



UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE GRADUAÇÃO
CENTRO MULTIDISCIPLINAR DE ANGICOS
CURSO INTERDISCIPLINAR EM CIÊNCIA E TECNOLOGIA

FRANCISCO PHELIPE ALVES DA CRUZ

SEGURANÇA DA INFORMAÇÃO EM REDES DE CORPORAÇÕES PÚBLICAS

ANGICOS/RN
2022

FRANCISCO PHELIPE ALVES DA CRUZ

SEGURANÇA DA INFORMAÇÃO EM REDES DE CORPORAÇÕES PÚBLICAS

Trabalho de Conclusão de Curso apresentado a Universidade Federal Rural do Semiárido - UFERSA, como requisito parcial para a obtenção do título de Bacharel em Ciência e Tecnologia.

Orientador: Prof. Dr. Rafael da Costa Ferreira

© Todos os direitos estão reservados a Universidade Federal Rural do Semi-Árido. O conteúdo desta obra é de inteira responsabilidade do (a) autor (a), sendo o mesmo, passível de sanções administrativas ou penais, caso sejam infringidas as leis que regulamentam a Propriedade Intelectual, respectivamente, Patentes: Lei nº 9.279/1996 e Direitos Autorais: Lei nº 9.610/1998. O conteúdo desta obra tomar-se-á de domínio público após a data de defesa e homologação da sua respectiva ata. A mesma poderá servir de base literária para novas pesquisas, desde que a obra e seu (a) respectivo (a) autor (a) sejam devidamente citados e mencionados os seus créditos bibliográficos.

C957s Cruz, Franciso Phelipe Alves da.
Segurança da informação em redes de corporações
públicas / Franciso Phelipe Alves da Cruz. - 2022.
45 f. : il.

Orientador: Rafael da Costa Ferreira .
Monografia (graduação) - Universidade Federal
Rural do Semi-árido, Curso de Ciência e
Tecnologia, 2022.

1. Política de segurança. 2. Ameaças vituais. 3.
Sistema de segurança. 4. Dispositivos físicos. I. ,
Rafael da Costa Ferreira, orient. II. Título.

Ficha catalográfica elaborada por sistema gerador automático em conformidade
com AACR2 e os dados fornecidos pelo(a) autor(a).

Biblioteca Campus Angicos
Bibliotecário: Helder Romero Maia Duarte
CRB: 15/673

O serviço de Geração Automática de Ficha Catalográfica para Trabalhos de Conclusão de Curso (TCC's) foi desenvolvido pelo Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (USP) e gentilmente cedido para o Sistema de Bibliotecas da Universidade Federal Rural do Semi-Árido (SISBI-UFERSA), sendo customizado pela Superintendência de Tecnologia da Informação e Comunicação (SUTIC) sob orientação dos bibliotecários da instituição para ser adaptado às necessidades dos alunos dos Cursos de Graduação e Programas de Pós-Graduação da Universidade.

FRANCISCO PHELIPE ALVES DA CRUZ

SEGURANÇA DA INFORMAÇÃO EM REDES DE CORPORAÇÕES PÚBLICAS

Trabalho de Conclusão de Curso apresentado a Universidade Federal Rural do Semiárido - UFERSA, como requisito parcial para a obtenção do título de Bacharel em Ciência e Tecnologia.

Defendida em: 15 / 06 / 2022.

BANCA EXAMINADORA

Rafael da Costa Ferreira, Prof. Dr. (UFERSA/Campus Angicos)
Presidente

Geomar Galdino da Silva, Prof. Dr. (UFERSA/Campus Angicos)
Membro Examinador

Maristelio da Cruz Costa, Prof. Dr. (UFERSA/Campus Angicos)
Membro Examinador

AGRADECIMENTOS

Em forma de gratidão agradeço à minha família, pela sua esperança de acreditar e investir em mim. Mãe, sua orientação e dedicação foi o que deu, em alguns momentos, a força que precisei para seguir. Pai, sua presença significou segurança e certeza de que não estou sozinho nessa caminhada, as minhas amigadas pela sutileza em manter o controle da situação onde eu achava que estava tudo virado ao avesso e principalmente, motivar que tudo é fase e no final tudo vai dá certo, agradeço ainda a UFERSA por fazer parte da minha evolução acadêmica, necessário para adquirir todo conhecimento para estar onde estou. A dedicação da família que se fez presente nas orientações importantes para a conclusão deste TCC.

*“Você pode encarar um erro como uma besteira a ser esquecida,
ou como um resultado que aponta uma nova direção. ”*

Steve Jobs

DEDICATÓRIA

Dedico esse trabalho de conclusão de curso primeiramente ao pai criador de tudo, que me deu o dom da vida e a honra de estar presente nesse momento de conquista, dedico também aos meus pais e toda minha família por me educar e ensinar os bons modos, sem eles eu não seria capaz de me estabilizar em um momento impar no meu aprendizado. Dedico em forma de agradecimento a UFERSA/SISU por abrilhantar meu potencial ao me selecionar para cursar o referente curso e por disponibilizar o processo seletivo que me foi submetido.

RESUMO

Devido à grande gama da tecnologia da informação em ascensão, o direcionamento da segurança de informações é um fator primordial e se faz importante numa rede corporativa, tanto privada quanto pública, o que explica a iniciativa da elaboração desta pesquisa. O monitoramento da rede de comunicação é um dos pilares da segurança da informação, dando confiabilidade no processamento de dados importantes e sigilosos que são compartilhados e acessados ao tempo todo. Os dados consequentemente se tornaram os mais importantes patrimônios de uma empresa, sendo um fundamento para as mesmas que desejam se manter ativa no mercado. Em uma época na qual o conhecimento e a informação são fatores de suma importância para qualquer organização, a Segurança da Informação é um pré-requisito que serve como subsídio para todo e qualquer sistema de informação, o que justifica a elaboração deste estudo. Nos dias atuais tudo pode ser feito por meio da internet, nossas informações correm nas redes em milésimos de segundos. Devido a essas trocas de informações foram criados vários meios de segurança para impedir alguém, que não seja a origem e o destino, tenha acesso as informações transmitidas. Mesmo com a tecnologia avançando e procurando meios de aumentar essa segurança, sempre existirão novas ameaças. Além dos métodos de prevenções, detecções e contra respostas no objetivo de sempre manter a ordem no andamento do serviço da rede corporativa, empresas fazem o uso de uma política de segurança em forma de relatório com a finalidade de direcionar todo o efetivo num possível sinistro, assim como prevenção para que não chegue a acontecer o problema, tanto para dispositivos físicos e estrutural, como para conteúdos digitais, além do mais o Disaster Recovery complementa a política de segurança da informação no âmbito de ser uma ferramenta responsável por voltar à normalidade as atividades após um desastre físico ou digital, trabalhando conjunto a antivírus que é um programa primordial na detecção e remoção das ameaças, assim como analisadores de tráfegos e vulnerabilidade.

Palavras-chave: Monitoramento de Rede. Política de Segurança. Dispositivos Físicos. Conteudos Digitais.

ABSTRACT

Due to the wide range of information technology on the rise, the direction of information security is a key factor and is important in a corporate network, which explains the initiative of this research. Network monitoring is one of the pillars of information security, giving reliability in the processing of sensitive and sensitive data that is always shared and accessed. The data have consequently become the most important assets of a company, being a basis for those who wish to remain active in the market. In an era in which knowledge and information are of paramount importance to any organization, Information Security is a prerequisite that serves as a subsidy for all information systems, which justifies the preparation of this study. In the present day everything can be done through the internet, our information runs on the networks in milliseconds. Due to these exchanges of information, various means of security have been created to prevent anyone, other than the origin and the destination, from having access to the information transmitted. Even with technology advancing and looking for ways to increase security, there will always be new threats. In addition to the methods of prevention, detection and counter-answers in order to always keep order in the progress of the service of the corporate network, companies use a security policy in the form of a report with the purpose of directing all the staff in a possible accident, as well as prevention so that the problem does not happen, for physical and structural devices as well as for digital contents, besides the disaster recovery complements the information security policy in the scope of being a tool responsible for returning to normality the activities after a physical or digital disaster, working together the antivirus that is a primary program in the detection and removal of threats, as well as traffic analyzers and vulnerability.

Keywords: Network Monitoring. Security policy. Physical Devices. Digital Contents.

LISTA DE FIGURAS

Figura 1 – Pastas infectadas.....	22
Figura 2 – Malware worms infiltrado no sistema.....	23
Figura 3 – Trojan encontrado num executável	24
Figura 4 – Keyloggers em execução	25
Figura 5 – Adwares camuflado em propagandas.....	26
Figura 6 – Hijackers no navegador.....	27
Figura 7 – E-mail infectado	29
Figura 8 – Pagamento da criptomoeda	30
Figura 9 – Phishing contra usuário	31
Figura 10 – Wireshark analisando portas vulnerável	36
Figura 11 – Ilustração do firewall.....	37
Figura 12 – Criptografia de um arquivo	38

LISTA DE ACRÔNIMOS

Link	Elemento de hipermídia formado por frases
Software	Programas de computadores
Hacker	Usuário com grande conhecimento de informática
Malware	Vírus digitais que infectam máquinas
Prompt	Ferramenta de serviços internos do sistema operacional
Cracker	Usuário que usa o conhecimento de informática para intenções mal-intencionadas
Flash	Reprodutor multimídia
Fake	Nome usado para coisas falsas
Linux	Sistema Operacional
Hub	Dispositivo concentrador de rede
Switch	Dispositivo distribuidor de pacotes nas redes
Webs	Páginas de internet com conteúdos digitais

LISTA DE SIGLAS

IP	Internet Protocol (Protocolo de Internet)
VoIP	Voice Over Internet Protocol (Voz Sobre Protocolo de Internet)
PC	Personal Computer (Computador Pessoal)
TCP	Transmission Control Protocol (Protocolo de Controle de Transmissão)
UDP	User Datagram Protocol (Protocolo de Datagrama do Usuário)
URL	Uniform Resource Locator (Localizador Padrão de Recursos)
PhD	Philosophy of Doctor (Doutor de Filosofia)
PSI	Política de Segurança da Informação
TI	Tecnologia da Informação
HTTP	HyperText Transfer Protocol (Protocolo de Transferência de Hipertexto)
DR	Disaster Recovery (Restauração de Desastre)

