CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA CURSO DE GRADUAÇÃO TECNOLÓGICA EM REDES DE COMPUTADORES

ASSUERO MOTA

JHONATHA HENRIQUE

SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS NO AMBIENTE CORPORATIVO

RECIFE/2020

ASSUERO MOTA

JHONATHA HENRIQUE

SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS NO AMBIENTE CORPORATIVO

Artigo apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores.

Professor Orientador: Mestre Adilson da Silva

RECIFE/2020

S729s Souza, Assuero Silva Mota de
Segurança da informação e proteção de dados no ambiente corporativo. / Assuero Silva Mota de Souza; Jhonatha Henrique Amaral Bernardino. - Recife : O Autor, 2020.
33 p.

Orientador (a): Adilson da Silva

Trabalho De Conclusão De Curso (Graduação) Centro Universitário Brasileiro – UNIBRA. Graduação Tecnológica em Redes de Computadores, 2020.

1. Segurança. 2. Informação. 3. Privacidade. 4. LGPD. 5. Violação. I. Centro Universitário Brasileiro - UNIBRA. II. Título

CDU: 004.7

AGRADECIMENTOS

Primeiramente gostaríamos de agradecer a Deus.

Ao nosso orientador Adilson da Silva por aceitar conduzir nosso trabalho de pesquisa.

A todos os nossos professores do curso de Redes de Computadores do Centro Universitário Brasileiro pela excelência da qualidade técnica de um.

E aos nossos pais que sempre estiveram ao nosso lado nos apoiando ao longo de toda a nossa trajetória.

“Nas grandes batalhas da vida, o primeiro passo para a vitória é o desejo de vencer.” (Mahatma Gandhi)

SUMÁRIO

Segurança da informação e proteção de dados no ambiente corporativo

Assuero Silva Mota de Souza
Jhonatha Henrique Amaral Bernardino
Adilson da Silva[1]

Resumo: Em decorrência de ataques sofridos por grandes empresas, surgiu a necessidade de meios onde os dados de clientes e funcionários de corporações fossem protegidos. Com isso houve uma certa urgência da criação de padrões que tornassem as informações e os dados de grandes instituições mais seguros. A partir disso serão citados neste trabalho os padrões de gestão da segurança ISO/IEC 27001 e 27002, também serão abordados meios legais que punem empresas que usam dados de funcionários e clientes de forma ilegal e formas seguras de compartilhamento de informações seguros para que ocorra uma redução nos casos de vazamentos de dados.

Palavras-chave: Segurança. Informação. Privacidade. LGPD. Violação

[1] : Professor da UNIBRA MSc. Adilson da Silva orientador.
E-mail para contato: adilsondasilva.professor@gmail.com

1 INTRODUÇÃO

A facilidade de se obter informação tem evoluido a cada dia, essa facilidade na comunicação mundial gera um problema: o acesso inadequado a informação que tem aumentado gerando falta de confiabilidade fazendo a segurança ser uma necessidade em todos os ambitos principalmente no corporativo. Sêmola (2003) define segurança da informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

Em um ambiente corporativo,criar vantagens competitivas nos negócios se faz necessário velocidade e eficiência e a falta de segurança traz consigo a falta de novas oportunidades de negócios pois justamente essas mesmas características serão a mais atingidas.

Segundo (Rezende e Abreu, 2000) a informação desempenha papéis importantes tanto na definição quanto na execução de uma estratégia, a eficacia das empresas são definidas pelos resultados que elas vão adquirindo.

Um estudo Realizado pelo Instituto Ponemon em parceria com a Varonis, descobriu-se que 62% dos funcionários afirmam que possuem acesso a dados que não seriam necessários para realizar suas tarefas diárias. Ainda, menos de 30% das empresas possuem registros do que seus funcionários estão fazendo com as informações (COMPUTERWORLD, 2016).

Assim, entender os problemas e as formas de resolvê-los torna-se imprescindível, principalmente porque não se pode proteger contra riscos que não se conhece. Portanto este estudo tem como principal objetivo apresentar os conceitos, as técnicas e as tecnologias de segurança que podem ser usados na proteção dos dados das empresas e organizações. A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa (Sêmola, 2003).

A formação de um ambiente seguro e as motivações para a

implementação de uma segurança coerente será comentada, os motivos que levam à adoção de determinada tecnologia, e também de certa forma trazer uma concientização do grande desafio e reconhecimento do valor da segurança dentro das organizações.

2 DELINEAMENTO METODOLÓGICO

Este estudo enquadrou-se no modelo de delineamento denominado pesquisa bibliográfica, que baseia-se nas informações colhidas de grupos de tecnologia, fóruns, livros e sites específicos sobre o assunto relatado.

Foram colhidas informações em algumas entrevistas feita a determinados gestores de T.I que tratam da questão de segurança em algumas empresas, aconselhamentos de segurança vivenciados foram utilizados como referência no nosso trabalho, informações triviais dos acontecimentos negativos em relação a eventos que marcaram época de certa forma para fortalecer nossos argumentos mostrando assim certa credibilidade no assunto que foi abordado. Foram trazidos certos discursos e trabalhos apresentados em universidades que nos ajudaram a realização da pesquisa como um todo.

Na primeira fase foi falado dos conceitos básicos da segurança da informação, na segunda fase da responsabilidade de se defender mostrando os variados problemas causados por ataques humanos ou tecnologicos que tem por objetivo a destruição dos dados ou ter algum tipo de beneficio pessoal envolvido, na nossa 3 fase foi mostrado mecanismos, técnicas e formas utilizadas para proteção dos dados, e na nossa última fase as leis protetivas para clientes e usuários que por algum motivo foram postos em situações comprometedoras.

O contato com o projeto foi bem tranquilo sendo o orientador receptivo a essa atividade e disposto a ajudar sempre que possível.

Segundo URIARTE (2005) ”O desenvolvimento da criatividade, Sensibilidade,motricidade, interdisciplinaridade, raciocínio, conhecimento de si e as inter-relações, são aspectos importantes para construções do conhecimento e do caráter do sujeito.

