INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO

CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

JOSÉ ADAILTO LOPES

SEGURANÇA DA INFORMAÇÃO NA CLOUD COMPUTING

Floresta

2016

JOSÉ ADAILTO LOPES

SEGURANÇA DA INFORMAÇÃO NA CLOUD COMPUTING

Monografia submetida ao Curso Superior de Tecnologia em Gestão da Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – Campus Floresta, como requisito obrigatório para obtenção do grau de Tecnólogo em Gestão da Tecnologia da Informação.
Orientador: Prof. Esp. Elismar Moraes dos Santos.

Floresta

2016

"Procure a sabedoria e aprenda a escrever os capítulos mais importantes de sua história nos momentos mais difíceis de sua vida"

(Augusto Cury)

L864s Lopes, José Adailto.
Segurança da Informação na Cloud Computing ./ José Adailto Lopes – 2016.
63f. il.
Monografia (Tecnólogo em Gestão de Tecnologia) – Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – Campus Floresta. Floresta, 2016.
Orientação: Prof. Esp. Elismar Moraes dos Santos

. 1. Segurança da Informação . 2. Cloud Computing . 3. Disponibilidade.
I. Título.

CDD: 005.82

JOSÉ ADAILTO LOPES

SEGURANÇA DA INFORMAÇÃO NA CLOUD COMPUTING

Monografia apresentada ao curso de graduação em Gestão da Tecnologia da Informação pelo Instituto Federal do Sertão Pernambucano, Campus Floresta, como requisito parcial para obtenção do grau de tecnólogo.

Aprovado em 09 de outubro de 2016.

BANCA EXAMINADORA

Profº. Esp. Elismar Moraes dos Santos
IF Sertão Pernambucano

Profº MSc. Severino do Ramo de Paiva
IF Sertão Pernambucano

Profª MSc. Ana Patrícia Vargas Borges
IF Sertão Pernambucano

AGRADECIMENTO

Agradeço em primeiro lugar a Deus que me deu forças para que eu possa ter concluido o curso superior em Gestão da Tecnologia da Informação.

Agradeço ao meu filho Ítalo José, por ser minha inspiração, minha fonte de energia, o motivador de todas as conquistas já alcançadas, e as quais almejo alcançar.

Agradeço a meu pai Adailto Anacleto Lopes e minha mãe, Ivanilde Maria da conceição Lopes, os quais batalharam para dar-me todas as condições para seguir com meus estudos.

A minha esposa, Rosana Iracir de Almeida, que insistiu e me inscreveu no Exame Nacional do Ensino Médio (ENEM), pois sem ela não teria dado o primeiro passo.

Àos amigos e membros do Instituto pelo apoio, Wagner Pinheiro, Lincoln Tavares, Jelcimar Souza, Henrique Monteiro, Ailson Calaça, Altair de Assis, entre outros. Em especial ao Professor Elismar Moraes, o qual dedicou parte do seu tempo e contribuiu através de suas orientações a conclusão do curso Gestão da Tecnologia da Informação.

Agradeço a vida por existir, e proporcionar momentos de superação e vitórias os quais estou vivendo.

RESUMO

Esta monografia apresenta uma ampla visão de como garantir a segurança dos dados em ambiente virtual chamada de *Cloud Computing* conhecido popularmente como Computação em Nuvem. Tem como objetivo principal mostrar de forma conceitual o que seria Segurança da Informação, e seus respectivos pilares ou principios, os quais uma empresa de *DATACENTER* deve adotar para que assim possa garantir aos usuários a segurança e a disponibilidade das informações. Busca ainda abordar sobre Cloud Computing, como de fato suas infraestruturas funcionam, destacando empresas fornecedoras de serviços, modelos de implantação, e suas respecitivas vantagens e desvantagens. E como proposta do trabalho, apresentar técnicas por meio de testes, algumas ferramentas que contribuem para que as informações tenham um alto nível de segurança.

Palavras-chave: *Cloud Computing*, Segurança da Informação, Disponibilidade.

ABSTRACT

This monograph presents an wide portrait on how to assure data security on virtual environment called Cloud Computing. It aims to demonstrate in a conceptual manner what would Information Security be as well as its respective pillars and principles on which a ordinary DATACENTER company must comply in order to assure its users with information security and availability. It also aims to approach Cloud Computing as it really keep its structure working, focusing on service providers, implementing standards and its advantages and disadvantages. As a conclusion this monograph intends to demonstrate technics through tests, some tools that support th process in order to make information possess high level of security.

Keywords: Cloud Computing, Information Security, Availability.

SUMÁRIO

1 INTRODUÇÃO

O paradigma da Computação em Nuvem parte do princípio de que todos os recursos de infraestrutura de TI (*hardware, software* e gestão de dados e informação), até então tratada como um ativo da empresa usuária passa a ser acessados e administrados por estas através da *internet* (Nuvem) com o uso de um simples navegador da rede mundial de computadores, utilizando-se qualquer tipo de equipamento – celulares inteligentes, notebooks, netbooks, desktops, etc. Fornecedores de tecnologia passam a prover a infraestrutura e os serviços capacitados para atender a essa demanda.

1.1 Definição do problema

A computação em nuvem está cada vez mais presente no dia a dia das empresas, assim, este estudo visa discutir sobre a segurança da informação aplicada à computação em nuvem através de conceitos e seus princípios.

Nesse cenário delineia-se uma série de questões que ainda precisam ser respondidas, afim de que se possibilite a sua plena utilização e adoção sem receios pelas empresas e usuários a respeito da segurança da informação. Por fim, há uma preocupação com os dados dos usuários sendo transmitido aos servidores na nuvem, o que pode representar um possível risco para aos mesmos. À medida em que as informações são transferidas para a nuvem, pessoas e organizações ficam preocupadas ao imaginar como estes dados serão armazenados e processados na nuvem. O fato dos dados estarem armazenados em vários locais, muitas vezes de forma transparente em relação ao seu ponto de localização, provoca insegurança quanto ao nível de privacidade a que estão expostos. Abordar sobre *Cloud Computing* analisando como funciona os serviços oferecidos por empresas como *Google*, *Amazon*, *Vmware*, *Microsoft*, analizar as vantagens e desvantagens de cada serviço oferecido, além de propor técnicas e citar algumas ferramentas para melhoria da segurança da informação na Computação na Nuvem.

O paradigma da Computação em Nuvem que está fundamentado na utilização de ferramentas fortemente difundidas em Tecnologia da Informação e Comunicação (TIC), (*Next Generation*, 2009) tem como principal característica a transformação dos modos tradicionais de como empresas utilizam e adquirem os recursos de TIC. Na adoção do modelo de Computação em Nuvem os processos de negócios e procedimentos precisam levar em conta a segurança e privacidade das informações que ficarão na nuvem, (CASTRO; SOUSA 2010).

Uma das grandes questões sobre Computação nas Nuvens está relacionada à segurança dos dados. Muitas empresas têm se preocupado com a segurança das informações, a integridade e os custos de manter as informações nas nuvens.

Os questionamentos de como lidar com a segurança das informações armazenadas na nuvem, nos leva à busca de soluções que visam padronizar a adoção dos serviços da nuvem, (CASTRO; SOUSA, 2010, p. 1).

Garcia *et al* (apud CLAUNCH, 2008) diz que os recursos de TI são fornecidos aos clientes através da *Internet*. Em outras palavras, a computação em nuvem é uma solução em que todos os recursos de informática (*hardware*, *software*, redes, armazenamento) são fornecidos aos usuários sem a necessidade de uma infraestrutura presente, somente virtual.

Dias *et al* (2012, apud CASTRO, 2011; CLESSIO, 2008) diz que Segurança da informação nada mais é do que garantir a integridade e proteção das informações de uma organização. Entretanto, o conceito de segurança da informação não se baseia apenas na proteção dos dados dentro de um computador, mas também dentro de um sistema, do ambiente externo à infraestrutura da empresa.

Segundo Cléssio (2008), informação é todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Portanto essa informação deve estar bem protegida para que nenhuma pessoa com más intenções possa ter o acesso, para que de alguma forma, possa prejudicar a empresa e/ou a alguém em específico.

Apesar da diversidade de benefícios oferecida pela computação em nuvem, na qual será discutida neste estudo, existem algumas situações que precisam ser mais bem analisadas, para que as empresas possam usufruir desta tecnologia sem maiores problemas.