SUMÁRIO

1 INTRODUÇÃO.....	15
2 REFERENCIAL TEÓRICO.....	17
2.1 CONCEITO INICIAL A SEGURANÇA DA INFORMAÇÃO.....	17
2.1.1. INTEGRIDADE	17
2.1.2. CONFIDENCIALIDADE	17
2.1.3. DISPONIBILIDADE.....	17
2.2 ESTRATEGIA DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO PÚBLICA.....	18
2.3 IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO NO AMBIENTE EMPRESSARIAL PÚBLICO.....	19
2.3.1. CONCIENTIZAÇÃO	20
2.3.2. GERENCIAMENTO DE CRISES	20
2.3.3. FUNCIONALIDADE DE SISTEMAS E PRIVACIDADES	21
2.4 AMEAÇAS.....	21
2.4.1. VÍRUS	21
2.4.2. WORMS	22
2.4.3. TROJANHORSE (CAVALO DE TRÓIA).....	23
2.4.4. KEYLOGGERS	24
2.4.4.1. SCREENLOGGERS	25
2.4.5. SPYWARE.....	25
2.4.5.1. ADWARES	26
2.4.5.2. SPAMS	27
2.4.6. HIJACKERS	27
2.4.7. RANSOMWARE.....	28
2.4.7.1. MONEY, UKASH E PAYSAFE	29
2.4.7.2. BITCOIN	29
2.5 PHISHING DENTRO DA INSTITUIÇÃO PÚBLICA.....	30
2.6 POLÍTICAS DE SEGURANÇAS DAS INFORMAÇÕES – PSI.....	32
2.6.1. DAS RESPONSABILIDADES.....	32
2.6.1.1. DATA CENTER.....	33
2.6.1.2. BACKUP	33
2.6.1.3. REDUNDÂNCIA	34
2.7 AÇÕES PARA A SEGURANÇA DA INFORMAÇÃO	34

2.7.1. FERRAMENTAS DE PREVENÇÕES	35
2.7.1.1. WIRESHARK	35
2.7.1.2. FIREWALL	36
2.7.1.3. CRIPTOGRAFIA	37
2.7.1.4. ASSINATURA DIGITAL	38
2.7.2. FERRAMENTAS DE DETECÇÕES	39
2.7.2.1. ANTIVÍRUS	39
2.8 A SÉRIE DE PREPARAÇÃO CORPORATIVA DO MARCO CIVIL DA INTERNET SETOR PÚBLICO	41
3 METODOLOGIA	42
4 CONSIDERAÇÕES FINAIS	43
5 REFERÊNCIAS BIBLIOGRÁFICAS.....	44

1 INTRODUÇÃO

No atual cenário mundial onde a tecnologia se encaixa como uns dos pilares de uma boa convivência, são aplicados a ela uma facilidade de se entreter e participar de diversas atividades ligado as informações. Algumas dessas são expressivas ao contato virtual, como por exemplo as redes sociais, e-mails, voz sobre IP, tendo à aproximação com diversas pessoas de todos os cantos do mundo, fator esse primordial para pessoas mal-intencionadas com interesses de tomar pose de alguns dados importantes para uma ocasião.

O grande acesso as informações de certo modo são facilitadas quando **não se** tem o conhecimento das precauções e dos agravantes que os danos podem gerenciar para uma pessoa ou também para uma empresa. Dados circulam constantemente em uma rede de comunicação e se proliferam de acordo a necessidade e importância do arquivo, é nesse caso que pode existir uma vulnerabilidade no sistema, assim se faz necessário o conhecimento e técnicas para que a situação não tome uma proporção de risco.

As reduções da vulnerabilidade dos sistemas partem do conhecimento técnico sobre os principais fatores de risco, tomando-se como base a segurança de informação em redes corporativas, onde por nível de estatísticas são por maiorias os públicos alvo de pessoas mal-intencionadas. Assim, pode-se identificar as causas de vulnerabilidade, explicar os passos importantes para uma recuperação em caso de invasão na rede e evitar de certo modo toda e qualquer intenção de ataque. Tendo a pesquisa analisado sobre os riscos do *malwares*, e observado o funcionamento desses tipos de vírus, a hipótese levantada por esta pesquisa é que: trazer repetição de algumas ações para vida útil da empresa dificultaria a contaminação desse tipo de ataque como utilização massiva de ferramentas de varredura, verificação da origem de alguns programas, e-mails e links de procedência duvidosa.

Diante das situações é notório a necessidade de as empresas compreender que independentemente da sua infraestrutura e poder de mercado é preciso estabelecer políticas de segurança, implantar um sistema de segurança através de normas, acesso moderado apenas para pessoas autorizadas em seus setores, utilizar *softwares* criados para esses devidos fins proporcionando um sistema de tecnologia mais seguro.

De certo modo, a segurança da informação é uma ferramenta de auxílio para um bom andamento de uma rede corporativa, por mais que seja a importância reservada para a segurança da empresa, ela nunca será absoluta, pois a tecnologia sempre está em evolução, podendo assim acontecer uma depreciação nas técnicas utilizadas atualmente ou *software* que usam uma programação elaborada para hoje. A técnica de agir em detrimento as vulnerabilidades

existentes é justo pois é a principal arma da pessoa mal-intencionada e nunca será uma tática ultrapassada.

Desta forma, o objetivo do trabalho é descrever os principais fatores de riscos as informações de bancos de dados de instituições públicas, como forma de difundir o conhecimento sobre o assunto e evitar possíveis danos ao erário.

2 REFERENCIAL TEÓRICO

2.1 CONCEITO INICIAL A SEGURANÇA DA INFORMAÇÃO

Diante do cenário sobre o assunto abortado, segurança da informação nada mais é que uma proteção no sistema de comunicação em redes, dando um suporte nos dados que são recebidos pelos usuários ou até mesmo enviados, além do mais, a segurança da informação tem a relação com os gerenciamentos de dados de uma rede, tais como, o armazenamento, a divisão e subdivisão compartilhada de formas sigilosas auxiliando-os nos conceitos de integridade, confidencialidade e disponibilidade que são os pilares da segurança da informação.

2.1.1. INTEGRIDADE

De acordo com Galvão (2015), a integridade garante que as informações são verdadeiras e não são afetadas por nenhum tipo de modificação durante o tempo de seu armazenamento ou percurso caso enviada a um destinatário. É a propriedade de preservar a informação estáveis dando garantia que ao chegar no destino ou sair da origem o mesmo não sofra alterações onde o usuário que o acessa possa de alguma forma identificar o proprietário sem fazer manipulações. Aplicando ao conhecimento; seria uma quebra da integridade, quando os dados são modificados intencionalmente por um usuário que não seja o titular.

2.1.2. CONFIDENCIALIDADE

A NBR ISO/IEC 27002 (2005), é a propriedade de garantir o acesso devidamente restrito as pessoas autorizadas estabelecidas através de níveis de admissões sendo capaz de haver propriamente dito a hierarquia ligado a política de segurança das empresas, de outro modo, também se aplica a proteção a divulgação não autorizada dos dados.

2.1.3. DISPONIBILIDADE

Segundo Galvão (2015), disponibilidade é a garantia de que a informação estará livre quando a pessoa devidamente autorizada a ter acesso fizer requisição para o seu uso. É a propriedade que garante a viabilidade da informação entre os usuários e os receptores, de certo modo é, facilitar o acesso a qualquer lugar e a todo tempo, disponível para que os usuários consultem ou utilizem para alguns fins de interesse da empresa, tanto como pessoal, como

também corporativo. Aplica-se do mesmo modo as vantagens de possuir essas regalias as informações em máquinas e equipamentos no setor empresarial monitorada pela equipe competente.

2.2 ESTRATEGIA DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO PÚBLICA

Sacconi (1998) induz que ao similar o específico conceito de estratégia, é possível analisar de instante que a informação exerce uma função rápida na tomada de decisões do gestor. Por dedução, garantir os princípios básicos que auxiliam no Norte do seu processo de proteção é um motivo estratégico de suma importância no âmbito da gestão de informação que é usada pela organização pública, pois apodera-se de forma correta e numa situação oportuna estabelece e autoriza a tomada de decisões de forma útil, ágil e efetiva, colaborando para que a organização desenvolva o sucesso no alcance de suas metas e de uma posição de destaque ou de excelência em seu campo de atuação.

Gimenez (1999, p.69) afirma que a gestão estratégica das informações é fundamental para as organizações, pois “possibilita tomadas de decisão que sustentam outros processos de gestão e outros processos estratégicos”.

2.2.1. IMPLANTAÇÃO CONTEMPORANEA DA SEGURANÇA DA INFORMAÇÃO NO SETOR PÚBLICO

Nobre, Ramos e Nascimento (2010) retratam de aspecto geral e tomando como base o ponto de vista científico, a segurança da informação está incluída sobre conhecimento de que se apresenta muitas lacunas, até mesmo de estudos específicos sob a vista do setor de gestão pública. A informação é um dado importante e que não se deprecia e nem deteriora com facilidade, é reaproveitável e tem seu valor estabelecido unicamente pelo usuário. Quando algum dado é disponibilizado na internet dificilmente sumirá totalmente, por isso é necessário fazer alguns procedimentos que se faz ter cautela.

Ciente da importância da segurança da informação no setor de organizações públicas e das responsabilidades desinente de sua falta ou deficiência, o Tribunal de Contas da União (TCU) passou a verificar, desde o ano de 2007, fundamentos no âmbito da governadoria de tecnologia da informação em que, os indicadores, investiga o percentual de fixação de práticas de segurança da informação em órgãos da administração pública federal (TRIBUNAL DE

CONTAS DA UNIÃO, 2010). Essa avaliação apresenta-se de suma importância, na percepção de observar o verdadeiro cenário e de se operar as orientações para que as organizações fixe um papel proativo, de feito a melhorar a eficiência e seu poder de decisão, a qualidade a ser prestado na confiabilidade próximo à sociedade, evitando, ainda, o desperdício de recursos públicos em ações corretivas ou em setores de gestões inadequado de ferramentas ou de soluções de segurança, no objetivo de garantir a integridade, confidencialidade e disponibilidade da informação. Empenhado na importância da segurança da informação no sistema público e dos efeitos sobrepostos da deficiência ou ausência, o sistema governamental passou a realizar, levantamentos na área da gestão pública de tecnologia da informação em que, entre outros indicadores, afere o percentual de implantação de práticas de segurança da informação em órgãos da administração pública.

Deste modo essa avaliação se faz importante no que condiz com o cenário atual de visualizar e proceder direções para que as instituições operem um sistema proativo, no sentido de melhorar o poder de decisão e a eficiência da qualidade do bom serviço prestado e respeitando a credibilidade garantida pela sociedade, preservando o desperdício de recursos públicos em uso inadequado de ferramentas, como em ações corretivas, como também em manutenções técnicas de soluções de segurança, no objetivo de garantir a integridade, confidencialidade e disponibilidade da informação.

2.3 IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO NO AMBIENTE EMPRESARIAL PÚBLICO

Numa organização empresarial, segundo Mañas (1999).

A Informação é um processo pelo qual a empresa informa-se sobre ela própria e seu ambiente, e por ele informa ao seu ambiente sobre ela mesma. A gestão da informação pode ser vista na empresa de duas maneiras: a) função por função, serviço por serviço, cada um por si; b) globalmente, em nível das áreas e da empresa. (1999, p.25)

Em outras palavras, a informação é o patrimônio transparente mais importante da empresa, onde as mesmas se preocupam com cada passo da utilização dos dados e do mesmo modo tentam manterem em uso da corporação. Empresas orientadas entendem a importância de elaborar projetos estratégicos, visando a proteção desse patrimônio e em consequência seus produtos e serviços.