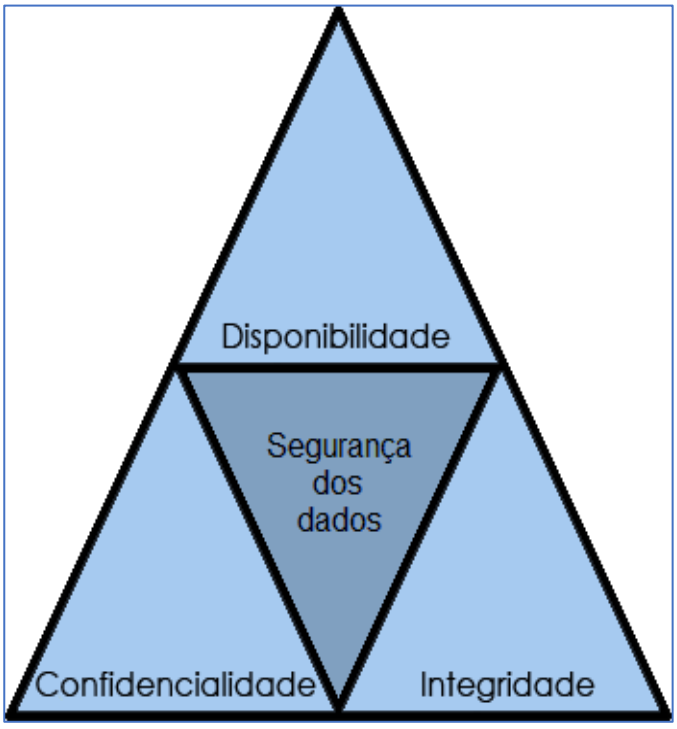
3 SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação é a parte responsável por garantir que não ocorra acessos não autorizados a todo ativo tecnologico como Computadores, Redes ou Fonte de Dados.

3.1 Principíos basicos da informação

Conforme Anderson (2003), Três atributos que devem ganhar importância quando se trata de Segurança e que agem de forma preventiva são: confiabilidade, integridade e disponibilidade, demonstrado na Figura 1.

Figura 1 - Segurança da Informação - Tríade CID



Fonte: Otto Carlos Muniz (2012).

- **Confidencialidade**

O manual de procedimentos do COBIT.5 (2012) A confidencialidade é o atributo da informação que garante que a informação será de acesso exclusivo a pessoas ou companhias autorizadas pelo fornecedor, confidencialidade é essencial para o mundo corporativo pois qualquer dado sigiloso que sofreu um vazamento poderá trazer vantagens competitivas para as demais empresas.

- **Integridade**

Para Galvão (2015) integridade como a informação que mesmo manipulada, ainda permaneceu com as devidas características iniciais a qual foi tratada pelo proprietário da informação, integridade é essencial faz comunicação ficar mais solida e evita retrabalhos portanto prejuízos e energia desperdiçada.

- **Disponibilidade**

Quem nunca passou por uma situação de congestionamento ou site acessado ficou fora ar, para (DANTAS, 2011) disponibilidade é o atributo que evidencia e faz com que nenhuma atividade seja paralisada e as empresas que prezam pelos seus negócios devem priorizar a disponibilidade a informação.

Outros autores (Dias, 2000; Wadlow, 2000; Shirey, 2000; Krause e Tipton, 1999; Albuquerque e Ribeiro, 2002; Sêmola, 2003; Sandhu e Samarati, 1994)também defendem que para uma informação ser totalmente segura ela ainda precisa dos seguintes atributos:

- **Autenticidade** – é quando se reafirma com exatidão sua origem.
- **Não repúdio** – quando não é possível negar o envio ou recepção de uma informação ou dado.
- **Legalidade** – é quando todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.

- **Privacidade** – neste caso é atribuído o caráter de confidencialidade a informação, é a capacidade de um usuário realizar ações em um sistema sem que seja identificado.

- **Auditoria** – Consiste no exame do histórico dos eventos dentro de um sistema para determinar quando e onde ocorreu uma violação de segurança.

3.2 Conceitos relacionados à SEGURANÇA DA INFORMAÇÃO

Para entender segurança é necessário entender alguns conceitos básicos como: Ameaças, Vulnerabilidades , Ativos, mecanismos de segurança e ciclo de vida da informação (Tatiele Zanella, 2017).

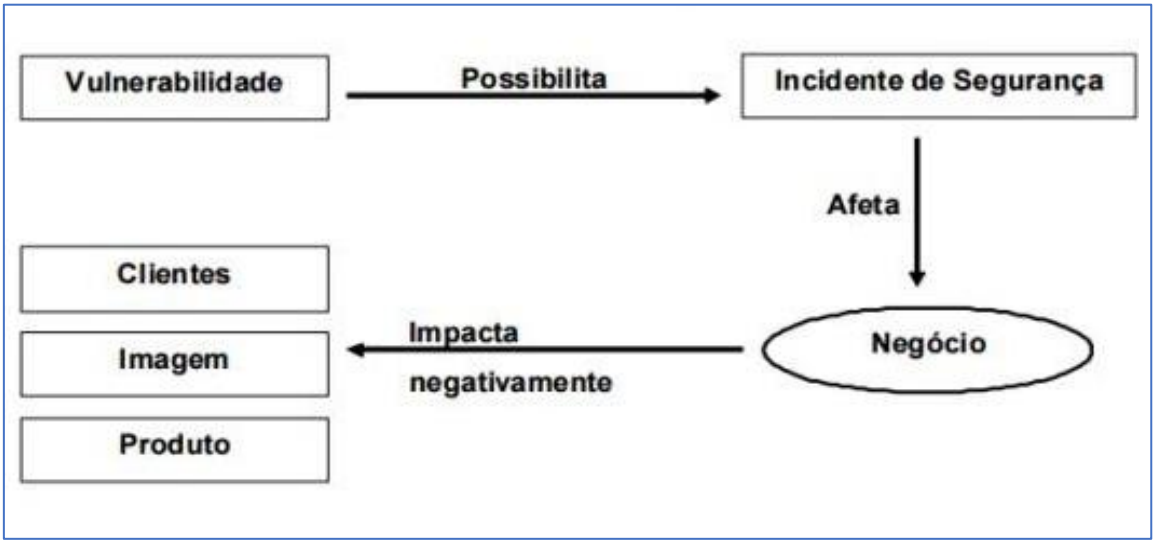
- **Ameaças** conforme (Sêmola, 2003) são agentes ou condições que afetam as informações e seus ativos, explorando as vulnerabilidades, gerando incidentes de perda de confidencialidade e impactos aos negócios da empresa.

