e punir conforme a lei do país, sendo que nem todos os países dispõem de sistema para punir esse tipo de crime.
Confiabilidade	Esse é um dos pilares da segurança da informação, sendo ele responsável por garantir a privacidade dos dados de seus usuários.
Integridade	Esse conceito baseia que as informações prestadas estão de maneira integras, sem adulterações ou modificadas do original, ela é base para tomada de decisões assertivas, é também para o entendimento correto do assunto procurado.
Disponibilidade	É a capacidade de estar disponível quando necessário, independente do momento ou

	eventualidade, a ausência dessa base pode acarretar atrasos para a realização de determinado trabalho, podendo gerar prejuízos.
Segurança dos dados	é necessário guardar as informações dos usuários de maneira segura, garantindo a disponibilidade, integridade, e confiabilidade, pois sem essas bases não existe segurança dos dados.
Controle de acesso	É uma ferramenta utilizada para garantir que somente o usuário autorizado acesse determinada informação.
Rastreamento de modificação ou acesso	É uma ferramenta que realiza a leitura de quem foi a última pessoa a realizar o acesso e o que foi modificado.

Fonte: https://guilhermebsschaun.jusbrasil.com.br/artigos/686948017/uma-lista-com-24-crimes-virtuais

4 GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO

Com o surgimento da internet e os meios tecnológicos de comunicação, existe uma preocupação global por segurança nas redes de internet, no início essa era uma área pouco explorada, mas com o avanço da tecnologia e a importância da informação, essa área ganhou destaque em vários meios tecnológicos, pois a proteção é um fator primordial para a continuidade de sua existência em diversos meios, sejam eles comerciais ou pessoal (TANENBAUM; 2011).

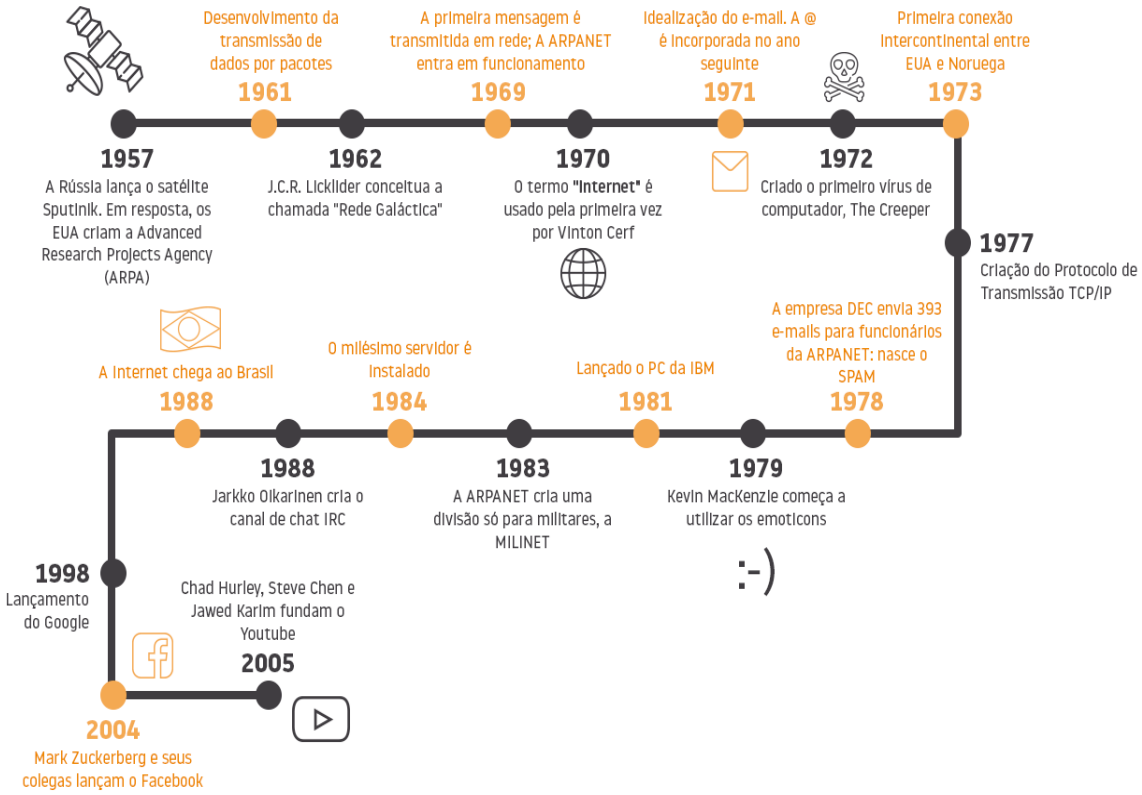
Vive-se em um momento onde as informações são essenciais para geração de renda e auxilio no comercio empresarial, garantindo as detentoras de informações a capacidade de tomadas de decisões mais assertivas, dando a essas empresas ou usuários a possibilidade de se tornar mais competidoras em um mundo globalizado e conectado por vários meios tecnológicos (TANENBAUM; WETHERALL, 2011).