A informação é um recurso que não se deteriora nem se deprecia facilmente, é reutilizável e tem seu valor determinado exclusivamente pelo usuário. Quando algo é disponibilizado na internet dificilmente ela será apagada totalmente, por isso é preciso fazer alguns procedimentos e se faz necessário ter cautela.

É importante ter toda uma infraestrutura que dê suporte a política de segurança ligado a um sistema de topologia da rede, auxiliando na identificação do setor em que ocorrer uma eventual discrepância aplicado a um gerenciamento de rede. Métodos contraceptivos são tão importantes quanto as próprias informações, como por exemplo a implantação de diretrizes na hora de cadastrar um funcionário ou até mesmo um cliente com logins monitorado pela equipe responsável, ter vigilância em e-mails corporativos e sistemas *VoIPs*, o investimentos em palestras, aulas e oficinas de conhecimentos sobre a importância dos métodos a todo o efetivo ligado a empresa serão procedimentos capazes de orientar as empresas a analisar que a segurança da informação é um item de importância para o bom andamento das atividades.

2.3.1. CONCIENTIZAÇÃO

De acordo com Silva *et al* (2003) é de suma importância o dever de tornar o efetivo das empresas conscientes das situações possíveis sobre os riscos, ataques, vulnerabilidades dos sistemas de informações através de princípios estabelecido pela empresa. A política de segurança deve ser um fator primordial na conscientização dos funcionários sendo importante a transmissão entre o que fazer e qual procedimento tomar numa possível exação.

2.3.2. GERENCIAMENTO DE CRISES

Para Fontes (2012, p.72) se faz necessário e incluído na política de segurança, métodos de gerenciamento em casos de incidentes dentro dos patrimônios das empresas, uma equipe deve ser preparada para de alguma forma desviar os problemas para uma válvula de escape, estando de sobre aviso e tendo ciência que poderá ser acionada assim que possível, nesta ocasião estabelecer um tempo ágil de recuperação orientando a todas as pessoas dos setores competentes das informações que houve uma tentativa ou até mesmo a própria invasão por pessoas mal-intencionadas na rede.

2.3.3. FUNCIONALIDADE DE SISTEMAS E PRIVACIDADES

Criar um monitoramento de gestão de pessoas com logins e senhas para funcionários com uma delimitação de contas privilegiada facilitando no controle de identificação da hora, do dia e de quem teve o acesso, além de ser uma praticidade para as empresas e os funcionários, também é uma alternativa de segurança e deve estar incluso na política de segurança como um método de prevenção e identificação em casos de ataques. Softwares destinados para essas funções devem estar atualizados e observados pela equipe de TI em casos de manutenções e configurações essenciais para manter esse método de gestão ativo.

2.4 AMEAÇAS

No setor empresarial é muito comum ter alguns conhecimentos de empresas que foram vítimas de um ataque cibernético, cada vez mais informações são importantes e aos olhos de *hackers* que visam alguns fins lucrativos, de certo modo, mesmo a empresa tendo um investimento na parte de segurança cibernética, usuários mal-intencionados usam de alguns artifícios para implantar seus ataques, chegando até mesmo a fazerem usos de técnicas físicas como por exemplo a engenharia social, onde o *hackers* utiliza dos conhecimentos pessoais das vítimas utilizando a inocência e confiança para persuadir o funcionário a dar informações sigilosas e que dão acesso às máquinas restritas como o objetivo de ter acesso às informações.

Assim como a engenharia social, existem várias outras maneiras de tentativas para obter o acesso às informações de uma rede corporativa, *malwares* são desenvolvidos no intuito de alterar valores dos *softwares*, tais como o código fonte de uma maioria de arquivos e o deterioram para obter sucesso nos seus objetivos dos computadores em que foram parasitados, bem como seu nome, também faz referência a vírus biológico que utilizam de um hospedeiro para se multiplicar. O vírus além de fazer alterações, podem interferir no funcionamento do programa e captar dados.

No sentido de melhorar o entendimento das ameaças envolvidas nas navegações de internet, dá-se a seguir alguns conceitos com base em Goodrich e Tamassia (2013):

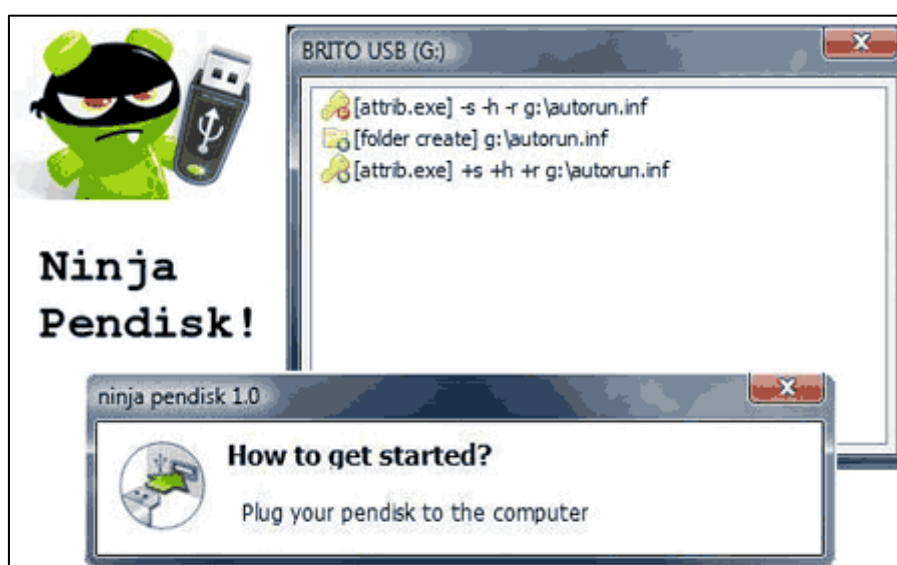
2.4.1. VÍRUS

Para Goodrich e Tamassia (2013) os vírus são *malwares*, ou seja, pragas virtuais desenvolvidas por pessoas mal-intencionadas com o objetivo de causar estragos aos dados da

máquina e se propagar em outros computadores de forma sigilosa sem ser percebida pelo administrador da rede da empresa. O vírus altera os parâmetros do programa em que se hospedou, no intuito de apagar, copiar, danificar e roubar informações facilitando o sucesso do criminoso virtual. Existem alguns meios de infecções elaborado por esses usuários de má índole, alguns são jogados na rede de forma discreta e até mesmo camuflado em e-mails, arquivos compartilhados e sites, outros são autos executáveis comumente aparece camuflados numa execução de outro programa.

A Figura 1 refere-se a arquivos infectado e alojado em um *PenDrive*.

Figura 1 – Pastas infectadas



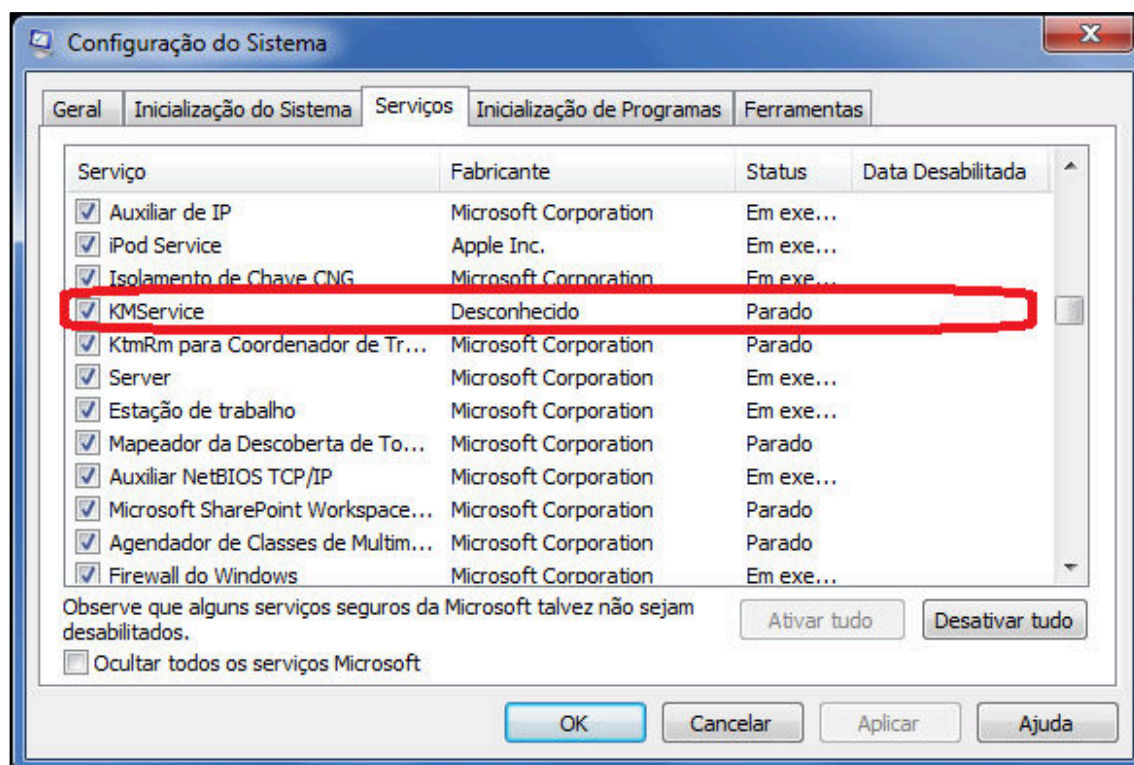
Fonte: <http://www.vejaisso.com/antivirus-online-verificar-virus-em-downloads-e-arquivos-gratis/>

2.4.2. WORMS

Worms é um tipo de malware com uma grande semelhança ao vírus (FERREIRA, 2009), o que difere é a forma de se propagar “sozinhos”, de certo modo eles não precisam de um arquivo hospedeiro para alterar suas estruturas e nem em executáveis. Eles se multiplicam devido a troca de dados em redes, numa empresa é bem mais rápido a velocidade de propagação e essa característica é o que faz prejudicial a máquina enchendo as memórias com suas cópias e dificultando o bom funcionamento do computador, e consequentemente das redes. Também é um malware de caráter sigiloso e se implanta no PC ou redes sem que os usuários percebam.