É o caso da segurança da informação. Como ocorre a segurança da informação na computação nas nuvens? Ela é realmente segura e eficaz? Como então garantir uma maior segurança da informação na *Cloud Computing*? A esses questionamentos pode-se dizer que, há ferramentas tecnológicas e provedores de serviços que contribuem para a segurança das informações armazenadas na computação em nuvens.

1.2 OBJETIVO GERAL

Compreender como ocorre a segurança da informação na computação nas nuvens

1.3 OBJETIVOS ESPECÍFICOS

- Apontar conceitos sobre *Cloud Computing*;
- Levantar conceitos sobre segurança da informação;
- Analisar o funcionamento e os serviços oferecidos em *Cloud Computing*;
- Propor técnicas de melhoria de segurança da informação na Computação nas Nuvens.

1.4 IMPORTÂNCIA DA PESQUISA

A importância desta pesquisa se dá pela necessidade de estudo mais detalhado de como funcionam os mecanismos de segurança da informação no contexto da computaçào nas nuvens. A proposta é dar uma visão geral de possíveis falhas ou vulnerabilidades que possam ser encontradas nas informações de usuários e empresas que estão armazenadas ou processadas em ambientes nas nuvens e apresentar por meio de estudo teórico, formas de como garantir que estes dados possam ter um nível aceitável de segurança.

1.5 MOTIVAÇÃO

A motivação pessoal para escolha do tema surgiu pelo interesse com o estudo adquirido no transcorrer do curso de Gestão da Tecnologia da Informação (GTI), com a disciplina, Segurança e Auditoria de Sistemas. Diante do que foi visto durante tal disciplina, foi possivel perceber que ainda existem paradigmas a serem arbordados com relação ao uso de *Cloud Computing* que leva os usuários se sentir inseguros ao utilizarem esse tipo de tecnologia para hospedar suas informações.

1.6 METODOLOGIA

A metodologia utilizada nesta pesquisa foi a qualitativa através de levantamento bibliográfico em fontes como: artigos, monografias, dissertações, revistas técnicas e outros.

Entende-se por pesquisa qualitativa aquela que procura não enumerar ou medir os fenômenos ou eventos estudados nem utiliza a análise estatística dos dados (GODOY, 1995). Assim, a pesquisa qualitativa busca compreender um fenômeno através de uma análise holística, com a coleta de diferentes tipos de informações no contexto em que o fenômeno ocorre, Miguel, (2007 apud YIN, 2001).

O levantamento bibliográfico, de acordo com Cunha, *et al* (2009 apud OLIVEIRA 2002), tem por finalidade conhecer as diferentes formas de contribuições científicas realizadas sobre determinado assunto ou fenômeno. Este tipo de pesquisa para Neuls (2012 apud MARTINS, 2002), tem como objetivo de recolher, selecionar, analisar e interpretar as contribuições teóricas já existentes sobre determinado assunto.

2 VISÃO GERAL DA SEGURANÇA DA INFORMAÇÃO

O item que ora se discute versa sobre a visão de Junior (2014). Assim ele comenta que, no dia 24 de novembro de 2014, a *Sony Pictures* passou a viver um pesadelo. A gigante da indústria do entretenimento sofreu um ataque *hacke*r que deixou um recado em todos os computadores da empresa com a assinatura "*Hacked by* #GOP". A partir de então, instaurou-se um clima tenso e o expediente foi encerrado para a maioria de seus funcionários.

O #GOP que assina a ação é uma sigla para "Guardians of Peace" (Guardiões da Paz). Trata-se de um grupo pouco conhecido, mas forte. Para Joseph Demarest, subdiretor da divisão de crimes virtuais do FBI, o malware que afetou a Sony é tão sofisticado que poderia contaminar 90% dos sistemas de segurança disponíveis atualmente. A única pista divulgada por enquanto é que o ataque teve origem em um hotel tailandês de cinco estrelas (JUNIOR, 2014).

Entre as consequências do ataque hacker está o vazamento de conteúdos secretos sobre filmes ainda não lançados pela Sony Pictures. Os vídeos estavam salvos em backups para serem enviados a agências ou outras pessoas. De Acordo ainda com o autor acima mencionado, cinco obras foram compartilhadas na *Internet* em alta qualidade: *Fury*, protagonizado por Brad Pitt; foi baixado mais de 1 milhão de vezes em 3 dias; *Annie*, protagonizado por Cameron Diaz; *Mr. Turner*, com Timothy Spall; *Still Alice*, protagonizado por Julianne Moore; *To Write Love on Her Arms*, com Rupert Friend.

Detalhes e especulações sobre outros filmes também foram divulgados. Os planos do produtor Matt Tolmach de abortar o filme do vilão Venom para colocá-lo no *Sexteto Sinistro*, por exemplo, foram revelados. Da mesma forma, descobrimos que Tom Cruise foi cotado para estrelar a cinebiografia de Steve Jobs. Mais essas questões são apenas detalhes se compararmos com a lista de 20 prováveis filmes que devem ser lançados pela *Sony* até 2017 (JUNIOR, 2014).

Em abril de 2011, usuários da *PlayStation* ficaram supresos ao saber que conteúdos digitais e partidas *multiplayer*, serviços fornecidos pela Sony estava fora do ar., porém, a frustação se transformou em empolgação quando grupos de hackativismo assumiram a autoria do ataque que levou a rede a ficar *offline*. O ataque foi motivado pelo processo que a Sony moveu contra o jovem George Hotz (Geohot), responsável pelo desbloqueio do *Playstation 3*. Na ocasião, os serviços fornecidos pela empresa ficaram fora do ar, consequentemente 77 milhões de pessoas ficaram sem acessar os serviços fornececido pela mesma. Além disso, os dados de mais de 24 milhões de contas foram roubados, contendo informações valiosas e que não estavam protegidas por criptografia, como números de cartões de crédito, senhas e histórico de compras. O prejuízo para a Sony foi de US$ 24 bilhões (ARRUDA, 2012).

Em março de 2011, as companhias de segurança *Symantec* e *Kaspersky* reportaram diversas tentativas de invasão aos seus bancos de dados. Porém, o grande afetado pela onda de ataques criminosos foi a RSA *Security*, que teve diversos de seus dados roubados por hackers não identificados. Esse fato é especialmente preocupante por que se relata de uma empresa que é a responsável por desenvolver ferramentas as quais prometem blindar milhares de sistemas contra invasões. Se nem mesmo as companhias que dispõe da última palavra em segurança estão protegidas, quais as esperanças que um usuário comum pode ter contra a ação dos criminosos virtuais? (GUGELMIM, 2011).

Em fevereiro de 2008, uma das maiores empresas petrolíferas do mundo teve computadores portáteis furtados com informações estratégicas de uma reserva gigante, descoberta no ano anterior, estimada em torno de 8 bilhões de barris de petróleo, sendo considerada uma das maiores descobertas de petróleo dos últimos anos. As notícias sobre esse evento ocuparam as principais manchetes na mídia mundial, além de exporem a fragilidade da segurança da informação em uma empresa multinacional, o que provocou a apreensão nos seus acionistas, (DANTAS, 2011).

Em 26 dezembro de 2004, um evento da natureza causou um grande estrago na

Indonésia. As ondas gigantes, conhecidas como tsunami, não só acabaram com vidas, como também destruíram povoados, empresas, e levaram junto com elas centenas de milhares de vítimas e o que encontrasse pela frente, e todos pegos de surpresa. As imagens dessa catástrofe natural também serão difíceis de ser esquecidas. Especialistas afirmam que sistema de alarme e de emergência instalados depois da catástrofe natural não funcionam de forma adequada devido a falta de manutenção, FOLHA DE S.PAULO (2012)

Esses acontecimentos refletem o quanto é complexa a questão da segurança. Se, de um lado, os ataques causasos por *hackers* mostraram os efeitos dos riscos de uma ação intencional que abala fortemente o sistema de segurança da informação de grandes empresas, por outro lado, as *tsunamis* deixaram claras as consequências dos riscos dos eventos da natureza, como também as falhas nos cuidados com o transporte de equipamentos como, informações estratégicas sobre importante descoberta de petróleo (DANTAS 2011).

Ainda de acordo com o autor, esses exemplos levantam uma questão peculiar: a proteção das informações. Em ambos os acontecimentos (ataques terroristas e *tsunami*), muitas informações foram destruídas e com elas muitos negócios. As empresas que foram atingidas por esses fatos puderam continuar com suas atividades de negócios? As empresas que retornaram às suas atividades possuíam um plano de recuperação de desastres? Quantas pessoas morreram em consequência de equipamentos e sistemas que deixaram de funcionar?