No início da era dos computadores, esses meios tecnológicos estavam nas mãos de universidades e exercito, mas com o passar do tempo surgiu os computadores para usuários em geral, transformando o modo de vida das sociedades, um mundo agora conectado e compartilhando dados em tempo real, ao mesmo tempo que isso foi uma solução para vários problemas, ele acabou gerando outas adversidades que necessitam de solução criativa para garantir um melhor ambiente para seus usuários (TANENBAUM; WETHERALL, 2011).

Depois do surgimento do computador, ainda não era comum acontecer crimes virtuais, pois a tecnologia tinha sido lançada recentemente e nem todos tinham acesso a ela, no entanto não demorou muito para que alguns indivíduos encontrassem meios de burlar o sistema e tirar proveito desses, surge então os primeiros ataques com a finalidade de tirar proveito da situação em benefício próprio (TANENBAUM; WETHERALL, 2011).

Apresenta-se seguir a figura para entender essa evolução da tecnologia.

Figura 4. Evolução da internet.



fonte:http://www.henet.com.br/site/historia-da-internet-a-trajetoria-da-ferramenta-que-revolucionou-a-nossa-comunicacao/

Ao verificar a figura consegue-se compreender que inicialmente os computadores foram criados com finalidade de armazenamento e processamento de dados, utilizados pelo poder militar, essa tecnologia foi compartilhada com universidades e percorreu um caminho consideravelmente curto até chegar aos nossos aparelhos celulares, atualmente a tecnologia que surgiu na década de 50 esta conectada a tudo que utilizamos no nosso dia a dia, estamos completamente conectados e transmitindo dados, e é nesse momento que encontramos uma advertência ao uso da tecnologia, pois ao mesmo tempo que as informações começaram a serem compartilhadas garantindo competitividade entre empresas, alavancando comércio virtual, ajudando pessoas a terem uma vida melhor com tecnologia disruptivas, também surge questões em relação ao acesso não

autorizado das informações, muitas vezes os usuários viram produtos comercializados para as empresas consumirem e produzirem através de algoritmos de tendências comportamentais produtos ou sugestões para alavancar vendas comerciais, entende-se que os dados do usuário, pertence ao usuário e esse é o responsável por autorizar o acesso ou não dos dados, no entanto grandes comparações utilizam informações de maneira ilícita, quebrando assim um dos pilares da segurança de dados, além disso temos também pessoas mal intencionadas que acessam os dados de terceiros ou de empresas para se beneficiar de alguma forma, ou seja, tanto empresas, quanto usuários de internet podem ter seus dados furtados e isso pode gerar prejuízos inestimáveis (TANENBAUM; WETHERALL, 2011).

4.1 PROTEÇÃO PELO GERENCIAMENTO DE SEGURANÇA

Existem alguns princípios básicos para realizar o gerenciamento de segurança da informação, eles têm que estar vinculados a disponibilidade, integridade, confiabilidade e autenticidade.

A disponibilidade garante aos seus usuários que a informação estará sempre disponível independentemente do momento que for solicitado, para garantir essa base é necessário que a exista um backup das informações, o firewall e o nobreak.