A Figura 2 descreve o malware *worms* hospedado em uma ferramenta de serviço do sistema Windows instalado sem o conhecimento do usuário

Figura 2 – Malware worms infiltrado no sistema



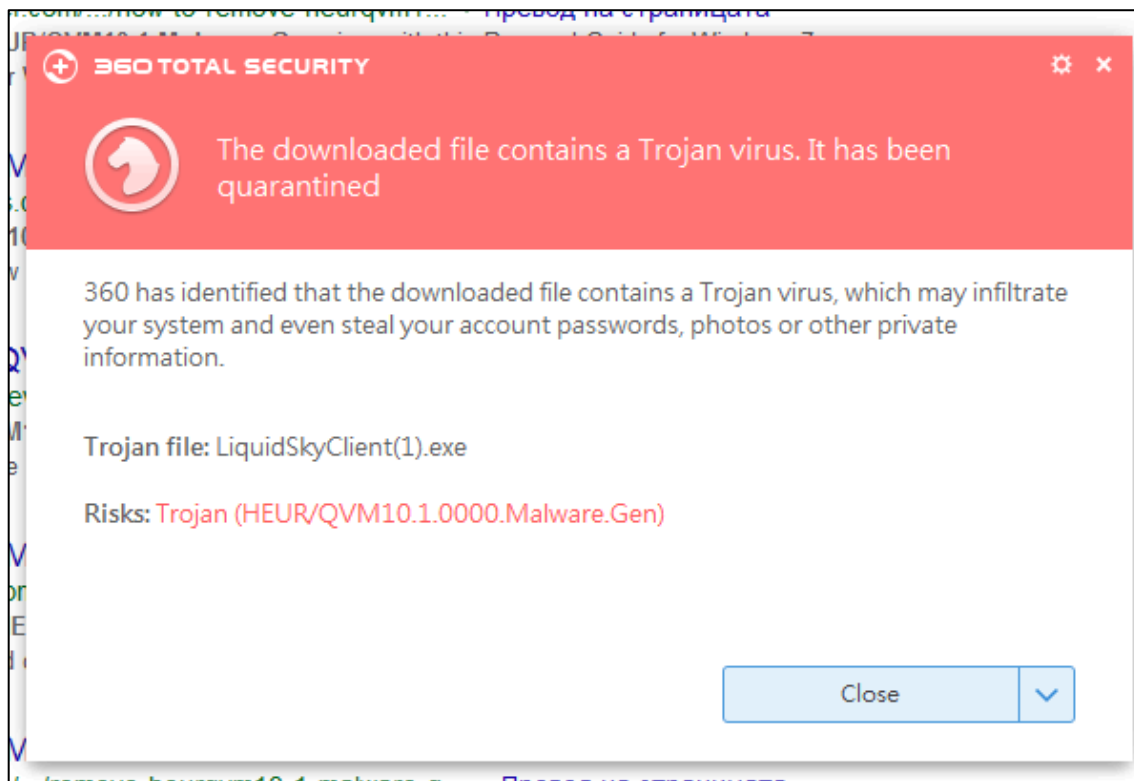
Fonte: www.foruminfolab.com.br

2.4.3. TROJANHORSE (CAVALO DE TRÓIA)

A partir da perspectiva do site da Fundação Joaquim Nabuco (2020) e da autora, o cavalo de troia se faz analogia ao ser nome o cavalo que foi presenteado pelos gregos aos troianos. É um malware, sem a execução do programa em que ele esteja sincronizado não há um risco eminente, ele se instala na máquina através de uma foto, música, pasta, jogo e entre outros, geralmente quando não se obtém o sucesso nas tentativas ou não foram encontrados resultados de falhas no sistema. Ao ser executado ele cria uma vulnerabilidade na porta da rede da empresa com intuito da pessoa mal-intencionada de invadir a máquina utilizando das portas TCP e UDP para interligar com a rede externa disponibilizando o acesso via prompt de comando para que o criminoso virtual entre em ação, além dessas características o trojan tem outras funcionalidades, como a captura das informações e aplicação de scripts.

A Figura 3 faz referência a uma detecção do *malware* trojan por meio de antivírus camuflado em um executável.

Figura 3 – trojan encontrado num executável



Fonte: liquidsky.blog.br

2.4.4. KEYLOGGERS

É um software agressivo e preocupante, caso seja utilizado com segundas intenções, o seu objetivo é o de capturar e transcrever as teclas que foram utilizadas pelo usuário. No momento em que o *keylogger* for executado ele pode sequestrar textos de e-mails, dados de protocolos importantes de uma empresa, senhas e logins de contas privilegiados, números de cartões, etc.

Segundo Machado (2012).

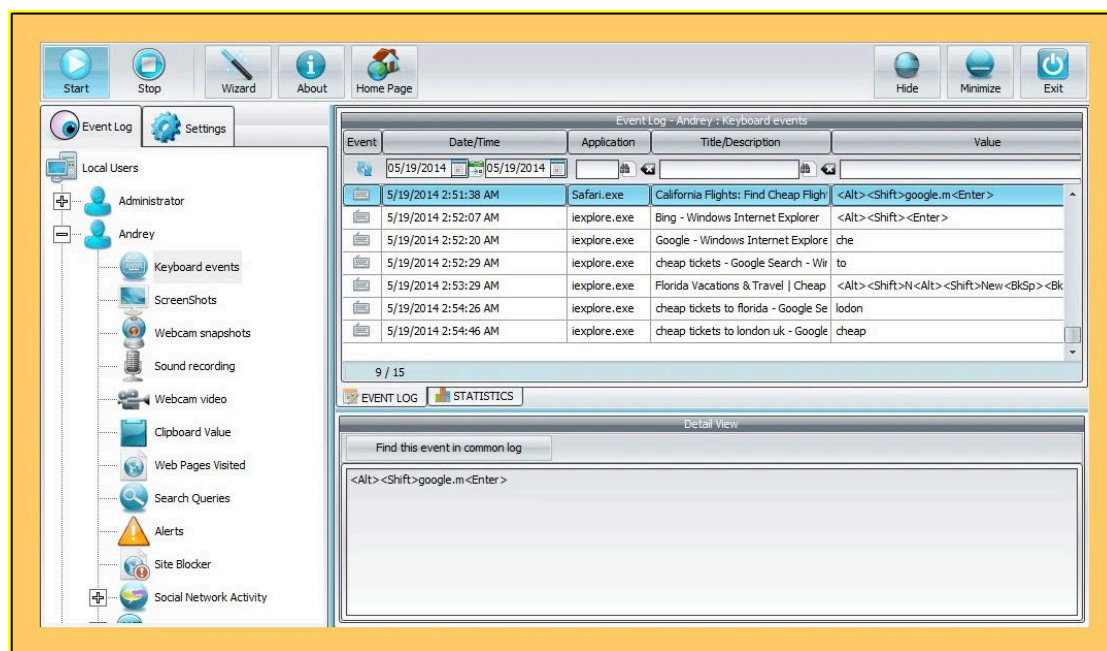
Keyloggers são aplicativos ou dispositivos que ficam em execução em um determinado computador para monitorar todas as entradas do teclado. Assim, aquele que deixou o programa em execução pode, em outro momento, conferir tudo o que foi digitado durante um determinado período. Aplicativos com a função keylogging foram criados para ações perfeitamente legais, como monitorar a atividade de funcionários de uma empresa ou até para os pais checarem que tipo de conteúdo seus filhos têm acessado na internet. (2012, p.67)

Existem alguns *keyloggers* programados para o envio automático até o criminoso virtual denominado cracker, para uma conta cadastrada que na maioria das vezes são e-mails. Devido

a evolução de prevenções contra esse malwares, foi desenvolvido o uso de teclado virtuais com a intenção de inibir a transcrição das teclas digitadas, mas a evolução também veio com os vilões, estes evoluíram e criaram um sistema de *screenloggers*.

Figura 4 estabelece uma ação do software *keyloggers* com os dados coletados ou os que ainda irão ser.

Figura 4 – keyloggers em execução



Fonte: geckoanndfly.com

2.4.4.1. SCREENLOGGERS

Goodrich e Tamassia (2013) relatam que o *screenloggers* é uma variante do *keyloggers* com a missão de observar o momento em que o cursor é movido e clicado, foi criado depois que encontraram métodos de prevenção dos softwares utilizando teclado virtuais.

2.4.5. SPYWARE

É um malware que tem o objetivo de espionar atividades de uma máquina quando esta é acessada. Ele gera um relatório de informações coletadas e envia para os criminosos virtuais sem que a empresa ou usuário perceba. Muitos assimilam a funcionalidade e objetivo com os trojans, porem o que os diferem é que os *spywares* não tem a característica de dominar e manipular as máquinas infectadas pelos crackers. Vale ressaltar que muitas empresas são

desenvolvedoras desses *malwares* no intuito de infectar concorrentes a fins de informações particulares. Existem variações de vírus espões como os *adwares*.

2.4.5.1. ADWARES

São vírus semelhantes aos *spywares* por possuir a sua mesma forma de infecção, instalação e desinstalação. Utilizam de propagandas tendenciosas e URLs falsas camufladas com o objetivo de esconder no mesmo anúncio o *spyware*. Ao longo do tempo foi se sofisticando no âmbito dos usuários ficarem interessados devidos ao método de persuasão. Crackers também utilizam executáveis para implantar o vírus espião no ato da instalação. É importante numa rede corporativa a cautela para uma ameaça de possível infecção, pois a inteligência do criminoso virtual para a empresa é mutua, devido os interesses por programas úteis para a mesma, facilitando no objetivo de invadir. (JAGATIC, 2005)

A Figura 5 mostra a aplicação do *adwares* no computador de um usuário sem algum programa de segurança.

Figura 5 – *adwares* camuflado em propagandas



Fonte: <https://www.techflier.com/2016/05/19/28-major-malware-types-and-how-to-avoid-or-remove-them/>

2.4.5.2. SPAMS

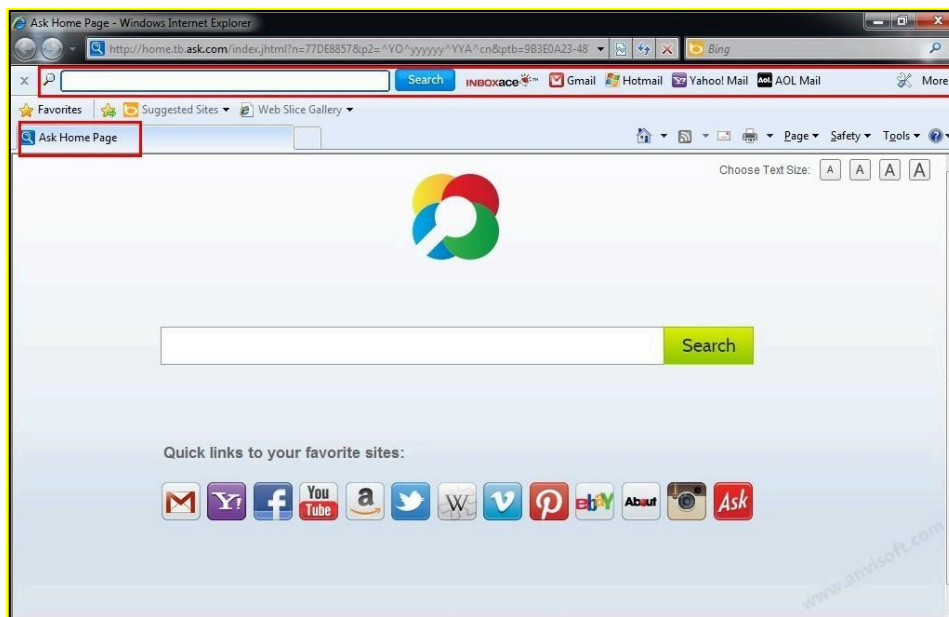
São mensagens de envio virtual para e-mails sem o consenso ou autorização do titular, nelas acabam vindo tipos de *spywares* e *adwares* camuflado em propagandas, avisos falsos para a troca de senhas das redes sociais, contas bancárias e entre outros. É considerado como um lixo eletrônico e tem um poder enorme no setor industrial, a *Sysmatec* afirma que nos últimos anos houve uma demanda de 72,9% de e-mails recebidos pelas empresas e de spam somavam o total de 40%, ou seja, mais que a metade do apurado. Entre esses fatores a perda de informações importante é um dos fatores prejudiciais, além de acumulação de banda e tempos perdidos para excluir da caixa de mensagens.