> E esses fatos levantam uma questão sobre a forma de proteção da informação. Para que isso aconteça, basta uma simples ação desatenciosa de um funcionário ao desabilitar o sistema de proteção de invasão e provocar um ataque de invasão ou negação de serviço, indisponibilizando os sistemas por algum período, ou ao negligenciar em não verificar periodicamente os equipamentos do sistema de detecção de incêndio, prejudicando o tempo de resposta ao fogo, levando à propagação de um incêndio na área do Centro de Processamento de Dados (CPD), destruindo todos os sistemas de informação da empresa. (DANTAS, 2011, p. 134)

2.1 Conceito de Segurança da Informação

Já citado anteriormente, Castro (2011) diz que Segurança da informação nada mais é do que garantir a integridade e proteção das informações de uma organização. Entretanto, o conceito de segurança da informação não se baseia apenas na proteção dos dados dentro de um computador, mas também dentro de um sistema, do ambiente externo à infraestrutura da empresa.

Segurança da Informação, de acordo com o site OFICINADANET (2008), está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade e disponibilidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados. O conceito de Segurança Informática ou Segurança de Computadores está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

Outro conceito importante é mencionado por Sêmola (2003) quando define a Segurança da Informação, como a proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto os pessoais. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas más intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

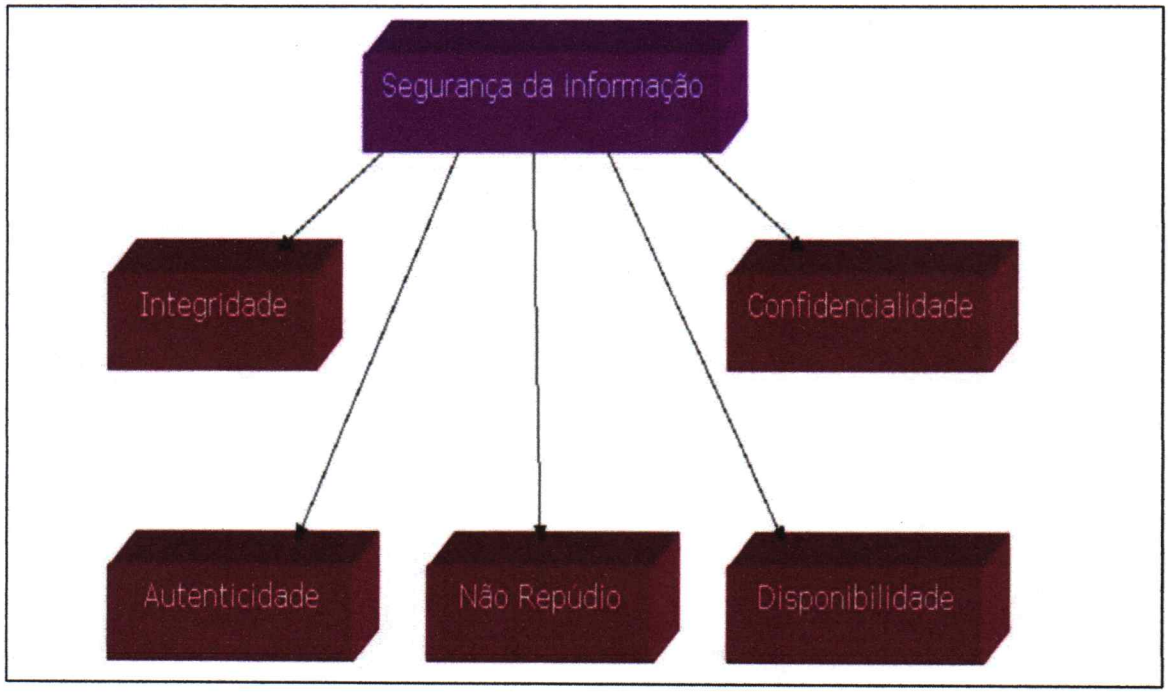
Segurança da informação pode ser definida como a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de possibilidades e investimentos. A segurança da informação é caracterizada pela preservação dos três atributos básicos da informação: confidencialidade, integridade e disponibilidade de acordo com o que diz Machado (2002 *apud* ISO/IEC 17799:2000).

2.2 Princípios básicos da Segurança da Informação

Segundo Clésio (2008), informação é todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Portanto essa informação deve estar bem protegida para que nenhuma pessoa com más intenções possa ter o acesso, para que de alguma forma, possa prejudicar a empresa e/ou a alguém em específico.

Filho (2004) diz que a Confidencialidade, Integridade e Disponibilidade são os princípios que dão base para poder pensar em iniciar qualquer projeto de segurança em qualquer empresa. Outros pontos que também devem ser levados em consideração são a autenticidade, o não repúdio, e nos últimos tempos, principalmente, a privacidade das informações.

A Figura 1 mostra os cinco pilares da segurança de informação



Fonte: (FILHO, 2004)

Estes pilares representam o que uma empresa de *DATACENTER* deve garantir ao cliente quando oferece o serviço de computação em nuvens.

Nos dois primeiros blocos da esquerda da Figura 5, têm-se Integridade e Confidencialidade, significa que a empresa que está oferecendo o serviço devendo garantir que os

dados não irão sofrer nenhuma alteração, mantendo sempre suas características originais, e permitindo que apenas pessoas autorizadas tenham acesso as informações salvas no banco de dados no servidor.

Os outros três blocos da Figura 1 são Autenticidade, Disponibilidade e Não Repúdio.

- A autenticidade significa que as informações não sofrão nenhuma alteração, mantendo-as sem modificações e garantindo que sejam sempre as mesmas.
- A disponibilidade é a garantia que usuário tenha condições de acesso ao sistema, arquivo ou informação a qualquer momento que ela acesse estas informações, estará sempre disponíveis para visualização, 24/7 (24 horas por dia, 7 dias por semana).

- Não Repúdio é o que irá garantir que ninguém negue aquela informação, sempre tendo o autor aqueles dados.

Na criação de proteção para os dados utilizam-se dois métodos para o controle: os físicos e os lógicos. O controle físico pode ser feito por um método de autenticação, usando biometria ou cartão de acesso. Os lógicos são sistemas, *softwares* e ferramentas que auxiliam a segurança dos dados, Filho (2004).

De acordo com Reicher, (2011 apud CUNHA, 2005), são definidos como ameaças os agentes ou condições que venham a causar incidentes que comprometam as informações por meio de exploração de vunerabilidade podendo assim causar um grande impacto nos negócios de uma organização ou de uma pessoa, tendo como consequência a perda de confidecialidade integridade e disponibilidade. Tais ameaçãs são classificadas quanto a sua intencionalidade, sendo divididas nos seguintes grupos:

- Naturais: ameaças decorrentes de fenômenos da natureza, como por exemplo, incêndio aquecimento, poluição, etc;
- Involuntárias: ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia, etc;
- Voluntária: ameaças propositais causadas por agentes humanos, como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador.

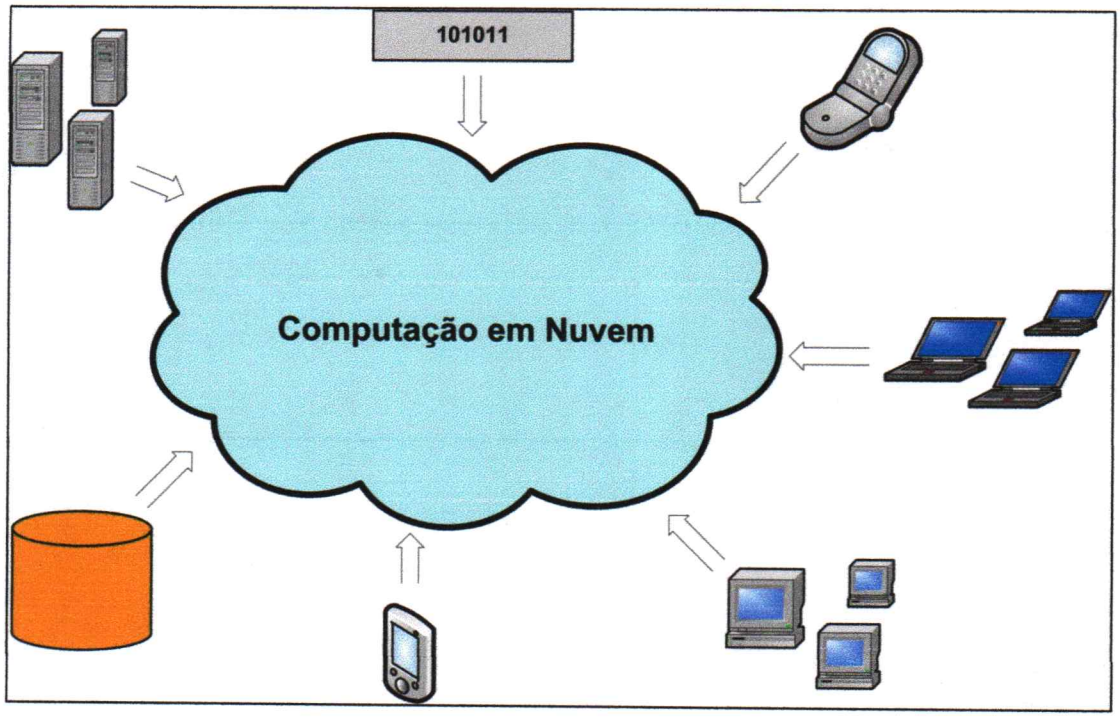
Para as pequenas e médias empresas, segurança da informação deve ser tratada com o máximo de cuidado possível. Isso porque se trata de uma organização em crescimento, e qualquer erro com as informações pode acarretar em perdas drásticas, comprometendo toda a instituição. Até porque os riscos sempre irão existir, assim como existe na vida. A questão é trazer o grau de risco a um nível aceitável, de modo que possamos evoluir na ultilização de tecnologias a um patamar mais confiável e consequentimente, mais eficaz, Reicher (2011 apud CUNHA, 2005).