- **Vulnerabilidade** são portas ou janelas abertas que são ocasionadas primordialmente por falhas no projeto de implementação do mesmo, problemas estruturais,não segmentos de normas, problemas com Hardware ou Software.

Em palavras citadas por (Galvão, 2015) em seu livro Fundamentos em Segurança da informação ele diz que fraqueza e fragilidade estão relacionados ao ativo da empresa e podem ser compreendidos como vulnerabilidade na estrutura organizacional, facilitando uma ameaça, causando um incidente.Sêmola (2003), afirma que vulnerabilidades são fragilidades presentes ou associadas a ativos que manipulam e/ou processam dados.

A vulnerabilidade desencadeia outros problemas na segurança como um todo, sendo assim na ilustração abaixo, o que o efeito da vulnerabilidade causa: (Figura 2).

Figura 2 – Vulnerabilidade



Fonte: Laureano(2005)

- **Ativos** são elementos que fazem parte dos processos de manipulação e processamento da informação. Podem ser definidos como ativos: a própria informação, meio que é armazenada, pessoa, tecnologia, sistemas, equipamentos utilizados para manuseá-la, transportá-la, descartá-la e que possua valor Tatiele Zanella(2017).

- **Ataques** são variadas ferramentas que são utilizadas para causar algum tipo de prejuizo ou abrir certas vulnerabilidades nos sistemas que as organizaçoes possuem exemplos de ataques são: Vírus, Engenharia social entre outros Laureano (2005).

3.3 Formas de obtenção de dados

3.3.1 Vírus de computador

É um programa ou trecho de código projetado para danificar seu PC através da corrupção de arquivos do sistema, utilização de recursos, destruição de dados ou sendo, de algum outro modo, um aborrecimento.

Em uma pesquisa realizada por Johnatan Strickland (HOW STUFF WORKS) ele descreve sobre alguns dos maiores virus já catalogados até 2012.

- **Melissa** Seu criador David L. Smith concedeu este nome ao vírus em homenagem a uma dançarina “exótica” do Estado da Flórida, EUA. Desenvolvido com base em uma simples macro do editor de texto Microsoft Word, um dos programas do pacote Microsoft Office, este vírus se espalhava pela internet atacava primeiramente a conta de email da vítima e ao ser aberto fazia cópias de si mesmo e enviava mensagens infectadas para as primeiras 50 pessoas da lista de contato. (JOHNATAN STRICKLAND 2012).

- **Klez** Este worm também se propagava por email realizando cópias de si mesmo. Porém ele podia carregar programas para o sistema operacional e deixá-lo inoperante. Podia também desativar o software antivírus da máquina e se fazer passar pelo mesmo. O mais interessante deste verme é que ao ser enviado ele não precisava utilizar de nomes que seriam desconhecidos para a vítima, mas ele utilizava de um nome da própria lista de contatos infectada, fazendo-se parecer legítimo (JOHNATAN STRICKLAND 2012).

- **I Love You** Criado nas Filipinas esta ameaça na verdade era um worm, pois fazia copias de si mesmo de forma automática. Se propagava também na forma de emails contendo o anexo love-letter-for-you.txt.vbs este programa roubava senhas digitadas pela vítima e 16 as enviava para o cracker que o desenvolveu. Estima-se que este verme causou um prejuízo aproximado de 10 bilhões de dólares. (JOHNATAN STRICKLAND 2012).

3.3.2 Engenharia Social

É um conjunto de técnicas e habilidades utilizadas para induzir as pessoas a revelarem dados confidenciais, que se tornam informações úteis para o fraudador (WHITMAN; MATTORD, 2012), o processo de exploração da fraqueza humana com a finalidade de extrair informações de um funcionário que a princípio precisa mantê-las de maneira privada é conhecido como Engenharia Social (ENGEBRETSON, 2011). É de conhecimento do engenheiro social que mesmo no maior ambiente de segurança que possa existir, há um componente delicado que pode vir a se romper facilmente: o ser humano (MITNICK, SIMON, 2003).

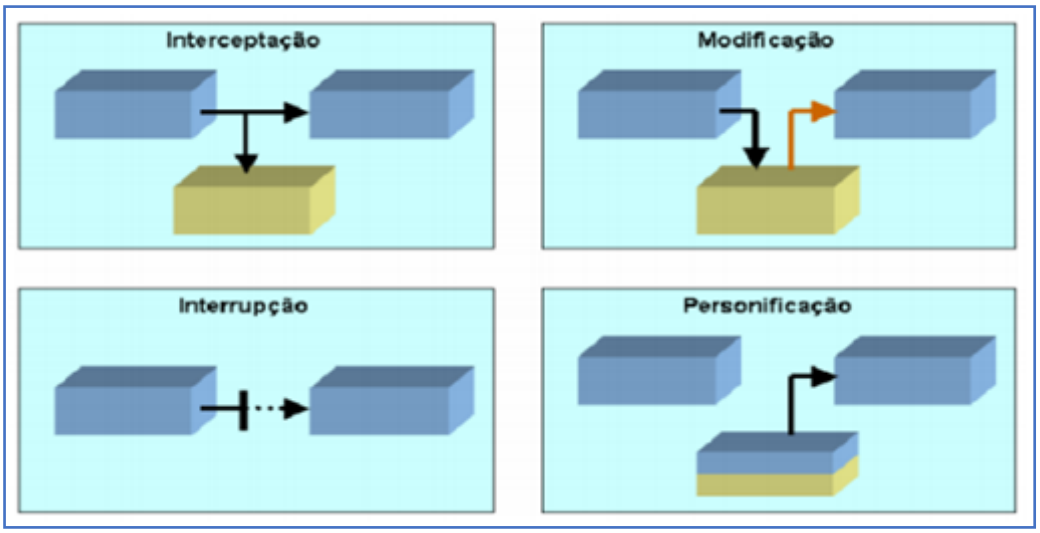
A fragilidade humana no ponto de vista de Workman (2008) está amplamente relacionada com a simpatia e confiança das pessoas, e eventualmente

os indivíduos mais confiantes têm maior probabilidade de submeter-se aos ataques de engenharia social. Mitnick e Simon (2003) esclarecem que faz parte da natureza humana depositar confiança nas pessoas, em especial quando os pedidos não induzem a suspeitas e quando aparentam ser razoáveis, então concientização através de palestras e treinos evitariam certos prejuizos causados pela engenharia social.