2.4.6. HIJACKERS

De acordo com Liska e Gallo (2017), os *hijackers* tem a capacidade de atacar o navegador alterando a URL discretamente, além disso, eles bloqueiam alguns sites responsável pela prevenção dessas malwares, outra característica é a instalação de barras de ferramentas no próprio navegador de forma sensata ficando assim difícil a percepção do usuário, também executa várias páginas sem o consenso do operante. Crackers utilizam dos *hijackers* para criar barras de ferramentas de programas usados nas próprias empresas e por ser um software utilizado no dia a dia fica menos notório a observação.

Na Figura 6, são apresentadas as barras de ferramentas criada no navegador denominadas *hijackers*.

Figura 6 – hijackers no navegador



Fonte: <https://www.techflier.com/2016/05/19/28-major-malware-types-and-how-to-avoid-or-remove-them/>

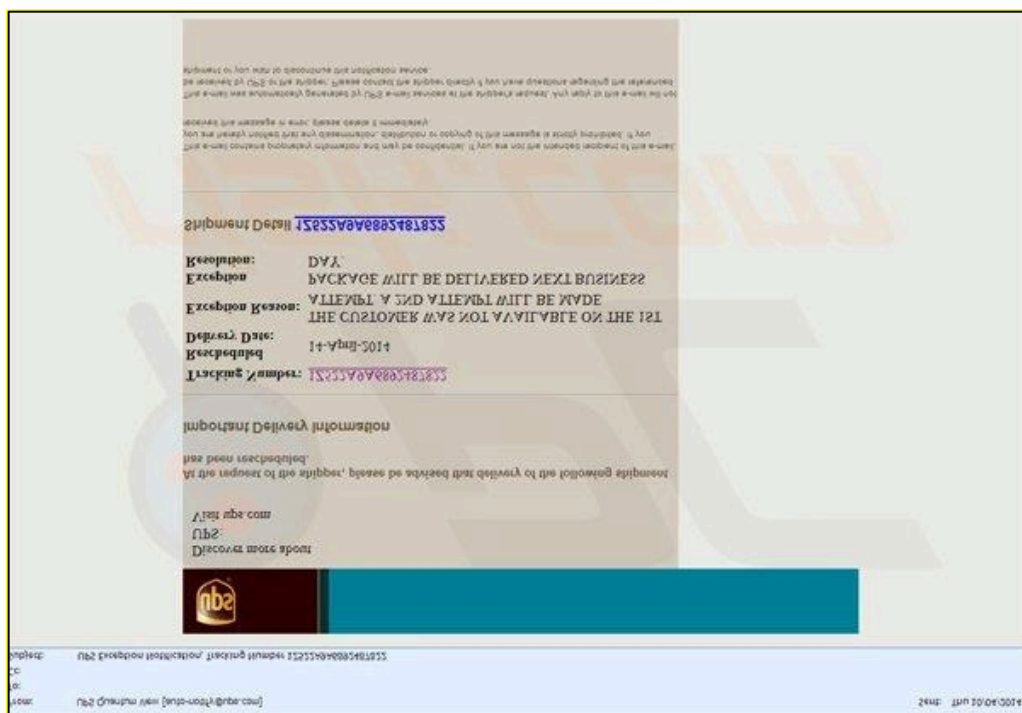
2.4.7. RANSOMWARE

O *ransomware* é um tipo de malware de característica criptográfica, onde ele utiliza das criptografias para modificar a base de arquivos dentro do sistema operacional. O primeiro *ransomware* foi criado por um Biólogo com PhD na universidade de Harvard, Joseph L. Popp. Ele reutilizou o Trojan e o modificou para informar ao usuário que determinado software havia expirado, caso efetivado com sucesso, iniciava o ataque do malware criptografando os arquivos e exigindo uma quantia em dinheiro para restaurar os arquivos criptografados, para Liska “O *ransomware* realmente saiu de moda no final dos anos 90 e não voltou a entrar em evidências até 2005.” (2017, p.17). A existência dos malwares, ao longo do tempo, foi dividida em cada necessidade de aplicação. Extorsionários digitais perceberam a importância do *ransomware* e então subdividiram suas funções entre: as que criptografam e as que restringe o acesso do arquivo. Um dos *ransomware* mais conhecido ao decorrer do tempo, é o *CriptoWall*, produzido capaz de se infiltrar no sistema operacional através de mensagens, e-mails, programas de vídeos e falsas atualizações de flash. Do mesmo modo que o extorsionário utiliza o *ransomware* para criptografar os arquivos, ele utiliza a criptomoeda como recompensa pela reversão dos ataques, atualmente a criptomoeda mais utilizada nesse processo é o Bitcoin, mas existem outras criptomoedas que trabalham com método pré-pagos como o *Ukash*, *MoneyPark* e *PaySafe*. O *Ransomware* é uma das ameaças cibernéticas mais utilizada nos dias atuais. Trata-se de um código malicioso que codifica as informações e os arquivos do seu computador e insere uma

tela com instruções para que o usuário possa recuperar tudo que criptografado em troca de moedas digitais.

A Figura 7 descreve um e-mail infectado após ter sido vítima do *ransomware*.

Figura 7 – e-mail infectado



Fonte: <https://www.pcrisk.pt/guias-de-remocao>

2.4.7.1. MONEY, UKASH E PAYSAFE

MoneyPark, *Ukash Paysafe* são tipos de transições de criptomoedas, semelhantes ao Bitcoin.

2.4.7.2. BITCOIN

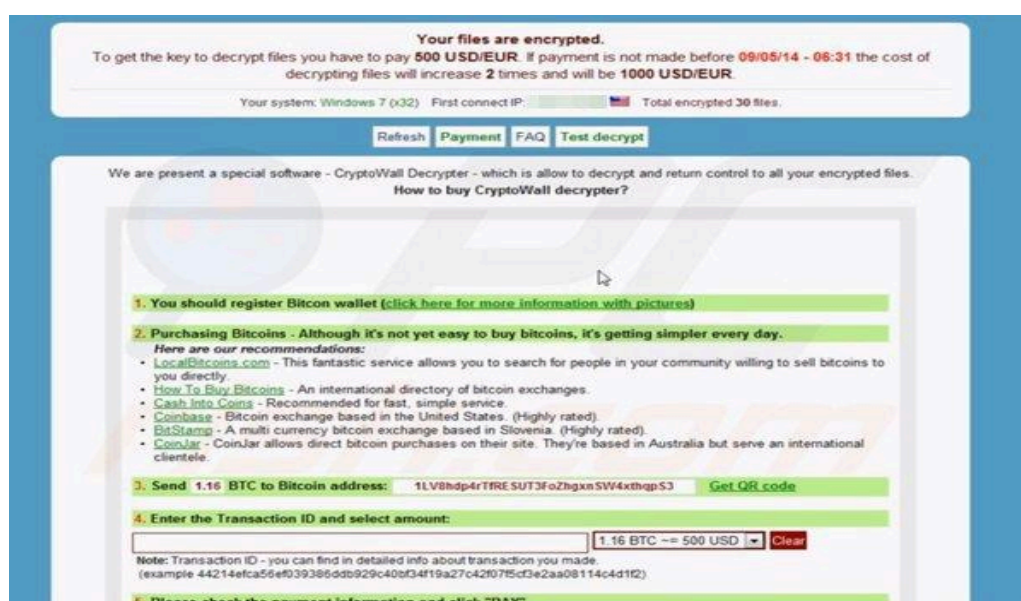
Bitcoin uma moeda real, porem virtual, sua forma de produção não é monitorada pelo BACEN, são controladas por uma rede digital *peer-to-peer*, ou seja, sem a dependência de bancos financeiros. Os *bitcoins* são emitidos por uma rede de milhares de computadores operados por pessoas que na maioria das vezes “cedem” suas máquinas para o serviço denominado mineração, “Data mining” cujo o efeito é criar as cripto moedas e registrar as transições feitas.

Para Liska e Gallo (2017):

Atualmente o *ransomware* é considerado uma das formas de ataque predominante contra sistemas de computadores, exigindo apenas uma exposição limitada a vulnerabilidade e um reconhecimento mínimo do alvo. Estima-se que uma das variantes mais conhecidas, o *CryptoWall* (atualmente extinto), foi capaz de extorquir 18 milhões de dólares até meados de junho de 2015. (2017, p.17).

A Figura 8 faz referência a uma página de pagamento do resgate *CryptoWall*.

Figura 8 – pagamento da criptomoeda



Fonte: <https://www.pcrisk.pt/guias-de-remocao>

2.5 PHISHING DENTRO DA INSTITUIÇÃO PÚBLICA

É bem claro que numa empresa há uma movimentação grande de pessoas manuseando informações de caráter específico. Além de funcionários, as empresas são vítimas das ameaças cibernéticas por meio lógico, mas não só por esses modos, criminosos virtuais estudam métodos de persuasão para o uso contra o efetivo da corporação. Segundo o Gartner (2018), 95% das ameaças iniciam pelo *phishing*. Os dados pessoais são algo de grande importância para uma pessoa e a empresa, não só os dados, mas fotos, arquivos, coisas que só a pessoa ou poucas tem o acesso. Por este modo existem crackers que buscam modos de roubar esses dados para vendê-las ou chantagear as vítimas.

Para OLIVEIRA, Vieira (2011) *phishing* é um termo classificado para a prática de “pescar” informações pessoais através de mensagens, pode ser parecido como alguns malwares

ou até spams, mas esse método é de característica física, onde o agente mal-intencionado visa os usuários funcionários da empresa e induz a ele ceder informações através de diálogos. Muitos crackers criam uma relação de amizade se passando por um amigo até mesmo chegando a uma relação amorosa fake, outros utilizam do telemarketing para ligarem após ter apurado algumas informações, ligam para as vítimas se passando por algum funcionário de cargo maior ou equiparado nas empresas e pedem algumas informações sigilosas sobre o acesso dele na rede corporativa. Esses métodos não tem uma iniciativa de prevenção, por de fato aproveitar da inocência e induzir ao funcionário falar.

De acordo com Laudon e Laudon (2007) existem maneiras de se educar para essas práticas com o objetivo de dificultar a ação ou até mesmo sanando essa possível forma de intrusão. *Phishing* junto com os *ransomware*, são as mais convencionais numa empresa, devido ser a forma mais que lucrativa para os crackers após infectados, além disso são as piores formas de reversão por atingir aos dados pessoais.

Figura 9 mostra o phishing, forma comum de engenharia social se passando por uma empresa.