3 *CLOUD COMPUTING*: CONCEITOS E CARACTERÍSTICAS

Com o avanço da sociedade humana moderna, serviços básicos e essenciais são entregues a quase todos de uma forma completamente transparente. Serviços de utilidade pública como água, eletricidade, telefone e gás tornaram-se fundamentais para nossa vida diária

e são explorados por meio do modelo de pagamento baseado no uso. As infra-estruturas existentes permitem entregar tais serviços em qualquer lugar e a qualquer hora, de forma que possamos simplesmente acender a luz, abrir a torneira ou usar o fogão. O uso desses serviços é, então, cobrado de acordo com as diferentes políticas para o usuário final. Recentemente, a mesma ideia de utilidade tem sido aplicada no contexto da informática e uma mudança consistente neste sentido tem sido feita com a disseminação de *Cloud Computing* ou Computação em Nuvem, (SOUSA; FLÁVIO *et al.* apud VECCHIOLA, 2009).

A Figura 2 mostra uma visão geral de uma nuvem computacional.



Fonte: Sousa, *et al* (2009)

Com isso, os usuários estão movendo seus dados e aplicações para a nuvem e assim poderão acessá-los de forma simples e de qualquer local desde que tenha acesso à *Internet.*

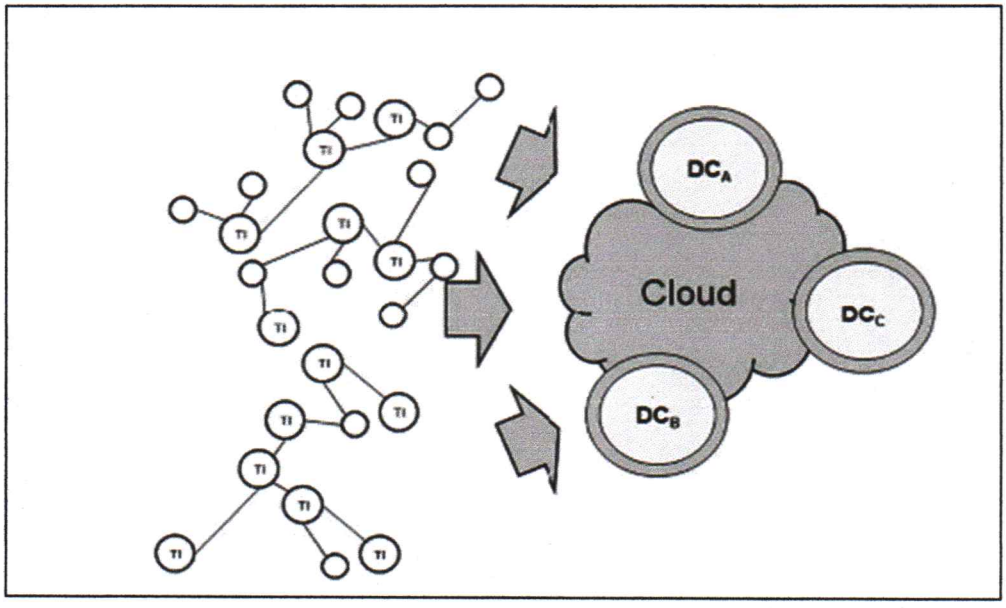
Na computação em nuvem, os recursos de TI são fornecidos como um serviço, permitindo aos usuários acessarem seus dados sem a necessidade de conhecimento sobre a tecnologia utilizada. Assim, os usuários e empresas passaram a acessar aplicações as quais a *Cloud Computing* oferece sob demanda independente de localização, o que aumentou a quantidade de serviços, como: armazenamento, processamento, compartilhamento, *web,* etc.

O conceito do que seria *Cloud Computing* ainda se aprimora. A ideia inicial da *Cloud Computing* foi processar as aplicações e armazenar dados fora do ambiente corporativo, dentro da grande rede, em estruturas conhecidas como *DATACENTERS*, otimizando o uso dos recursos. O conceito de *Cloud Computing* hoje é mais abrangente. A arquitetura *Cloud Computing* significa mudar fundalmentalmente a forma de operar a TI, saindo de um modelo baseado em aquisição de serviços. Atualmente o serviços de *Cloud Computing* decorrente da organização em nuvem pública são fornecidos em sua grande maioria por grandes organizações como, *Google, Microsoft, Amazon, Rackspace* e outros grandes provedores regionais que hospedam e executam os aplicativos dos clientes empresariais. A nova arquitetura introduzida pela *Cloud Computing* permite que as organizações escolham o modelo adequado para a arquitetura dos seus aplicativos e onde armazenar os seus dados (VERAS, 2012)

Dias (2012), sobre esse assunto, busca definir *Cloud Computing*, como sendo um avanço tecnológico no sentido de não ter mais aplicativos instalados no próprio computador, usando tudo nas nuvens. Ou seja, não é mais necessário ocupar espaço na memória do computador local, pois os dados dos usuários estarão sendo acessados pela *Internet*. Entretanto, deve-se prestar atenção a alguns pontos negativos como, por exemplo, a indisponibilidade da *Internet*. Essa instabilidade está relacionada com o local de onde se está acessando os dados.

No que diz respeito ao Datacenter (DC), Veras (2012) diz que este é o responsável pelo armazenamento, processamento das informações contidas nas nuvens conforme ilustra a Figura 3. Ou seja, com os recursos de TI, os dados dos usuários encontram-se centralizados em grandes pontos de armazenamento e processamento, assim facilitando com que os ultilizadores possam acessar seus dados através dos *Datacenters* que é onde ficam armazenadas as informações. A nuvem na verdade é um conjunto de grandes pontos de armazenamento e processamento de dados e informações.

Figura 3- Formação da Nuvem de TI



Fonte: VERAS, 2012, p.32.

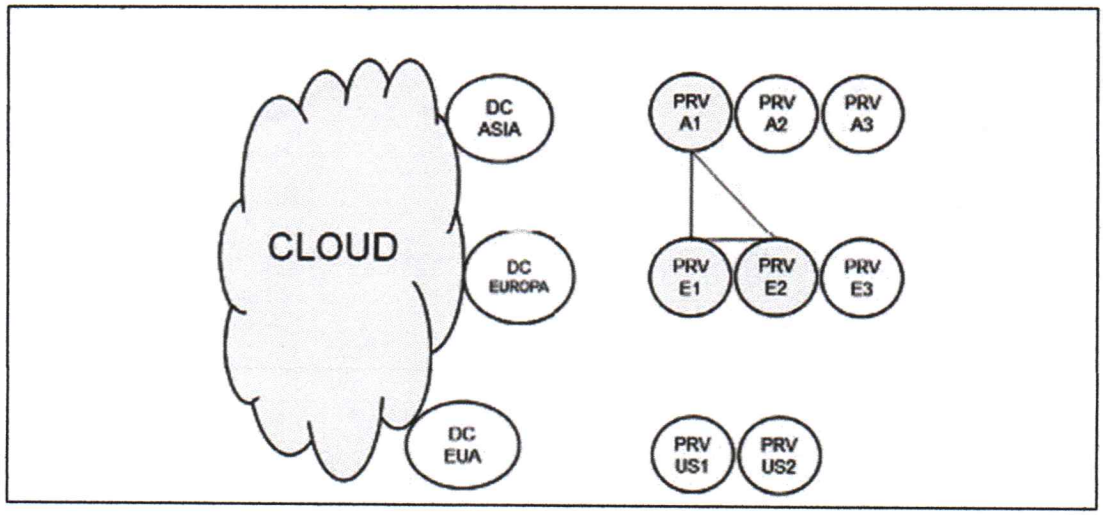
A centralização em grandes estruturas, como os *Datacenters* na arquitetura *Cloud Computing*, é viabilizada pela atual oferta de banda e pela existência de tecnologias que permitem alto poder de processamento e armazenamento em estruturas que reduzem o *Total Cost of Ownership* (TCO) da infraestrutura de TI. Estas estruturas, por outro lado, demandam muita energia e, consequente, refrigeração tornando os projetos mais complexos (VERAS, 2012).