De acordo com Laureano (2005), um ataque só terá sucesso dependendo da vulnerabilidade do sistema e das medidas de proteção que ele possui.

Na (Figura 3) é mostrado os tipos de ataques que existem: interrupção, interceptação, modificação e personificação.

Figura 3 – Tipos de Ataques



Fonte: Laureano(2005)

Para Marcos Laureano (2005), interrupção é quando a informação ficará indisponível, não é mais possível acessá-la, interrompendo o fluxo normal da mensagem ao destino. Interceptação é quando informações sigilosas poderão ser visualizadas por pessoas sem autorização. Modificação incide na alteração das informações por pessoas não autorizadas, violação da integridade da mensagem. Personificação define-se como uma pessoa que acessa as informações ou a

transmite se passando por pessoas autênticas, violação da autenticidade.

3.4 Mecanismos de Segurança da Informação

São formas, procedimentos estabelecidos para se criar soluções rapidas e funcionais quando não se ocorre tais procedimentos estaremos o sistema ficará disponivel a ataque maliciosos, existe 3 medidas funcionais antes que são as preventivas, durante o processo que são as medidas detectaveis eas corretivas que funcionam depois do ocorrido.

- **Medidas preventivas**, segundo Sêmola (2003), são medidas cujo objetivo são evitar incidentes que possam acontecer. Visam manter a segurança já implementada que estabeleçam a conduta e a ética da segurança da organização, para fortalecer o que Sêmola descreve existem esses exemplos preventivos: palestras de concientização aos colaboradores tratando desse assunto,servidores de firewall ou mesmo determinados gerenciamento de Rede através do windows server entre outros software.

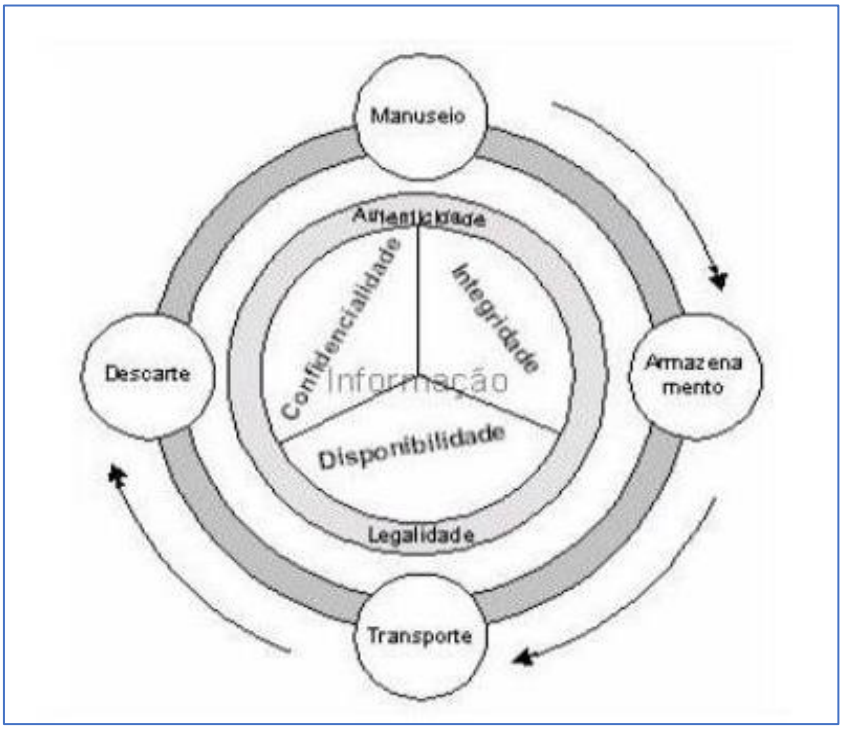
- **Medidas Detectaveis** onde são utilizados determinados softwares que indetificam o causador ou o possivel causador do problema e o gerenciador de redes tomara as determinadas atitudes cabiveis SolarWinds Security Event Manager segudo o site dnsstuff(2020) é considerado o melhor software IDS(intrusion dection system) essa é uma maneira de se indetificar além desse exemplo desenvolvimento de crachas e alarmes irão auxiliar na detectação de pessoas e ações criminosas também.

- **Medidas Corretivas** nesse caso é algo mais minusioso pois se remete a um reconstrução ou reparo de algo a qual ja perdeu sua integridade nesses casos reuniões restritas voltadas a redução dos impactos, backups ou variedades de software de restaurações.

- **Ciclo de Vida da informação** Assim como nós seres humanos que se tem um ciclo de vida e respeita-se ele para se ter total segurança na nossa evolução

assim tambem é a informação os dados a qual a empresa possuem. como na (Figura 4) os 4 ciclos de acordo com SÊMOLA em seu livro Gestão da segurança da informação(2003).

Figura 4 - Quatro momentos do ciclo de vida da informação



Fonte: Sêmola (2003).

- **Manuseio:** abrange a criação ou alteração da informação SÊMOLA (2003).
- **Armazenamento:** quando a informação é armazenada, por exemplo, em um banco de dados, anotações no papel ou arquivo digital SÊMOLA (2003).
- **Transporte**: momento em que a informação é conduzida ou transportada, seja ela por meio eletrônico ou fax SÊMOLA (2003)
- **Descarte:** é o momento quando a informação é descartada, excluída ou inutilizada, como por exemplo, quando um registro, arquivo eletrônico ou papel é excluído SÊMOLA (2003).

Nota-se que um ciclo de vida da informação sendo respeitado de acordo o

conceito de proteção dos dados.enquanto os dados estiverem ativos para uma empresa não trará nenhum tipo de prejuizo. A informação ainda precisa chegar ao fim de seu ciclo o mais adequado possivel, novamente, armazená-la de forma protegida e com acesso restrito, ainda que o arquivo seja ? morto?(João Castilho 2013).

Abaixo consta alguns exemplos de empresas que sofreram alguns ataques trazendo prejuizos a si e também a todos que de certa forma são vinculados a ela seja investidores, clientes ou colaboradores:

Em agosto de 2013, o Yahoo teve o maior vazamento de dados da história onde afirma que dados associados a mais de um bilhão de contas de usuários foram roubados, entre eles, nomes, endereços de e-mail, números telefônicos, datas de nascimento e senhas criptografadas (COMPUTERWORLD, 2016).