Figura 9 – phishing contra usuário



Fonte: <https://www.techflier.com/2016/05/19/28-major-malware-types-and-how-to-avoid-or-remove-them/>

2.6 POLÍTICAS DE SEGURANÇAS DAS INFORMAÇÕES – PSI

A política de segurança da informação é uma direção que a empresa estabelece para todo o elo corporativo através de missões sobre regras, no intuito de proteger seu patrimonial digital e físico, com o dever de ter uma boa sincronia conjunto ao efetivo e equipe de TI.

Para Fontes (2006):

A Política de Segurança da Informação (PSI) é um documento que deve conter um conjunto de normas, métodos e procedimentos, os quais devem ser comunicados a todos os funcionários, bem como analisado e revisado criticamente, em intervalos regulares ou quando mudanças se fizerem necessárias. É o SGSI que vai garantir a viabilidade e o uso dos ativos somente por pessoas autorizadas e que realmente necessitam delas para realizar suas funções dentro da empresa. (2006, p.45)

A gestão da segurança é complementada e tomada como base da norma ABNT NBR ISO/IEC 27001:2005V, reconhecida mundialmente como um padrão de referência da segurança da informação e tem como funcionalidade o objetivo de além da segurança de dados a restrições de acessos, gerenciamento de redes, controle de efetivo com contas/logins seguindo os pilares responsáveis pela integridade, confidencialidade e disponibilidade. A empresa deve impor um costume aos funcionários a ler normatizações referente a PSI estabelecendo limitações e responsabilidades em casos de incidentes causados pelos próprios colaboradores da corporação.

2.6.1. DAS RESPONSABILIDADES

Segundo Fontes (2006) é da responsabilidade da equipe de TI ornamentar um limite estrutural para cada setor, viabilizando o conforto para as funcionalidades, organizar o ambiente empresarial físico, tais como, configurações nas máquinas, instalações de softwares com o objetivo de monitorar os computadores, instalações de antivírus e variantes, restrições a websites inapropriados. Além da colaboração da equipe de TI, é essencial a responsabilidade da administração da rede corporativa a instalação de refrigeração no data center, sistematização na estrutura organizacional física dos ativos de redes, segurança física em setores restrito ao acesso e toda parte de infraestrutura física é destinada para empresa a missão de providenciar essa estrutura com o objetivo de auxiliar na proteção das informações.

2.6.1.1. DATA CENTER

O data center é uma infraestrutura composta de vários servidores trabalhando simultaneamente e são responsáveis por administrar todos os dados digitalmente processados. Algumas empresas criam e gerenciam essa estrutura com caracterização própria, onde a equipe de TI destinada para essa área auxilia no andamento do serviço. Uma das características dos data center são nas maiorias das vezes o uso do sistema operacional Linux, devido ser um software de código aberto, facilitando a customização, o manuseio dos colaboradores e a segurança contra-ataques virtuais, por ser um sistema mais resistentes a ameaças e menos procurado por crackers.

Seguindo como política de segurança, o data center é o setor primordial para esse quesito, devido ser o local onde armazena todas as informações processada pela empresa no dia a dia. Sistema contra invasão, tanto como digital, quanto a física, devem ficar 24 horas em evidência de monitoramento. A restrição ao acesso de até mesmo funcionários da empresa faz parte de uma política de segurança fornecida diante das conscientizações do efetivo para o entendimento fundamental do serviço, além disso instalações de câmeras, biométrica restrita apenas para funcionário destinado ao data center, portas com trava elétrica vigiada por guardas de segurança, cartões de acesso com mecanismo ante clonagem.

Mesmo com o selecionamento do efetivo para o acesso ao data center, também se faz importante o controle da equipe de TI, registro de toda a movimentação deve ser elaborado e autorizada pelo chefe do setor, para que seja fornecido o acesso dentro da sala sem soar o alarme de invasão. Além da segurança física do data center, deve haver uma boa estrutura auxiliadora com projetos de refrigeração, sistema anti-incêndio e geradores de energias em caso de queda de energias fornecendo um bom funcionamento dos serviços na rede corporativa.

2.6.1.2. BACKUP

Doug Heckman (2012) questiona que diante as responsabilidades da equipe de TI e do setor administrativo, o *backup* das informações é conscientizado de ambas as partes e faz parte da política de segurança da informação presente na corporação. A norma ABNT NBR ISO/IEC 27001:2005V recomenda que backup das informações sejam arquivados em lugares longe do núcleo operacional da empresa ou em outra sede da rede corporativa, também tenha uma mídia de alojamento confiável. O *backup* tem a garantia que os dados não serão alterados tais como; propriedades, bancos de dados, configurações e arquivos pessoais fornecendo assim a

integridade dos mesmos. “É evidente que o procedimento de *backup* é um dos recursos mais efetivos para assegurar a continuidade das operações em caso de paralisação na ocorrência de um sinistro”. (FFREITAS E ARAUJO, 2008, p. 133)

Estudos sobre o assunto questionado explicam que no atentado de 11 de setembro de 2001 o maior erro da não prática de *backup*, foram empresas ter estabelecido o arquivamento dos dados na torre oposta, ou seja, as empresas da torre A tinham seus arquivos guardados na torre B e empresas da torre B tinham arquivos guardados na torre A e não em outro local distante, após o ataque as duas torres, muitas empresas sumiram por ter perdido suas informações e não terem mais acesso a elas.

2.6.1.3. REDUNDÂNCIA

Na PSI a redundância vem como uma ferramenta de auxílio e contra resposta ao mesmo, desse modo é de suma importância uma boa infraestrutura para possível utilização dessa política de segurança. As informações são garantidas com a redundância de rede, pois há réplicas de dispositivos fundamentais para os fluxos de dados, auxiliando tanto para entrada reserva numa possível danificação de um aparelho, quanto no uso da mesma função, fazendo assim um trabalho mutuo para ambos e deixando a rede de comunicação fluida. Numa empresa é primordial essa prática, pois no ambiente operacional existem muitas máquinas ligadas a uma rede de comunicação fazendo necessário uma largura de banda leve para o tráfego de dados e a reposição imediata de outros dispositivos.

2.7 AÇÕES PARA A SEGURANÇA DA INFORMAÇÃO

Por Geus e Nakamura (2007, p. 194-195) a segurança da informação são métodos, práticas elaboradas, técnicas, mecanismos e recursos usados para a proteção e prevenção de todo um sistema de dados, tanto pessoal, quanto empresarial. É importante se dizer que mesmo com o investimento alto em ferramentas de imunidade dos dados, empresas não potencializam seus dados estatísticos sobre um nível de controle contra as ameaças cibernéticas, devido ao grande avanço tecnológico e criações de práticas em softwares assim como também em hardwares.

Assim como as ameaças existentes no meio tecnológico, também existem ações para a prevenção das informações, as práticas de segurança intercalam de nível básico ao complexo, dependendo sempre do gestor de TI qual ele irá adotar como prioridade na resposta de possíveis

ataques. Algumas práticas são de prevenções, ou seja, operam de maneira que inibam algumas vulnerabilidades presente nos sistemas, outra prática é de detecções, assim como o nome já se refere, ele detecta a invasão dos malwares e já sincroniza com a outra prática que é a de contra resposta, fornecendo a atividade fundamental para a reversão da intrusão no computador ou em casos mais graves no sistema corporativo.

2.7.1. FERRAMENTAS DE PREVENÇÕES

Em um sistema de dados há um grande gerenciamento de equipamentos tecnológicos que operam sobre um sistema operacional programado por pessoas especializadas. Desse modo é fundamental salientar que falhas ou até mesmo aberturas foram deixados ao longo da programação desses softwares e que existem programas criado para detectar justamente essas discrepâncias virtuais nos computadores, como na própria rede de comunicação dos usuários. A forma de execução dessas ferramentas segundo Russo (2000), é uma simulação de visita a o site ou algum serviço web, procurando pontos fracos, após a verificação, ele cria um relatório explicando detalhadamente o agrave da situação e os pontos de que precisam ser tomados para inibir ou melhor dizendo diminuir as chances de *ciber* ataques. Uma das ferramentas mais usada pelas empresas, é o *wireshark*.

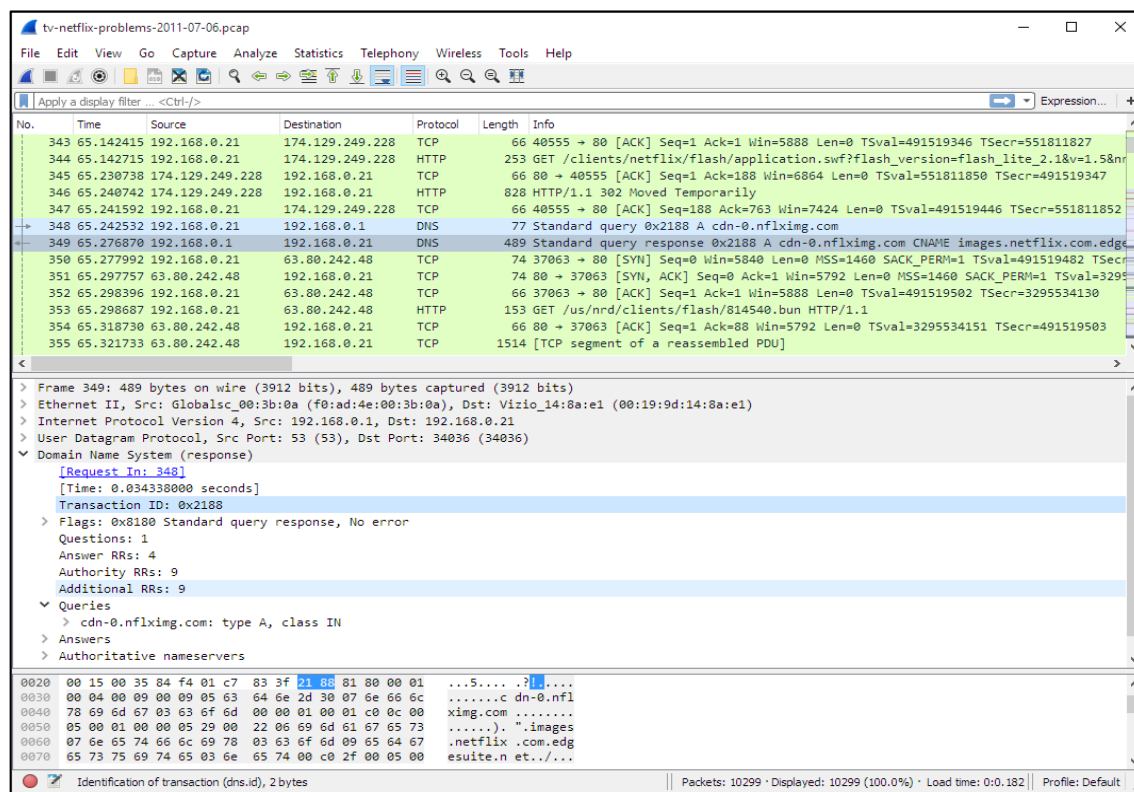
São inúmeras formas pelas quais os usuários e empresas podem se prevenir de ameaças e ataques externos através da internet. Oliveira (2013, p. 41-42) cita entre elas:

2.7.1.1. WIRESHARK

O *Wireshark* (WIRESHARK, 2016) é um software que analisa as rotas dos dados e filtra por protocolos jogados na rede, ou seja, por essa forma de aplicação é possível monitorar e gerenciar a entrada e saída de informações dos computadores com diferentes protocolos, facilitando a detecção de uma possível vulnerabilidade na rede. Essa técnica de prevenção é denominada “*sniffers*” e nem sempre é utilizada para fins benéficos, pois são ferramentas também usadas por crackers no intuito de analisar o tráfego de informação e “pescar” um dado importante. Numa empresa o ciclo de importações é vasto e são atrelados a dispositivos que ampliam o compartilhamento de dados, criando rotas para elas, numa rede de comunicação local dentro de uma empresa com computadores ligados por hubs ou switches, outro usuário mal-intencionado pode usar o *sniffers* para coletar dados.