- Nobreak é um aparelho com capacidade de disponibiliza energia para o funcionamento do sistema em situações de emergência, ele é utilizado para que não haja o cessamento de energia dos aparelhos conectados a rede, garantindo assim que no caso de uma eventualidade o serviço não deixe de ser prestado ou seja, mesmo com falta de energia, o serviço não deixará de funcionar.
- Firewall é uma ferramenta de bloqueio de conteúdo que pode ser configurada para evitar ataques de terceiros ao sistema, ele impede a penetração de dados que possam ser nocivos a atrapalhar a prestação de serviços.

- Backup é utilizado para armazenamento das informações, normalmente os usuários e empresas utilizam esse serviço para garantir que caso aconteça alguma eventualidade como furto das informações ou corrompimento dos dados, haja um backup de segurança com os dados, é recomendado a utilização de 2 backups, sendo um de segurança, caso um seja corrompido o outro automaticamente assume e o serviço não deixa de ser prestado.

A integridade é outra base importante, ela garante que os dados estão de maneira integra, e que somente pessoas autorizadas podem modificar ou alterar seu conteúdo, isso impede que terceiros acessem seus dados e façam manipulações não autorizadas, as ferramentas utilizadas para ter a garantia da integridade de um sistema de dados ou informações são as assinaturas digitais e o backup.

- Assinatura Digital é uma assinatura de determinado documento, sendo que quando há uma alteração a assinatura anterior é invalidada, necessitando de uma nova assinatura, isso garante o controle sobre os documentos assinado.

A confiabilidade é a garantia que somente pessoas autorizadas podem acessar determinada informação, ou seja a informação é sigilosa, e somente o usuário pode determinar quem pode acessa-la, a ferramenta utilizada para garantir a confiabilidade é a criptografia.

- Criptografia é uma técnica ou conjunto de princípios que mistura as informações por meio de um algoritmo com essa finalidade, é transforma a informação em algo que não seja possível reconhecer.

Além disso é necessário garantir através de autenticações e restrições que somente os usuários com autorização acessem os dados, então é necessário que todos que tenham acesso a rede utilizem senhas individuais para a liberação de conteúdo, é isso não envolve somente empresas que armazenam dados, mas também usuários que fazem uso de redes.

A autenticidade avaliza a confiança da autoria da informação, demostrando também o não repudio, isso significa que o autor da informação não pode recusar a sua autoria, reconhecendo assim quem é o emissor da informação, as

ferramentas capazes de garantir a autenticidade da informação é biometria, assinatura digital e certificado digital.

- Biometria é uma forma de identificar o usuário através de alguma característica física única, servindo como se fosse um CPF, por exemplo: leitor de íris, reconhecimento facial, leitor da digital, comando de voz e etc.
- Certificado digital é uma forma de garantir que determinada informação realmente pertence ao emissor, exemplo em determinados sites existe um cadeado na parte superior, aquilo garante que de fato o site pertence a empresa.

Em frente a isso, pode-se dizer que o objetivo geral é chegar ao ponto onde a segurança da informação consiga inibir qualquer risco de segurança para usuários, e garantir que as informações geradas estejam protegidas de qualquer ataque ou falhas do sistema (TANENBAUM; WETHERALL, 2011).

5 CONSIDERAÇÕES FINAIS

O uso de redes de internet se tornou algo essencial para várias áreas de atuação da sociedade, nossos postos de trabalho necessitam de computadores conectados à internet, nossa comunicação, as compras e vendas de empresas, independentes da localização geográfica, a sociedade está conectada as redes de internet e compartilhando informações em tempo real.

O avanço dessas novas tecnologias de compartilhamento de informações em redes de internet abriu um leque de opções para pessoas e empresas efetuarem seus negócios e gerenciarem suas vidas, tudo de maneira rápida e integrada.

No entanto do mesmo modo que esse compartilhamento de diversas informações facilitam a vida e abrem portas para novas possibilidades, eles também geram problemas de segurança da informação, pois dados não autorizados podem ser vazados sem autorização do usuário, fazendo assim gerar problemas na questão de sigilo e segurança.

O objetivo de quem utiliza as redes de internet para obter dados ou informações sem autorização de seus usuários são diversos, podendo ser para ganhar vantagem competitiva no mercado, prejudicar a imagem do usuário, entre tantos outros motivos.