Também em 2013, mais de 4,6 milhões de usuários do aplicativo Snapchat receberam uma notificação de que seus números de celulares e localização foram divulgados sem suas permissões (LANDIM, 2014).

Outra brecha na base de dados da T-Mobile nos EUA ocasionou a exposição de dados de 15 milhões de consumidores norte-americanos ligados à operadora entre setembro de 2013 e setembro de 2015. Foram roubadas informações pessoais como nomes, endereços, números do Seguro Social, número de carteira de motorista e outros (COMPUTERWORLD, 2015).

Entre 2006 e 2008, a empresa Heartland especializada em pagamentos, sofreu um problema de SQL Injections (códigos que se comunicam diretamente com o banco de dados), onde permitiu aos crackers roubarem dados de pagamento de aproximadamente 130 milhões de cartões de crédito e débito.

O roubo de 5,6 milhões de números de cartões de crédito da Visa e da MasterCard de uma administradora de cartões americana, em fevereiro de 2003.

4 Violação de Dados

Caracterização uma violação dos dados quando uma determinada empresa ou organização sofre um incidente de segurança em questão dos dados pelo a empresa é responsável, uma violação ela atingi todos os pontos da tríade de segurança que é confidencialidade, disponibilidade e integridade Mateus Mello Garrute (2020).

Se a violação foi suscetível a ponto de causar riscos para os direitos e as liberdades das pessoas envolvidas, a empresa deverá apresentar notificações às autoridades de controle com no máximo um prazo de 72 horas após ter o conhecimento da violação, mesmo que o incidente tenha resultando apenas na visibilidade dos dados a terceiros, já ocorreu a violação na segurança a que se refere a lei Mateus Mello Garrute (2020).

Assim, a empresa ou organização deve garantir a minimização dos danos causados e responder satisfatoriamente as expectativas dos interessados e da sociedade. As informações pessoais protegidas pela lei são aquelas determinadas ou determináveis.

Ou seja, quaisquer dados que permitam a identificação de uma pessoa natural ou os tornem possíveis, tais como: Nome, Sobrenome, E-mail, Numeração de documentos e de cartões de crédito, Dados bancários, Informações médicas, Localização , Endereços de IP;E os chamados “testemunhos de conexão”, mais conhecidos como *cookies* então esses tipos de violação você poderá exigir através das autoridades seus direitos instituídos Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016

5 SEGURANÇA NO AMBIENTE CORPORATIVO.

Hoje existe uma grande quantidade de dispositivos ativos nas empresa com a inserção dos Smartphones, sendo assim soluções básicas são importantes e bem vindas para diminuir ataques de curiosos ou de verdadeiros bandidos cibernéticos que podem e poderão causar dano a rede, alguns dessas soluções são: Criptografia, Modificação de Senhas, Utilizações de software protetivos entre outros (Atalla Neto 2017).

- **Criptografia**: é o mínimo mais efetivo, quando o invasor não possue tanta experiencia no que esta fazendo existem metodos com WPA3(Wifi protected access) e AES (Advanced encryption standard) que podem criar chaves criptograficas de 256 bits o que dificulta o acesso indevido.(Priscilla Kinast 2019).

- **Mudança de senha padrão dos respectivos dispositivos**: os modelos de dispositivos sem fio vêm com senhas padrões de acesso, que qualquer cracker iniciante pode quebrar, por 33 isso é preciso alterar esta senha logo na instalação do aparelho, para evitar possíveis invasões Antonio Njaim(2013).

- **Limitação de endereços IP**: ao configurar tal roteador ou ponto de acesso, é recomendado limitar o número de endereços IP que serão distribuídos nessa rede. Por exemplo, se serão somente quatro computadores que acessarão esta rede, não é necessário deixar a distribuição de endereços IP até 200 possíveis, que é o padrão de fábrica do dispositivo. É interessante também configurar um filtro de endereços IP, permitindo ou negando certos IPs ao acesso a determinadas portas ou sítios da internet Antonio Njaim(2013).

- **Utilizar firewall**: é bom a utilização de um hardware ou software de firewall, como o Zone Alarm, McAfee e Norton, que aumentará ainda mais a segurança desta rede Antonio Njaim(2013).

- **Intensidade do alcance de sinal(wire-less)**: Através do gerenciamento dos roteadores é possível limitar a área de abrangência do sinal fazendo com que só pessoas do setor proprio da empresa tenha acesso ao sinal ofertado Antonio Njaim(2013).

- **Atualizações**: vemos em muitos locais a imaturidade quando o quesito é atualizações mas novas atualizações são extremamente importante não só do sistema operacional, mas roteadores e softwares então atualizações de firmware são básicas mas podem trazer grandes benefícios Flavia Dutra (2020).

6 TÉCNICAS DE DEFESA UTILIZADAS NA PROTEÇÃO DOS DADOS

6.1 Heurística

Origina do grego Heuriskein, que significa descobrir é uma tecnologia projetada para detectar códigos maliciosos e tomar soluções rapidas, a solução de segurança analisa um arquivo e compara o seu comportamento com certos padrões que podem indicar a presença de uma ameaça.

Segundo (Fabrício Teixeira, 2016) é um procedimento simplificador (embora não simplista) que, em face de questões difíceis envolve a substituição destas por outras de resolução mais fácil a fim de encontrar respostas viáveis, ainda que imperfeitas. Tal procedimento pode ser tanto uma técnica deliberada de resolução de problemas, como uma operação de comportamento automática, intuitiva e inconsciente.

6.2 Removedor de Propagandas

São softwares geralmente gratuitos que auxiliam para que adwares não entrem em seu computador ou celular sem autorização pois na maioria das vezes entram em seu dispositivo sem autorização causando certa lentidão e também são difices de desistalar, existem software como adwcleaner que ajuda na remoção de adwares Antonio Njaim(2013).

6.3 Software Antispyware

Antispyware é um script ou programa para a remoção de um ou mais spywares de uma máquina ou rede. A questão é que, por vezes, a remoção de um spyware exige um protocolo específico Hugo Bär(2017).

O antispyware é desenvolvido para detectar códigos espiões ou spywares quando tentam realizar alterações em arquivos de registro do sistema operacional. Também trabalham com sistema de base de dados com ameaças conhecidas catalogadas em seu banco por isso precisam se manter atualizados para detecção

de novas possíveis ameaças. Antonio Njaim(2013).