A Figura 10 demonstra o uso do software *wireshark* com a técnica de *sniffers*.

Figura 10 – wireshark analisando portas vulnerável



Fonte: wireshark.com

2.7.1.2. FIREWALL

O firewall também tem o objetivo de examinar o tráfego, atual como barreira filtrando os dados de entrada e saída entrando em algumas camadas de rede e direcionando conforme é exigido pela equipe de TI da empresa.

Segundo a Rodrigues,

Firewall é uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas. "Parede de fogo", a tradução literal do nome, já deixa claro que o firewall se enquadra em uma espécie de barreira de defesa. A sua missão, por assim dizer, consiste basicamente em bloquear tráfego de dados indesejado e liberar acessos bem-vindos. (2017, p. 01)

De forma mais dinâmica o firewall pode se comparar o firewall com uma portaria de acesso, onde se faz necessário para a entrada, o cumprimento legal das determinações posta

pela administração, tais como; primeiramente se identificar, aguardar a resposta do usuário, não oferecer nenhum risco a segurança do estabelecimento e não levar consigo qualquer informação ou objeto sem a autorização informada a portaria. Ele pode ser utilizado para bloquear o uso de alguns aplicativos ou de modo mais flexível, pode alertar que o aplicativo é um tipo de software não relacionado na política de segurança da empresa. De forma mais simples, também é usado para filtrar o uso do protocolo HTTP, permitindo o tráfego de dados para algumas páginas webs e bloqueando outras inúteis para a rede corporativa.

A imagem 11 ilustra uma situação do uso do firewall na rede de comunicação interna e externa.

Figura 11 – ilustração do firewall



Fonte: <https://www.estudopratico.com/firewall-maneiras>

2.7.1.3. CRIPTOGRAFIA

A criptografia é considerada por muitos profissionais de TI, como uma ferramenta bastante complexa por ser entendida como um conjunto de prática sincronizada com uma legenda tabelada. São códigos revertidos em técnicas para modificar informações observadas por meio de algoritmos, onde se utiliza um texto convencional para alterar por cifras, ficando assim ilegíveis a outros usuários. A empresa junto com a equipe tecnológica, estabelece o método de reversão do código aos funcionários autorizados da empresa. Hoje se titularia a

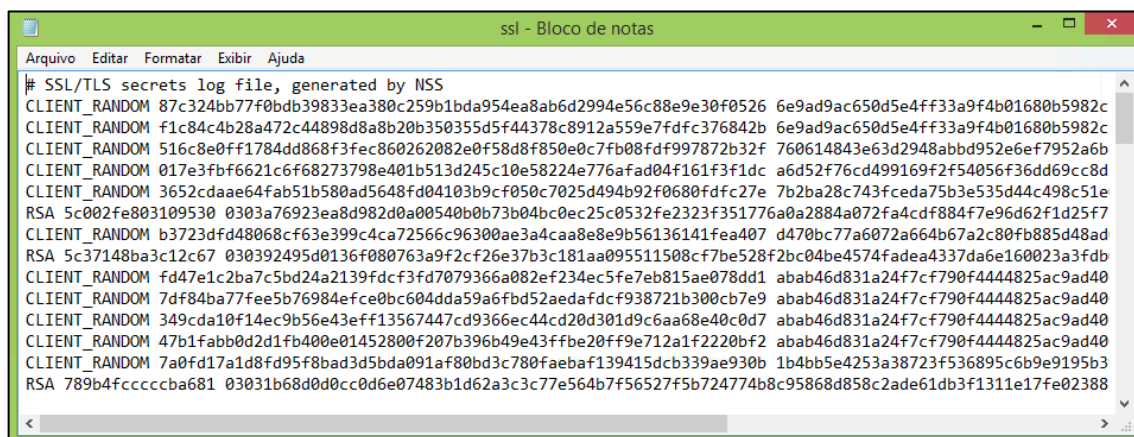
criptografia como um fator de extrema importância para a sequência de dados e informações da rede corporativa, senha e logins são funções de acesso rotineiro no dia a dia dos serviços, invasões cibernéticas contra essas estruturas são facilitadas caso não aconteça a criptografia. Ela mesma foi um avanço na segurança da informação e tanto, mas nada a garante que é um procedimento totalmente confiável, mesmo sendo o mais confiável possível. Além dos algoritmos, são utilizadas chaves com finalidade de reforçar a segurança, essas chaves protegem as palavras cifradas que só serão decifrados com a utilização da mesma chave empregada nessa situação.

Para a Lagrange,

Criptografar consiste em camuflar a mensagem a ser transmitida por um meio que 'não é totalmente confiável de maneira que apenas o destinatário consiga entendê-la. Para tanto, é preciso que apenas o destinatário e o remetente tenham conhecimento de um dado necessário para a correta conversão da mensagem. Esse dado é a chave. Assume-se que qualquer outra pessoa conhece o algoritmo utilizado para encriptar/deciprar e que apenas a chave é secreta. (1989, p. 21)

A imagem 12 mostra uma criptografia de um arquivo.

Figura 12 – criptografia de um arquivo



Fonte: <https://null0blog.wordpress.com/category/wireshark/>

2.7.1.4. ASSINATURA DIGITAL

É uma prática de identificação do usuário que faz uso a máquina, é uma ferramenta de caráter específico de empresas devido à grande interação de informações compartilhadas. Ela permite a comprovação da autenticidade da informação envolvendo a integridade da mesma

objetivando sua criação e o andamento sem nenhuma alteração no compartilhamento da rede de comunicação.

2.7.2. FERRAMENTAS DE DETECÇÕES

Assim como ferramentas de prevenções, as de detecções tem um objetivo primordial e eficaz, no intuito de não permitir que a situação se alastre ao ponto de não ter mais uma maneira de reversão imediata ou, fazer com que o criminoso virtual consiga invadir com o objetivo de roubar uma informação de caráter sigiloso, crucial para o andamento das atividades nas empresas.

2.7.2.1. ANTIVÍRUS

Antivírus são programas com múltiplas funcionalidades operacionais, extremamente importante no uso diário da tecnologia tanto para o usuário pessoal, quanto para os usuários empresariais, suas funcionalidades vem com o propósito de procurar os malwares, detectar intrusões no sistema da máquina e remover os vírus que de alguma forma conseguiram ultrapassar as barreiras de proteções.

Devido ao grande avanço da tecnologia, antivírus ganham novas versão de manuseio sincronizando com outros métodos de prevenções e detecções, umas das mais comuns é o firewall, por trabalhar de maneira conjunta e similar, desse modo, tendo conhecimento que a grande parte de vírus para usos maliciosos são atrelados aos *spywares*, antivírus capacitam essa funcionalidade com o objetivo de inibir a ação desses malwares, mas não só com os spy, o antivírus tem sua finalidade abrangente para os trojans, vírus, *worms*, *keyloggers*, *hijackers*, *adwares*, *spywares*, *ransomwares* (de uma forma mais superficial), spams e entre outros. Assim como todos os métodos de precauções e resguardos das informações não são 100% eficaz, o antivírus tem um grande “poder de fogo” porém não é uma exceção deste fato, pois alguns desses softwares não conseguem exterminar o vírus encontrado, em consequência de que os mesmo são sequencias de *bytes* e chega ser modificado pelo conhecimento do cracker que o programa de responsabilidade preventiva não irá da conta, mas em contra partida, existe uma maneira de reverter a situação, substituindo o arquivo infectado por outra igual “limpo” do próprio software, lembrando que esse método também não é 100% objetivo e que alguns vírus já infectado, conseguem multiplicar para outros arquivos, ou seja, esse método acaba sendo falho.

Mesmo com essas exceções o investimento na área da segurança pela rede corporativa tem que ser de fato, uma grande alternativa, analisando que não irá fazer parte dos lucros, mas será uma ferramenta fundamental para não cair a produção devido as informações estarem em segurança, tendo assim um bom andamento dos serviços para empresa.

2.7.3. FERRAMENTAS DE RESPOSTAS

São utilizados com a intuição de reverter as ameaças já instaladas nos equipamentos tecnológicos e na rede de comunicação da empresa, fornecendo uma importante segurança para as informações alvos de criminoso virtuais. Os métodos de contra resposta são caráter de pronto emprego, ou seja, em caso de urgência, serão acionados para sanar o problema. Antivírus que é uma ferramenta da detecção, pode ser usado para a remoção de discrepâncias, mas específico para conteúdo digital, já o Disaster Recovery (DR) é de âmbito geral para o uso da empresa.

2.7.3. DISASTER RECOVERY

Seguindo os planos na área da segurança da informação o Disaster Recovery não é aplicado exclusivamente para esse fim, pois é uma ferramenta bastante usada no ambiente empresarial com a consequência de planejar atividades crucial para a recuperação de equipamentos, infraestruturas e informações das empresas que são por muitas vezes são bem estruturadas fisicamente, mas não os protegem totalmente de ações climáticas e morfológicas numa possível situação. O DR é uma ferramenta de contra resposta a uma ocasião já empregada na empresa em forma de relatório/manual posto para o efetivo ter direcionamento na hora de uma precisão. O método de backup é caracterizado como um DR e tem preocupação de ser utilizado para recuperar os dados já guardados num dispositivo. Diante do entendimento sobre DR, podemos classificar como uma política de segurança da empresa orientado para a parte física como também da digital e classificar como uma ferramenta de resposta.

2.8 A SÉRIE DE PREPARAÇÃO CORPORATIVA DO MARCO CIVIL DA INTERNET SETOR PÚBLICO

O Projeto de Lei nº 2.126/2011, do Marco Civil da Internet no Brasil, se faz referente ao que é moderno em alguns pontos de vistas. Não só os conteúdos elaborados apresentam presciências no que se relacionam as matérias integrada no ordenamento jurídico brasileiro, como também a produção da minuta do anteprojeto de lei transpareceu atualmente no Brasil e fora empregadas com poucas oportunidades no mundo anteriormente.