A figura 3 ilustra a relação entre *Cloud Computing*, *Datacenter*s e Virtualização. *Cloud Computing* é formada por vários *Datacenters* e, por sua vez, os *Datacenters* são formados por diversos pools de recursos virtuais (PRV na figura 3). Estes pools de recursos podem inclusive envolver mais de um *Datacenter*.

Sobre virtualização Garcia, (2009) diz que é a capacidade de criar instâncias de sistemas operacionais virtualmente (máquina virtuais), ou seja, com pelo menos uma única máquina podemos ter vários sistemas operacionais rodando ao mesmo tempo, simulando vários servidores. Para computação em nuvem, esse é um conceito extremamente importante sendo, para muitos estudiosos da área, uma das bases da *Cloud Computing*. A virtualização nos leva inexoravelmente em direção à flexilização e ao *Cloud Computing*. Há várias coisas que a Virtualização faz para abrir as

portas da computação em Nuvem e empurrar as organizações para detro dela, são os inúmeros benefícios de virtualizar com a redução dos custos de mantenção, pois o número de máquinas é reduzido e melhora o desempenho das máquinas. Pois se a empresa possui três maquinas que ficam muito tempo ociosas a organização pode substituir essas três máquinas por apenas uma, Garcia (apud THOMAS BITTMAN, 2009).

Figura 4- Relação entre *Cloud Computing*, *DATACENTER* e Virtualização

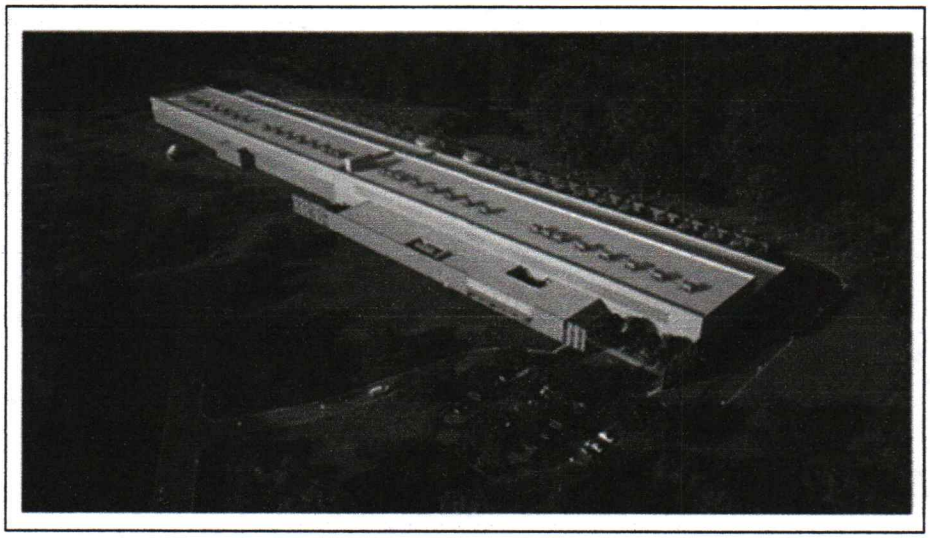


Fonte: VERAS, 2012, p.32.

O tamanho dos *Datacenters* é outra questão relevante. Qual seria o tamanho adequado? O ganho de escala e as novas tecnologias que permitem melhorar a eficiência energética têm possibilitado a construção de *Datacenters* de grandes dimensões. A figura 4 ilustra o novo *Datacenter* do Facebook, em Oregon, nos Estados Unidos.

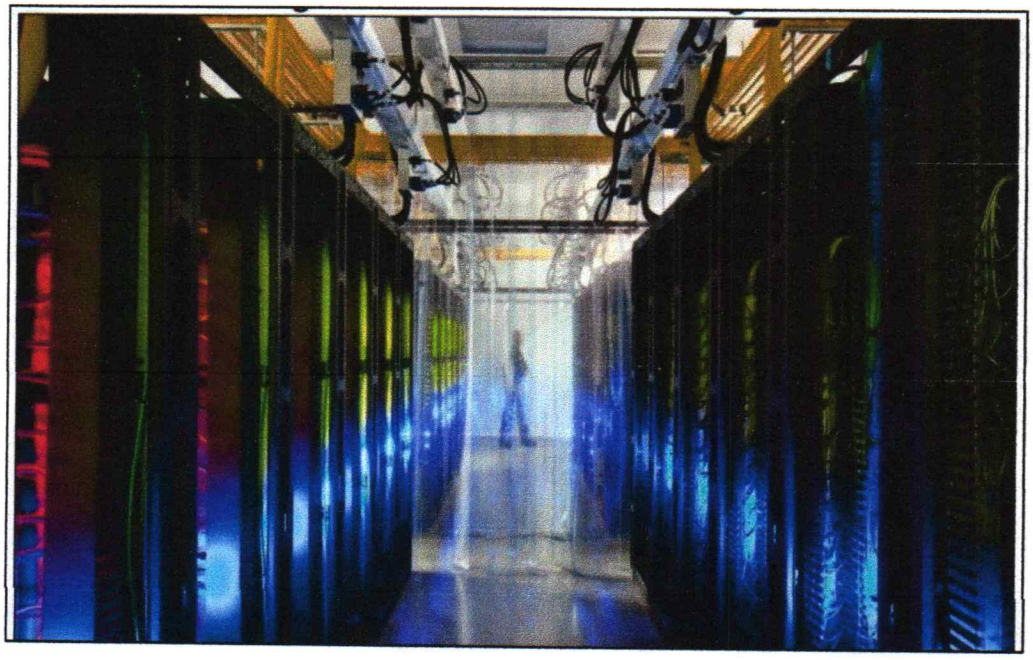
Conforme as Figuras 5 e 6, PEREIRA (2013) diz que os *Datacenters* são imensas estruturas físicas de armazenamento, que chegam a medir mais de 10.000 metros quadrados e abrigam milhões de servidores. Por questão de segurança, muitos não têm divulgados a sua localização.

Figura 5 - O novo *Datacenter* do Facebook, em Oregon, nos Estados Unidos



Fonte – VERAS, 2012, pag. 33.

Figura 6- *Datacenter* da *GOOGLE*



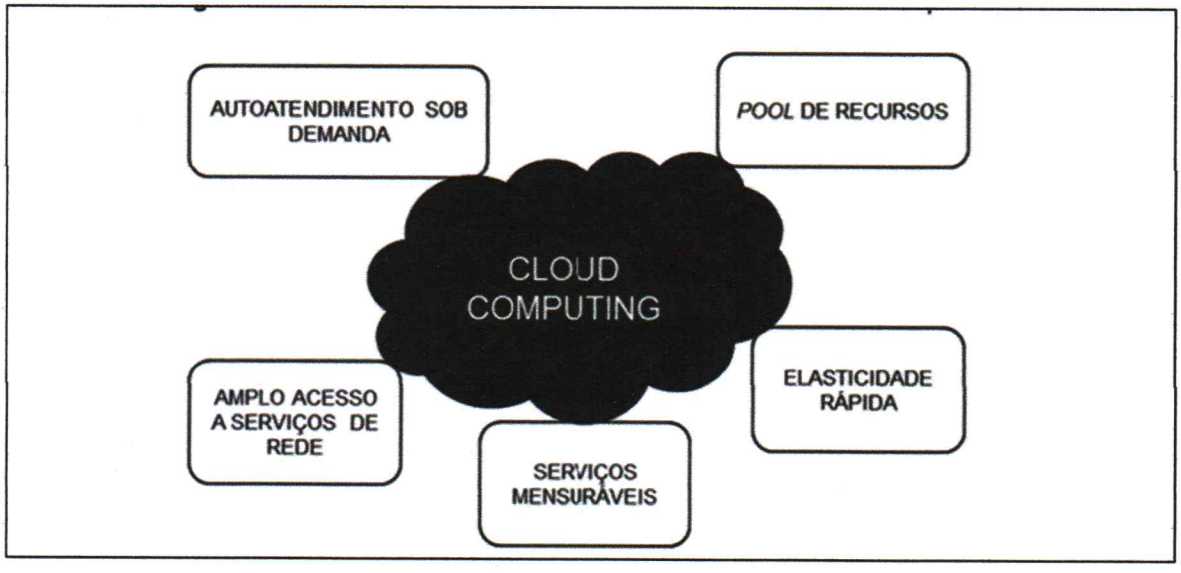
Fonte: *Google,* s.d.