7 Formas Seguras de transmissão e compartilhamento de dados

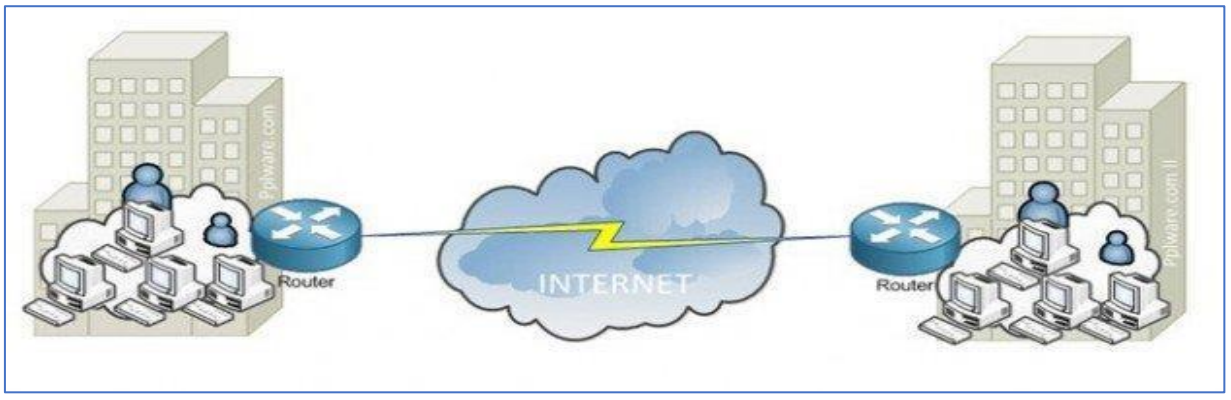
7.1 VPN (REDE VIRTUAL PRIVADA)

Segundo (MAGALHÃES, 2002) Esta forma de transmissão e compartilhamento de informações é uma solução bastante eficaz para a empresa ou determinado grupo de empresas que desejam obter mais segurança em sua rede de computadores estando eles no mesmo ambiente físico ou não porém a VPN não disponibiliza um alto nível de confiabilidade e segurança para com as informações que transitam por ele.

Segundo o site Canaltech (Pedro Cipoli, 2020) afirma que por meio da criptografia nas informações e nas comunicações entre hosts da rede privada é possível aumentar a confidenciabilidade dos dados que trafegam pela rede. Por meio do sistema de tunelamento, os dados podem ser enviados sem que outros usuários tenham acesso, e mesmo que os tenham, ainda os receberão criptografados. Por isso, é fundamental que os dispositivos responsáveis por cuidar da rede VPN devem ser capazes de garantir segurança e integridade das informações e dos dados que são transmitidos.

como exemplo de VPN (Figura 5):

Figura 5- VPN



Fonte : Pedro Cipoli (2012)

Conhecendo VPN é importante relatar o que é o IPSec (IP Security Protocol) Segundo o (Pedro Cipoli 2012) Essa ferramenta permite que todos os dados passem pelo gateway para serem cifrados antes de percorrerem o caminho para a máquina de destino ou decifrado antes do recebimento dos dados.

Ricardo Dahab(2003) relata que O IPSec integra mecanismos de autenticação, gestão e distribuição de chaves o IPSec utiliza o conceito de Associação de Segurança (Security Asociation - SA), que permite a comunicação entre duas ou mais entidades comunicantes e descreve todos os mecanismos de segurança a serem utilizados e essa flexibilidade permite que sejam utilizadas sempre as normas mais recentes disponíveis, incrementando ainda mais a segurança.

A VPN, portanto, é mais uma possível solução para aumentar a segurança principalmente nos casos onde há várias redes em diferentes pontos que se interligam e compartilham informações, devendo somente o administrador da rede atentar para questões como velocidade e largura de banda disponível para tal aplicação ser executada sem gerar atrasos e prováveis perdas para a empresa(Antonio Njaim, 2013).

7.2 Link Dedicado

Um link dedicado é uma solução feita especialmente para corporações que precisam de maior garantia e estabilidade em termos de conexão tanto entre si como na web, a sua característica é disponibilidade ininterrupta 24 horas por dia, e sete dias por semana.(Telium Networks 2018).

Segundo Telium Networks 2018 um empresa ao ter link dedicado ela garante mais segurança e desempenho nas suas funcionalidades alguns beneficios dessa tecnologia Confiabilidade ,Maior escalabilidade, Suporte adequado e otimizado, Melhor qualidade no acesso à internet, Facilidade no monitoramento do tráfego de dados , Diminuição de perdas de arquivos e dados, Dispositivos tecnológicos atualizados e de ponta (Telium Networks 2018).

8 Características de segurança com o controle da ISO/IEC.

8.1 ISO/IEC 27001

De acordo com o site Stefanini (2019), um Sistema de Gestão de Segurança é uma ferramenta corporativa para abordagem organizacional da questão. Implementá-lo significa adotar estratégias, políticas, planos, controles, medidas e diversos outros mecanismos de **gestão**. Sua estrutura pode ser elaborada de acordo com a norma ISO 27001.

A ISO 27001 é um padrão para sistema de gestão da segurança da informação publicado em outubro de 2005 pela ISO(International Organization for Standardization) aborda os dados baseados em PDCA(Plan-Do-Check-Act), em suas diretivas da ISO/IEC são descritas no anexo SL como as normas devem ser estruturadas.

> Com o crescimento constante da tecnologia da informação houve uma necessidade urgente de medidas de segurança adequadas à informação. Assim a International Standardization Organization (ISO) publicou a ISO/IEC, uma norma internacional de gestão de segurança da informação que se tornou uma das iniciativas mais importantes para o gerenciamento de T.I, Washington Almeida(2020).

Ela descreve como colocar em prática um sistema de gestão de segurança da informação avaliado e certificado de forma independente. Permitindo assim que os dados financeiros e confidenciais sejam protegidos de forma mais efetiva, reduzindo a probabilidade de ataques e acessos ilegais ou não permitidos.

A ISO/IEC 27001 identifica riscos e define os controles para o gerenciamento ou eliminação dos mesmos e flexibiliza a adaptação dos controles às áreas da empresa.