O que deveria significar a solução para vários problemas enfrentados pela sociedade, se tornou tema importante para a garantia da segurança da informação pois quando o usuário se sente inseguro, ele deixa de utilizar uma ferramenta que pode ajudar a evolução da sociedade, o usuário ainda pode continuar utilizando as redes mas procurando aqueles sites ou empresas virtuais que ofereçam maior segurança para seus dados.

Em relação a esse receio surge a segurança da informação, para a proteção dos dados compartilhados, ou armazenados em bancos de dados, os países se preocupam com esse tema, pois isso significa mais confiabilidade nas ferramentas utilizadas pelos seus usuários.

Referente a isso, o estudo do tema tem o objetivo de avaliar as formas de proteção para a segurança da informação, demostrando os principais problemas que surgem na utilização das redes e como resolve-los, pois essa tecnologia apresenta um crescimento continuo, dessa forma é interessante desenvolver fórmulas de proteção de dados na internet.

REFERÊNCIAS

História da Internet**: A trajetória da ferramenta que revolucionou a nossa comunicação**. disponível em: http://www.henet.com.br/site/historia-da-internet-a-trajetoria-da-ferramenta-que-revolucionou-a-nossa-comunicacao/ > acesso em 15/10/2020.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 2007.

GUILHERME, Schaun**. Uma lista com 24 crimes virtuais**. https://guilhermebsschaun.jusbrasil.com.br/artigos/686948017/uma-lista-com-24-crimes-virtuais . Acesso em 15/10/2020

Segurança da informação – **princípios básicos de segurança**. Disponível em: https://www.grancursosonline.com.br/download-demonstrativo/download-resumo/codigo/vxD8%2BTdlEdg%3D#:~:text=Existem%20quatro%20princ%C3%ADpios%20b%C3%A1sicos%20de,%2C%20Integridade%2C%20Confidencialidade%20e%20Autenticidade.&text=De%20acordo%20com%20o%20Princ%C3%ADpio,dispon%C3%ADvel%20sempre%20que%20for%20preciso.> acesso em 15/10/2020.

WEBBINSIDER. ITIL **e a segurança da informação.** Disponível em: https://webinsider.com.br/itil-e-a-seguranca-da-informacao-parte-i/. acessado em 15/10/2020

MARCIANO, João Luiz Pereira. **Segurança da Informação: uma abordagem social**. Brasília, 2006. Disponível em: < http://repositorio.unb.br/bitstream/10482/1943/1/Jo%C3%A3o%20Luiz%20Pereira%20Marciano.pdf> Acesso em: 15 jan. 2017.

MARCONI, Marina de Andrade. LAKATOS, Eva Maria. **Metodologia científica**. 5 ed. São Paulo: Atlas, 2007.

OLIVEIRA, Gabriella Domingos de; MOURA, Rafaela Caroline Gaudêncio de; ARAÚJO, Francisco de Assis Norberto Galdino de. **Gestão da segurança da informação: perspectivas baseadas na tecnologia da informação**. 2012. Disponível em: <

http://portaldeperiodicos.eci.ufmg.br/index.php/moci/article/viewFile/2111/1311> Acesso em: 11 mar. 2017.

RIGON, Evandro Alencar; WESTPHALL, Carla Merkle**. Modelo de avaliação da maturidade da segurança da informação.** VII Simpósio Brasileiro de Sistemas de Informação. 2011. Disponível em: < http://www.lbd.dcc.ufmg.br/colecoes/sbsi/2011/modelodeavalicao.pdf> Acesso em: 12 jan. 2017.

SILVA, Fábio Alves da**. A evolução das tecnologias de segurança da informação a partir das demandas do setor financeiro**. Curitiba: UFPR, 2014. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/187759/Jesiel%20TCC%20final.pdf?sequence=1> Disponível em: Acesso em: 15/09/2020.

STALLINGS, Stallings William, **Criptografia e segurança de redes,** Quarta Edição, São Paulo, Pearson Editora do Brasil, 2008.

TANENBAUM, Andrew S.; WETHERALL, David J. **Rede de computadores.** 5. ed.

São Paulo: Saraiva, 2011.