3.1 Características essenciais da Computação em Nuvem

Mell *et al* (2011), cita a seguir algumas características básicas de serviços e implantação para uma *Cloud Computing*.

- Autoatendimento sob demanda: funcionalidades computacionais são providas automaticamente sem a interação humana com o provedor de serviço.
- Amplo acesso ao serviço de rede: recursos computacionais estão disponiveis através da *Internet* e são acessados via mecanismo padronizado, para que possam ser utilizados por dispositivos móveis e portáteis, computadores, etc.
- *Pool de recursos:* recursos computacionais (físicos ou virtuais) do provedor são ultilizados para servir a múltiplos usuários, sendo alocados e realocados dinamicamente conforme a demanda.
- Elasticidade rápida: as funcionalidades computacionais devem ser rápidas e elasticamente providas, assim como rapidamente liberadas. Os usuários dos recursos devem ter a impressão de que ele possui recursos limitados adquiridos (comprados) em qualquer quantidade e a qualquer momento.
- Serviços mensuráveis: os sistemas de gerenciamento utilizado pela *Cloud Computing* controlam e monitoram automaticamente os recursos para cada tipo de serviço (armazenamento, processamento e largura de banda). Esse monitoramento do uso dos recursos deve ser transparente para o provedor de serviço, assim como para o consumidor do serviço utilizado.

Figura 7 – Caracteristica da *Cloud Computing* defineda pela NIST.



Fonte – VERAS, 2012, pag. 36.

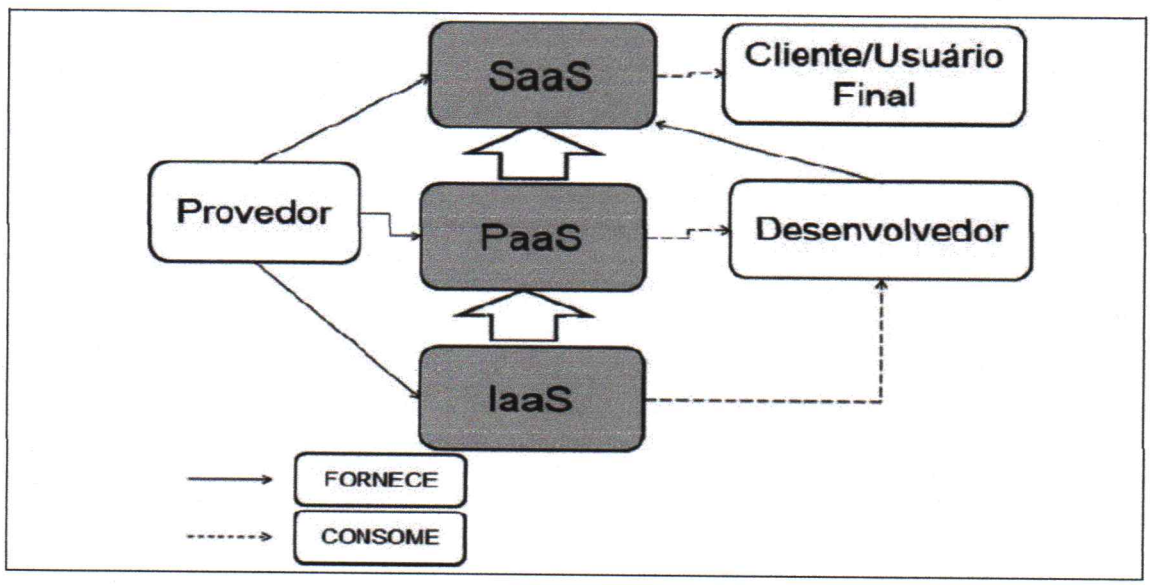
A proposta da *Cloud Computing* de acordo com VERAS (2012), é criar a ilusão de que o recurso computacional é infinito e ao mesmo tempo permitir a eliminação do comprometimento antecipado da capacidade. Além disso, a idéia é permitir o pagamento pelo uso real dos recursos. Do ponto de vista prático, os provedores, em sua grande maioria, ainda não estão preparados para disponibilizar esta forma de serviço e muitos ainda têm dificuldades de gerenciar os níveis de serviço.

3.2 Modelos de Serviços da *Cloud Computing*

Souza *et al* (2009) dizem que o ambiente de computação em nuvem é composto por três modelos de serviços. Estes modelos são importantes, pois eles definem um padrão arquitetural para soluções de computação em nuvem.

A Figura 7, ajuda a definir os atores e os seus diferentes interesses em *Cloud Computing*. Sendo que os atores podem assumir vários papéis ao mesmo tempo de acordo com seus interesses, sendo que apenas o provedor fornece suporte a todos os modelos de serviços.

Figura 8 – Papeis em *Cloud Computing*



Fonte: VERAS, 2012, pag. 38.

- Infraestrutura como serviço (*Infrastructure as a Service – IaaS*)

O IaaS é a parte responsável por prover toda a infraestrutura necessária para a PaaS e o SaaS. O principal objetivo do IaaS é tornar mais fácil e acessível o fornecimento de recursos, tais como servidores, rede, armazenamento e outros recursos de computação fundamentais para construir um ambiente sob demanda, que podem incluir sistemas operacionais e aplicativos. A IaaS possui algumas características, tais como uma interface única para administração da infraestrutura, *Application Programming Interface* (API) para interação com *hosts, switches*, balanceadores, roteadores e o suporte para a adição de novos equipamentos de forma simples e transparente. Em geral, o usuário não administra ou controla a infraestrutura da nuvem, mas tem controle sobre os sistemas operacionais, armazenamento e aplicativos implantados, e, eventualmente, seleciona componentes de rede, tais como *firewalls*.

- Plataforma como serviço *(Platform as a Service – PaaS)*

A PaaS oferece uma infraestrutura de alto nível de integração para implementar e testar aplicações na nuvem. O usuário não administra ou controla a infraestrutura subjacente, incluindo rede, servidores, sistemas operacionais ou armazenamento, mas tem controle sobre as aplicações implantadas e, possivelmente, as configurações das aplicações hospedadas nesta infraestrutura. A PaaS fornece um sistema operacional, linguagens de programação e ambientes de desenvolvimento para as aplicações, auxiliando a implementação de sistemas de *software*, já que contém ferramentas de desenvolvimento e colaboração entre desenvolvedores.

- *Software* como serviço *(Software as a Service – SaaS)*

Este modelo proporciona sistemas de *software* com propósitos específicos que estão disponíveis para os usuários através da *Internet*. Os sistemas de *software* são acessíveis a partir de vários dispositivos do usuário por meio de uma interface *thin client* como um navegador *Web*. No SaaS, o usuário não administra ou controla a infraestrutura subjacente, incluindo rede, servidores, sistemas operacionais, armazenamento ou mesmo as características individuais da aplicação, exceto configurações específicas. Com isso, os desenvolvedores se concentram em inovação e não na infraestrutura, levando ao desenvolvimento rápido de sistemas de *software*.