O Marco Civil da Internet no Brasil é tem como base um projeto de Lei que visa elencar origens e enfatizar normas da natureza fundamental para os contatos dos ciberespaços no Brasil, de maneira que seja habilitado uma regularização minimamente no mundo virtual, tal como uma produção de equipamentos para que a União tenha uma resposta adequada às demandas alusiva, sem comprometer a função de liberdade intrínseco à internet. O proposito declarado pelo Projeto de Lei nº 2.126/2011 é manter a gama do direito inerente ao ciberespaço atualizado, apropriado aos limites da rede, garantindo a responsabilidade e o respeito aos direitos dos usuários, fixar com transparência sobre os inúmeros atores sociais atualmente nesse ambiente e direcionar critérios para a o desempenho governamental defronte a sociedade em rede.

Seguindo o que foi relatado, a importância de uma essência de um marco normativo da internet é notada. Nesse seguimento, Thompson descreve:

A internet diversamente estabelecida por um marco jurídico seria um espaço completamente aberto. Sem paredes, portas, sem cadeados, mas também sem expectativas de privacidade, sem espaços recônditos para as nossas diferenças, sem sanções sociais legítima e razoavelmente organizadas para as nossas faltas. Um espaço imediato, de confronto direto e permanente entre o bom, o ruim e o perverso. Sem granularidade expressiva. Sem civilidade. Sem liberdade, portanto. (2012)

Desse modo, não se refere da legislação que enfatiza sobre questões pontuais, mas em compostura à natureza clara e transnacional da internet, da mesma forma que à velocidade em que acontecem as mudanças nesse âmbito, uma regulamentação de integridade altamente restrita não deteria o condão de ser amplamente aplicada, tal como arremetia o risco de converter-se em algo obsoleto antes da sua própria aprovação. Posto isso, O Marco Civil deteve como ênfase respeitar suas prudências em relação as características relativas à internet, mantendo o ambiente preservado com os mesmos contatos referente ao mesmo, preservando o espaço suas interações.

3 METODOLOGIA

O estudo foi realizado com base na coleta de informações bibliográfica oriundas de livros, artigos científicos e conhecimentos adquiridos através de leituras específicas, com o objetivo de descrever, orientar e policiar sobre os principais riscos ao banco de dados de empresas, redes públicas e os fatores que afetam a sua segurança. Perante a uma sociedade cada vez mais informatizada, os perigos de um ciber-ataque a uma rede de dados corporativa pública, só avança. Filiar alguns parâmetros preventivos e sempre debater sobre prováveis ameaças, pode suceder em pontos para as instituições.

Para certificar uma boa segurança das informações de um banco de dados em uma rede de uma determinada instituição, é indispensável um investimento de boa qualidade na área de TI, até mesmo que esse investimento não traga um retorno instantâneo às empresas. A doutrina aplicada aos estudos da Segurança da informação condiz é uma forma de prevenir de perda nas quais; o usuário tenha a informação contida em um banco de dados ou uma rede, sempre se estará a dispor, de forma confiável e íntegro para seus funcionários, tratando assim a continuidade dos processos realizada pelas instituições e empresas, que não assente em pessoas mal-intencionadas.

4 CONSIDERAÇÕES FINAIS

Essa pesquisa relata a importância do setor tecnológico operacional na rede corporativa no cenário atual com o avanço demasiado dos compartilhamentos das informações orientado pelo uso da rede de comunicação na finalidade de crescer as atividades estabelecidas pelas empresas com impulso aos negócios num âmbito da união das organizações e na operacionalidade dos serviços oferecidos.

Sobre o avanço em que o mundo nos oferece, a tecnologia é sempre motivo de alertas, pois com a evolução, a tecnologia evolui junto trazendo desafios para os gestores de TI das empresas tanto para a segurança, quanto para a estrutura. A informação é considerada como um dos patrimônios mais importante da empresa em consequência disso a demanda de ameaças virtuais aumentou muito no intuito de resgatarem informações pessoais ou da rede corporativa para a finalidade de fins lucrativo dos crackers.

Em detrimento dos impasses constantes que as redes das empresas são submetidas, criaram a necessidade de questionar no cenário atual os principais perigos que arremetem as organizações e as ferramentas utilizadas na prevenção, detecção e contra resposta dos sinistros existentes.

Evidenciando a vulnerabilidade encontrada nos processos de informações atuais e a difícil tarefa dos profissionais de TI para se prevenir de ameaças que trafegam nas redes de comunicações e internet, ainda pode-se ressaltar o usuário físico, talvez com a maior vulnerabilidade dentre as maiorias já pesquisados, pois as informações em sua parcialidade são manuseadas por eles fornecendo os maiores perigos para os dados das empresas. Podemos questionar que a segurança total é uma teoria distante da prática, nem a evolução constante das tecnologias é o suficiente para manter as informações em segurança, e os 100% de objetividade pode ser aproximado se houver uma gestão ativa de políticas de segurança conjunto as ferramentas mencionadas.

Portanto a segurança da informação está longe de um trabalho unitário, pois depende da colaboração não só dos gestores, mas sim da conscientização de todos os colaboradores que fazem uso das informações, desde o simples funcionário até o diretor da corporação devem ter conhecimento da importância de tomar os devidos cuidados de segurança na operação dos equipamentos transmissores das informações.

5 REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, Nonata S. **Segurança da Informação (TI)**. Administradores, Fortaleza, jul. 2008. Disponível em: <http://www.administradores.com.br/artigos/tecnologia/seguranca-da-informacao-ti/23933/>. Acessado em 09/09/2018

BORGES, Marcio Vieira. **Vírus e antivírus**. Trabalho apresentado a matéria de segurança digital, Universidade do Estado da Bahia, Campus II – Alagoinhas, 2014.

BRASIL. Santo Digital. **Segurança no data center: como é feita?** Disponível em: <http://www.santodigital.com.br/seguranca-no-data-center-como-e-feita/>. Acessado em 18/09/2018

BRASIL. IntroduceTI – tecnologia para crescer. **O que é política de Segurança da Informação (PSI)?** Disponível em: <http://introduceTI.com.br/blog/o-que-e-a-politica-de-seguranca-da-informacao-psi/>. Acessado em 13/09/2018

BRASIL. Brlink. **O que é Disaster Recovery e porque um gestor de TI precisa se preocupar com isso?** Disponível em: <https://www.brlink.com.br/blog/aws/o-que-e-disaster-recovery/>. Acessado em 09/09/2018

BRASIL. **Invasão**. Disponível em: <http://www.invasao.com.br/coluna-andre-09.htm>. Acessado em 01/09/2018

BRASIL. **Meu positivo**. Disponível em: <https://www.meupositivo.com.br/panoramapositivo/seguranca-da-informacao/>. Acessado em 14/09/2018

BRASIL. Redação E-Commerce News. **5 formas de prevenção contra crimes virtuais**. Disponível em: <https://ecommercenews.com.br/noticias/dicas/5-formas-de-prevencao-contracrimenes-virtuais/>. Acessado em 13/09/2018

BRASIL. **EXAME**. Disponível em: <https://exame.abril.com.br/mercados/entenda-o-que-e-bitcoin/>. Acessado em 01/09/2018

BRASIL. **PCrisk**. Disponível em: <https://www.pcrisk.pt/guias-de-remocao/7496-cryptowall-virus>. Acessado em 12/09/2018

BRASIL. **Tecmundo**. Disponível em: <https://www.tecmundo.com.br/seguranca/196-o-que-e-um-trojan-.htm>. Acessado em 09/09/2018

BRASIL. **Afrikatec**. Disponível em: <http://www.afrikatec.com.br/serie-a-evolucao-do-ransomware-parte-2-a-origem/>. Acessado em 01/09/2018

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de segurança para internet**, 2018. Disponível em: <https://cartilha.cert.br/malware/>. Acessado em 01/09/2018

LISKA, Allan; GALLO, Timothy. **Ransomware defendendo-se da extorsão digital**. São Paulo. Ed. Novatec, 2017.

MARCIANO, João Luiz Pereira. **Segurança da Informação** - uma abordagem social. 2006. 211 f. Tese apresentada ao Departamento de Ciência da Informação e Documentação da Universidade de Brasília, Brasília, 2018. Acessado em 01/09/2018

MEDEIROS, Carlos Diego Russo. **Segurança da Informação: Implantação de Medidas e Ferramentas de Segurança da Informação**. 2001. 75 f. Joinville, 2005. Disponível em: http://www.linuxsecurity.com.br/info/general/TCE_Seguranca_da_Informacao.pdf. Acessado em 11/09/2018

MONTEIRO, Emiliano Soares. **Segurança em Ambientes Corporativos**. Florianópolis: Visual Books, 2003.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec Editora, 2007.

REIS, Verônica Lagrange Moutinho dos. **Criptografia, Segurança de Dados e Privacidade** - Até que ponto pode-se confiar na discrição dos computadores? 1989.

RODRIGUES, Vanessa. **Modulo II – Segurança de Redes**. Tese apresentada ao instituto de ensino SENAC, Rio Grande do Sul, 2015.

SYMANTEC CORP. Social Media Protection Flash Poll 2011. **In: ADDED Soluções em tecnologias da informação**. Riscos nas Redes Sociais - Alerta às empresas que não preservam conteúdo relacionado aos negócios nas redes. Disponível em: <http://www.added.com.br/noticia/riscos-nas-redes-sociais.html>. Acessado em 17/09/2018

SZYMANSKI, Thiago. **3 mil pessoas são vítimas de ciber Crimes no Brasil a cada hora**. Relatório divulgado pela Symantec engloba valores de perdas em 24 países. Brasil está acima da média. 2011. Disponível em: <https://www.tecmundo.com.br/crime-virtual/13579-3-mil-pessoas-sao-vitimas-de-ciber-crimes-no-brasil-a-cada-hora.htm#ixzz1c04qfPUg>. Acessado em 17/09/2018

NOBRE, Anna C. S; Ramos, A. S. M; Nascimento, T. C. **Fatores que influenciam a aceitação de práticas avançadas de gestão de segurança da informação: um estudo com gestores públicos estaduais no Brasil**. Rio de Janeiro: XXXIV Anpad, 2010.

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Normalização Definição** Disponível em <http://www.abnt.org.br/normalizacao/o-que-e/o-que-e> acesso em 09 nov. 2020

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de Informação com Internet**. Rio de Janeiro: LTC, 1999.

FONTES, Edison. **Políticas e Normas para a Segurança da Informação**. Rio de Janeiro: Brasport, 2012.

GEUS, Paulo Lício de; NAKAMURA, Emilio Tissato. **Segurança de Redes em ambientes corporativos**. São Paulo: Novatec, 2007.

OLIVO, CK. **Avaliação de características para detecção de phishing de email**. Dissertação(mestrado), Pontifícia Universidade Católica do Paraná, Curitiba, 2010.

THOMPSON, Marcelo. **Marco civil ou demarcação de direitos? Democracia, razoabilidade e as fendas na internet do Brasil**. **RDA-Revista de Direito Administrativo**, Rio de Janeiro, v. 261, p. 203-251, set./dez. 2012. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/8856/7678>

AMARAL, Francisco. **Direito Civil: Introdução**. 7.ed. Rio de Janeiro: Renovar, 2008.