Ela pode ser implementada em qualquer tipo de organização provendo metodologias para a implementação da gestão da segurança da informação em

uma organização e possibilita que organizações obtenham certificação confirmando a implementação da segurança da informação e dos dados em conformidade com a ISO/IEC 27001.

A ISO/IEC 27001 tem como filosofia a gestão de riscos: descobrir onde os riscos estão, e então tratá-los sistematicamente:

Os controles que são implementados em geral estão na forma de políticas, procedimentos e implementações técnicas.

8.2 ISO/IEC 27002

Em meio a um cenário onde empresas sentem a necessidade de buscar uma estruturação dos processos internos para garantir a segurança de seus negócios contra os vários tipos de ameaças virtuais, surgiu a norma internacional NBR ISO/IEC o qual tem como objetivo a boa prática para a gestão da segurança da informação.

Ela consolida conhecimentos necessários para quem busca estruturar sistemas de gestão da segurança da informação (SGSI). A ISO/IEC 27002 é um código de Práticas para a Gestão de Segurança Da Informação, estabelecendo diretrizes e princípios gerais para iniciar, implementar e melhorar a gestão da informação em organizações.

Anteriormente denominada como ISO/ IEC 17799 em 2005 foi incorporada ao novo esquema de numeração como ISSO/IEC 27002. A norma tem como intuito descrever como os controles na implementação em sistemas de gestão de segurança na informação podem ser estabelecidos.

Com o aumento da interconectividade a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ABNT NBR ISO/IEC 27002).

> A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, e recomendado que ela seja sempre protegida adequadamente (ABNT NBR ISO/IEC 27002; Bernard, 2007).

Com isso, foram desenvolvidos três elementos básicos para que a segurança da informação possa ser estabelecida e seguida, de forma que apenas os responsáveis pelos dados passados possam acessá-los e alterá-los. (Ramos et al., 2008; Miller e Murphy, 2009).

9 GDPR

Para que uma sociedade se mantenha em ordem é necessário que seus indivíduos tenham direitos e deveres pré-estabelecidos (Docusign 2018). Com isso, a implementação e cumprimento de normas funcionam como um tipo de garantia de que cidadãos e órgãos institucionais continuem em conformidade e equilíbrio.

Como Descrito no portal Docusign(2018) , o GDPR trata-se de um conjunto de regras que servem para normalizar as praticas de uso de informações consideradas adequadas no ambiente de trabalho. Ela faz parte de um grupo de iniciativas que tem como ponto principal fortalecer a ideia de cidadania digital. Podendo ser entendido como manuseio responsável da tecnologia por pessoa física ou corporação o conceito relaciona-se diretamente aos exercícios e cumprimento dos direitos e deveres.

De acordo com o portal Docusign(2018) a GDPR tem como finalidade preencher lacunas da segurança ao cidadão digital, pois mesmo que diversas atividades sejam executadas no meio eletrônico como compras e vendas, algumas delas não estão completamente regulamentadas.

Criada em 2012 e aprovada em 2016 o GDPR está sendo implementado pelos países da União Europeia . Trata-se de um conjunto de leis que assegura o manuseio de informações pessoais em plataformas online. É um grande regulatório de uso de dados pessoais no universo virtual, Valéria Reani(2018).

Em 25 de maio de 2018 entrou em vigor na União Europeia o GDPR (Regulamento Geral sobre Proteção de dados). Como explica o site Docusign(2018) a GDPR visa proteger os dados dos cidadãos e evitar que sejam utilizados sem seu consentimento. É uma legislação que da as pessoas o máximo de segurança da privacidade.

O GDPR tem impactado direto nas relações de serviço e comerciais entre empresas, por meio de mecanismos inteligentes. De modo geral o direito é restrito ao território onde foi implementado, ou seja, as leis de um país só podem ser aplicadas em seu território, se um infrator descumpri-la fora da área de jurisdição o mesmo não poderá ser penalizado.(Peduti Advogados, 2019)

Porém, nesse caso, bastaria as empresas saírem do território da União Europeia para fugir da aplicação da lei.(Peduti Advogados, 2019) Por isso o GDPR foi construído, para ser aplicado como um todo, caso uma empresa europeia contrate uma empresa estrangeira que viole o GDPR , a autoridade não irá penalizar a empresa estrangeira(por estar fora do território), mas a empresa europeia será responsabilizada legalmente pela violação promovida pela empresa que contratou.

Dessa forma a união Europeia garante que o GDPR será cumprido, mesmo fora do território europeu, tornando-se assim uma legislação "mundial" (Docusign, 2018). Com isso, todo aquele que possui acesso a dados de cidadãos, empresas e/ou governos europeus esta sujeito a ele.

10 LGPD

No mundo contemporâneo, com o crescimento no desenvolvimento tecnológico, houve uma grande carência na segurança e proteção de dados. Após o vazamento e perda de dados de várias empresas de grande porte e até do governo, foi descoberta uma certa vulnerabilidade na segurança da informação, (Scielo 2007) vulnerabilidade essa ao qual tornou a espionagem corporativa e ataques de crackers mais acessível.

Com isso, em 2018 a Lei Geral de Proteção de Dados Pessoais(LGPD n° 13.709), foi desenvolvida e então sancionada pelo ex-presidente Michel Temer. Essa lei tem como intuito regulamentar o tratamento de dados pessoais de usuários e clientes por parte de empresas públicas e privadas. (PASSARELI, 2019)

Em 2019, ao pesquisar a fundo sobre a transferência Internacional de dados pessoais englobada pela Lei Geral da Proteção de Dados, VIEIRA(2019) encontrou uma lacuna legislativa nas leis brasileiras em relação a proteção e transferência Internacional de dados pessoais que foi sanada com a criação da LGPD.

A lei 13.709, de 14 de agosto de 2018 Art.1° dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A LGPD traz consigo novas concepções jurídicas definindo as circunstâncias em que os dados pessoais podem ser tratados, determina inúmeros direitos para os proprietários dos dados e desenvolve vários procedimentos e normas para que não corra o risco de vazamento de dados.

Rodrigues (2019) buscou estudar e explorar a segurança da informação sobre a ótica das principais normas que regem o que já é realidade no mercado europeu e o qual será possível em abril de 2021 em todo o território brasileiro.

O artigo segundo da LGPD dispõe sobre os fundamentos da legislação, tratando de seus apoios, das bases sob a disciplina da proteção de dados. A LGPD pautou sete fundamentos que alicerçam a proteção de dados pessoais, citados a seguir.