3.3 Modelos de Implantação da *Cloud Computing*

Segundo o guia de Segurança para áreas críticas focado em Computação em Nuvem o *Cloud Security Alliance* (CSA) (2009) V 2.1 independentes do modelo de serviço utilizado (SaaS, PaaS ou IaaS) existem quatro modelos de implantação de serviços de nuvem:

- **Nuvem privada:** nesse modelo de implantação, os serviços são operados exclusivamente por uma única organização. Os serviços podem ser gerenciados pela organização ou por terceiros, e pode existir no local ou fora do ambiente da empresa.
- **Nuvem Pública:** A infraestrutura de nuvem é disponibilizada ao público em geral ou a um grande grupo industrial e é controlada por uma organização que vende os serviços de nuvem o serviço é conhecido como pague por uso.
- **Nuvem Comunitária:** A infraestrutura da nuvem é compartilhada por diversas organizações e suporta uma determinada comunidade que partilha interesses (por exemplo, a missão, os requisitos de segurança, política ou considerações de conformidade). Ela pode ser administrada pelas organizações ou por um terceiro e pode existir no local ou fora do ambiente da empresa.
- **Nuvem híbrida:** a infraestrutura é uma composição de duas ou mais nuvens (privada, pública ou comunitária) que continuam a ser entidades únicas, porém, conectadas através de tecnologias proprietárias ou padronizadas que propiciam a portabilidade de dados e aplicações. A nuvem híbrida impõe uma coordenação adicional a ser realizada para uso das nuvens privadas e públicas.

A Oracle sugere uma comparação entre os modelos de nuvem pública e privada do ponto de vista dos benefícios obtidos.

3.4 *Benefícios comuns a nuvem pública e privadas:*

- Alta Eficiência.
- Alta Disponibilidade.
- Elasticidade.
- Rápida Implementação.

3.4.1 Benefícios da Nuvem Pública:

- Custos Iniciais Baixos.
- Economia de Escala.
- Simplicidade para Gerenciamento.
- Pagamento como Despesas Operacionais.

3.4.2 Benefícios da nuvem privada:

- Maior Controle de Segurança, compliance e qualidade de serviços.
- Mais fácil integração.
- Custos totais mais baixos.
- Despesas de capital e despesas operacionais.

3.5 Modelo para segurança da CSA

O modelo de referência para segurança desenvolvido pela CSA na versão 2.1, segundo (VERAS, 2012), demonstra de forma abrangente as relações e dependências entre os modelos de serviços da *Cloud Computing*. O modelo tem por objetivo compreender os riscos de segurança envolvido em uma solução baseada em *Cloud Computing*.

O modelo serve para entender os riscos envolvidos com a *Cloud Computing*, mesmo que a forma que alguns provedores implementem os serviços não seja exatamente assim.

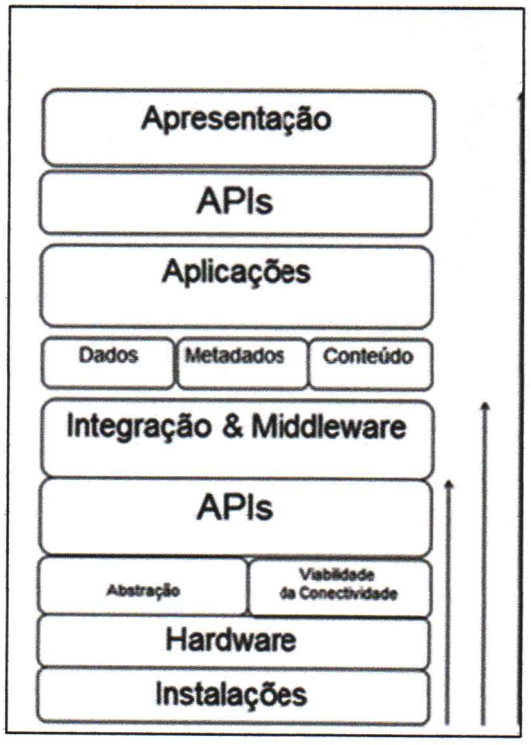
O modelo IaaS inclui os recursos de infraestrutura desde as instalações até as plataformas de *hardware* que ali residem. Incorpora a capacidade de abstrair recursos e oferecer conectividade física e lógica a estes recursos. Além de fornecer um conjunto de APIs que permitem a gestão e outras formas de interação com a infraestrutura por parte dos clientes.

O modelo PaaS acrescenta uma camada de integração com *frameworks* de desenvolvimento de aplicativos, recursos, de *middleware* e funções como banco de dados, mensagens e filas, permitindo aos desenvolvedores criarem aplicativos para a plataforma cujas linguagens de programação e ferramentas são suportadas pela pilha.

Já o modelo SaaS fornece um ambiente operacional autocontido usado para entregar

todos os recursos do usuário, incluindo o conteúdo, a apresentação, as aplicações e a capacidade de gestão.

Figura 8 – Modelo de referência para segurança de *Cloud Computing*



Fonte: VERAS, 2012, pag. 43.

3.6 Arquitetura *Multitenancy* ou Multi-Inquilino

Segundo VERAS, (2012) arquitetura *multitenancy* trata da arquitetura de aplicações onde uma única instância do *software* roda em um servidor e vários inquilinos acessam. Diferentimente da virtualização que, por sua vez, é uma arquitetura de aplicação e infraestrutura orientada a serviço e tecnologias e protocolos baseados na *Internet,* como meio de reduzir os custos de *hardware* e *software* usados para processamento, armazenamento e rede. Na arquitetura *multitenancy* os inquilinos utilizam a mesma instância do servidor e não máquinas virtuais distintas. No caso da nuvem a arquitetura *multitenancy* implica em poder forçar a aplicação de políticas, segmentação, isolamento, governança, níveis de serviços de forma diferente por perfis de usuários. As preocupações com segurança multitenancy servem tanto para provedores de nuvem pública como para nuvens privadas que possuem unidades de negócio que precisam ser separadas logicamente, mas que utilizam a mesma infraestrutura.

A arquitetura *multitenancy* sugere que o provedor de nuvem tenha abordagem de design e arquitetura que permita economia de escala, disponibilidade, segurança, isolamento, eficiência operacional, aproveitando o compartilhamento da infraestrutura, dos dados e serviços através de diferentes clientes (VERAS, 2012)

A qualidade do serviço SaaS depende da arquitetura *multitenancy*. A proposta do modelo de serviço SaaS é ter uma aplicação atendendo a múltiplos inquilinos. Importante ressaltar que inquilinos não são usuários individuais, mas empresas clientes do *software* (VERAS, 2012).

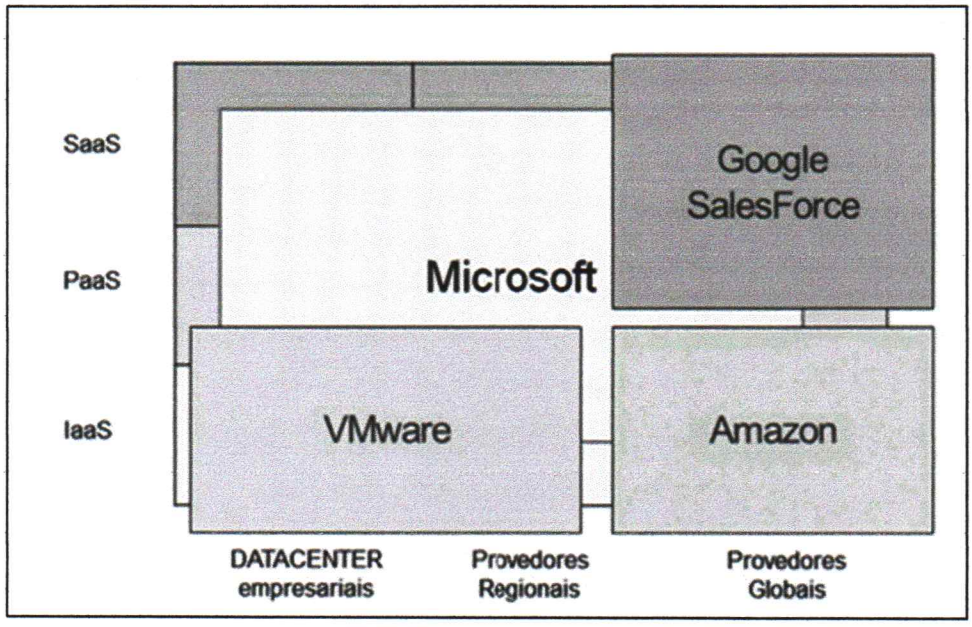
3.7 Iniciativas e Aplicabilidade

Veras (2012), destaca as principais empresas que deram iniciativa na área de *Cloud Computing*.

- *Google* e *SalesForce*: São provedores globais que estão focados em provimento de *software* como serviço (SaaS) e plataforma como serviço PaaS.
- *Amazon*: é a principal fornecedora de infraestrutura como serviço IaaS.
- *VMware*: é fornecedora de produtos de infraestrura para *datacenters* empresariais e provedores regionais que entregam IaaS.
- *Microsoft*: possui a oferta mais completa, funcionando como provedor global para solução para *datacenters* e provedores regionais.