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade;

i. - a autodeterminação informativa;

ii.- a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da

imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

11 CONSIDERAÇÕES FINAIS

Os resultados finais que obtivemos pegando a base de dados das empresas citadas é que ignorar a segurança não farão eles sumirem ou algo do gênero, mas pelo contrário observamos que independente do seu porte todas as empresas que estão diretamente ligadas aos seus ativos de dados ou software ou hardware, devem implementar mecanismos de segurança para minimizar os incidentes e quando ocorrerem não sejam graves, ainda percebemos que existe também a necessidade dos colaboradores serem treinados, observados e orientados para determinada segurança e controle total do mesmo.

Implementação de segurança visa simplesmente conter as ameaças e vulnerabilidades que os ativos por natureza possuem, dessa forma foram citadas algumas formas de mecanismos de defesa ao longo dos capítulos.

Após essas implementações todos os colaboradores e gestores podem observar que necessidade existe para se dar a atenção a importância da segurança da informação no âmbito corporativo.

Apesar de ainda sim possuir certa resistência e falta de maturidade para aceitar as exigências o retorno é bem positivo entre as pequenas, medias e grandes empresas.

Além das ferramentas e instruções dadas também sugerimos melhorias e adequações para uso das mesmas, nosso intuito é incentivar o uso de ferramentas distintas, mas funcionais pois vivemos em uma era cibernética onde constantes atualizações são feitas dia após dia e novas tecnologias surgem e com isso nasce também a necessidade de novos e mais eficientes meios de segurança para suprir as necessidades dos usuários

12 REFERÊNCIAS

ABNT NBR ISO/IEC 27002 – Tecnologia da informação – **Técnicas de segurança** – Código de prática para a gestão de segurança da informação,2007.

COMO IMPLEMENTAR AS REGULAMENTAÇÕES DA GDPR. Fevereiro 8, 2019. Disponível em: < https://peduti.com.br/blog/como-implementar-gdpr/> Acesso em 19 de março se 2020.

COMPUTEREORLD. **Vazamento na Experian expõe dados de 15 milhões de consumidores nos EUA**. Out. 2015. Disponível em :< https://computerworld.com.br/2015/10/02/vazamento-na-experian-expoe-dados-de-15-milhoes-de-consumidores-nos-eua/> . Acesso em: 17 de maio de 2020.

Fernando Palma CID **Confidencialidade integridade e disponibilidade**. Dezembro de 2016.

FONTES, Edison. **Segurança da Informação: O Usuário faz a diferença**. São Paulo: Saraiva, 2006.

GALVÃO, Michele da Costa. **Fundamentos em Segurança da Informação**. São Paulo: Person Education do Brasil, 2015.

GDPR: entenda o que é o Regulamento Geral de Proteção de Dados. 20 de dezembro de 2018. Disponível em:< https://www.docusign.com.br/blog/gdpr-entenda-o-que-e-o-regulamento-geral-de-protecao-de-dados/ > Acessado em 17 de Março de 2020.

Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. 31 de outubro de 2007. Disponível em

https://www.scielo.br/scielo.php?pid=S180717752007000300007&script=sci_arttext&tlng=pt. Acesso em 17 de maio de 2020.

LANDIM, Wikerson. **Snapchat é hackeado e dados de 4,6 milhões de usuários são expostos.** Janeiro de 2014. Disponívelem:<https://www.tecmundo.com.br/ataque-hacker/48625-snapchat-e-hackeado-e-dados-de-4-6-milhoes-de-usuarios-sao- expostos.htm> Acesso em: 08 de março de 2020.

LAUREANO, Marcos Aurelio Pchek.Gestão de **Segurança da Informação**, <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf> 2005. Acesso em:05 de junho 2020.

MACÊDO, Diego. **Modelos e mecanismos de segurança da informação**, 2014. Disponível em: <https://www.diegomacedo.com.> Acesso em 11 de Março de 2020

Mitnick K, Simon W. The art of deception. Indianapolis. Wiley. 2002.

Ramos A, Bastos A, Lyra A, Andrucioli A, Affonso C, Poggi E, Pinto E, Blum RO, Alevate W, Marinho Z. Security officer – **guia oficial para formação de gestores em segurança da informação**. 2th ed. Porto Alegre: Zouk,2008

NBR ISO/IEC 27002 – **Tecnologia da Informação** – **Técnicas de segurança**

OLIVEIRA, Wilson José de. Segurança da Informação: **Técnicas e Soluções**. Florianópolis: Visual Books Ltda, 2001.

Os critérios da informação pela perspectiva da segurança. Dezembro de 2016. Disponível em: <https://www.portalgsti.com.br/2016/11/cid-confidencialidadeintegridade-e-disponibilidade.html>

PASSARELLI, Vinícius**. LGPD: entenda o que é a Lei Geral de Proteção de Dados Pessoais.** 31 de maio de 2019. Disponível em

https://politica.estadao.com.br/blogs/fausto-macedo/lgpd-entenda-o-que-e-a-lei-geral-de-protecao-de-dados-pessoais/. Acesso em 17 de maio de 2020.

Regulamento Geral sobre a Proteção de Dados. 26 de abril de 2018. Disponível em:

RODRIGUES, T. F. **Análise do sistema de segurança da informação da empresa ndd. Repositórios de relatórios- Engenharia de Produção**, n. 1, 2019.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**, **uma visão Executiva.** Rio de Janeiro: Elsevier, 2003.

STALLINGS, William. **Criptografia e segurança de redes**. São Paulo: Pearson Prentice Hall, 2008.

STEFANINI. **Você sabe o que é a gestão em segurança da informação?**, 2019. Disponível em: <https://stefanini.com/pt-br/trends/artigos/gestao-em-seguranca-da-informacao> br/modelos-e-mecanismos-de-seguranca-da-informacao/>. Acesso em: 11 de junho 2020.

TATEOKI, V. A. **A proteção de dados pessoais e a publicidade comportamental.** Revista Juris UniToledo, v. 2, n. 01, 2017.

VIEIRA, V. R. N. **Lei Geral de Proteção de Dados:Uma análise da tutela dos dados pessoais em casos de transferência internacional**. 2019. 77 f. Trabalho de Conclusão de Curso (Graduação em Direito) –Universidade Federal de Uberlândia, Uberlândia, 2019.