Silva (2015) diz que, se tratando da expansão da computação em nuvem, podemos complementar que as aplicações que estão atualmente no mercado, não foram totalmente desenvolvidas aparadas no conceito de computação em nuvem, mas em algumas funcionalidades que esta tecnologia oferece, como as ferramentas de e-mail, quando as mensagens eram armazenadas no cliente de e-mail, no computador dos usuários.

Figura 9 – Iniciativas dos fornecedores de serviços de nuvem:



Fonte: VERAS (2012, pag 44).

3.8 Vantagens e desvantagens da *Cloud Computing*

Existem vantagens e desvantagens a serem consideradas ao adotar soluções de *Cloud Computing* conforme VERAS (2011) *et al* apud GUERRA (2012).

3.8.1 Vantagens

- **Menores custos de infraestrutura:** A idéia é se pagar somente pelo que consome sem ter que investir capital aos recursos de infraestrutura interna, esses tipos de fornecimento englobam serviços como, armazenar arquivos em discos (HD), diminuir a necessidade de fornecer manutenção da infraestrutura física de redes locais cliente/servidor.

- **Aumento da utilização da infraestrutura:** Custos divididos entre contratantes que utilizam de recursos de TI comuns utilizados em apoio ao provedor, tendo como objetivo reduzir custos de compras ou utilização de *software* e *hardware* coletivo, como: *firewalls*, discos (HD), módulos de memórias, switch, computadores, etc.

- **Aumento da segurança:** Uma infraestrutura centralizada pode ajudar a melhorar rotinas de *backup*, otimizá-las e testá-las, todos os dados dos sistemas podem estar alocados na estrutura contratada em um único local.

- **Acesso a aplicações sofisticadas:** Aplicações com alto custo podem ser utilizadas com recursos sob demanda, permitindo acesso a aplicações conforme as necessidades, reduzindo investimentos e alocação de recursos.

- **Economia de energia:** Redução de custo de energia e refrigeração, pois os servidores se tornam virtuais e não ficam mais no ambiente do contratante.

- **Aumento da produtividade por usuário:** Como o usuário pode acessar as aplicações disponíveis de qualquer lugar tende a ter um aumento de produtividade em sua rotina de trabalho, em qualque tipo de aplicação (sistema), torna - se disponível 24 horas por dias 7 dias por semana.

- **Aumento da confiabilidade:** com a existência de contingência quase que obrigatória, tende-se a melhorar a confiabilidade das aplicações disponíveis aos clientes. Geralmente as empresas contratadas possuem links de dados redundantes, geradores de energia, etc.

- **Escalabilidade sob demanda:** facilidade em alocar recursos sob demanda, como por exemplo: aumento de memória, discos (HD), processadores, capacidade dos computadores conforme as necessidades.

3.8.2 Desvantagens

- **Falta de interoperabilidade:** a maioria dos modelos disponíveis ainda é realizada de forma integrada verticalmente e limita a escolha da plataforma, além de não definir um padrão comum entre as distribuições dos serviços. Seria como no passado comprar um banco de dados que não se comunicava com outro;

- **Compatibilidade entre operações:** muitas das aplicações disponibilizadas para nuvem ainda são incompatíveis com as aplicações legadas. Nem todo o ambiente possibilita realizar a integração de um sistema local com uma aplicação na nuvem;

- **Dificuldades em obedecer a normas regulatórias:** ainda se faz necessário definir ou estabelecer critérios legais de uma forma melhor estruturada. Não existem leis ou regulamentações sobre a proteção de dados armazenados nos servidores, etc;

- **Segurança inadequada:** O compartilhamento de estrutura e base de códigos por serem centralizados pode se tornar prejudicial em alguns casos para o negócio dos contratantes. Riscos para as informações dos usuários, ao ter seus dados em ambientes utilizados também por outros clientes desconhecidos.

Percebe-se que, as organizações necessitam de implementação dos serviços de *Cloud Computing* tendo como melhoria elasticidade nas suas aplicações, recursos físicos, tecnológicos e humanos. Esta é uma opção para a utilização de soluções de nuvem, mas cabe ao tomador de decisão avaliar os custos e riscos a cada nova situação de contratação, uma vez que os custos com a tecnologia tendem a cair com a sua proliferação e utilização em massa por entidades públicas e privadas. A utilização de *Cloud Computing* não é apenas para os que não têm recursos físicos, tecnológicos e humanos, mas sim para todos que desejam maximizar suas aplicações (sistemas) ou tarefas com a utilização da nova tecnologia da informação e comunicação emergente no mercado (GUERRA, 2012).

3.9 Riscos

Segundo Veras (2012), risco de *Cloud Computing* é a possibilidade que algum evento imprevisto, falha ou mesmo mau uso, ameace um objetivo de negócio.

O autor citado anteriormente, sugere alguns cuidados que o cliente deve ter para mitigar o risco referente à aquisição de serviços de um provedor de *Cloud Computing*, descrito a seguir:

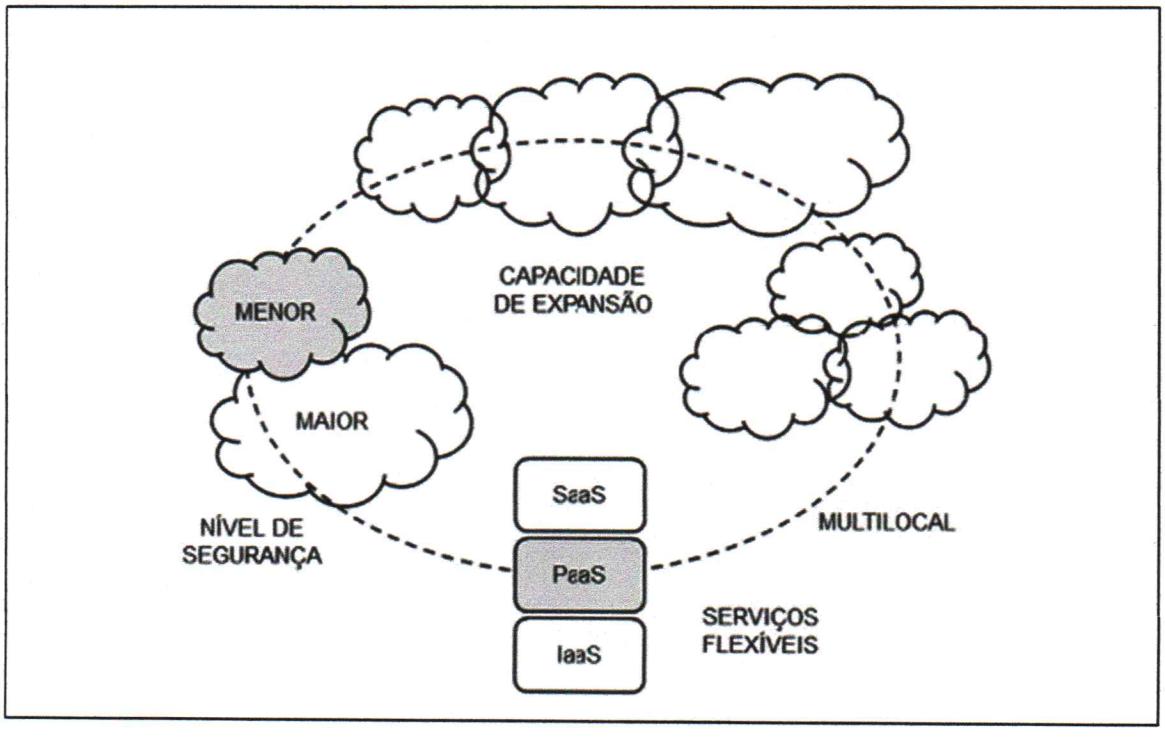
- Saber como é feito o acesso dos usuários.
- Saber como o provedor obedece às normas de regulação.
- Saber onde se localizam os dados.
- Saber como os dados são segregados.
- Saber como os dados são recuperados.
- Saber como é feito o suporte.
- Entender a viabilidade do provedor no longo prazo.

Ainda segundo Veras (2012), o aspecto chave a ser avaliado na opção de entregar os serviços de TI para um fornecedor de *Cloud Computing* é o risco da perda do controle de dados internos, e ele de fato existe. O que deve ficar claro é que o ambiente de *Cloud Computing* é essencialmente diferente do ambiente tradicional da computação. Muda-se de um modelo amparado em equipamentos para um modelo orientado a serviços.

Os serviços de *Cloud Computing* precisam ser elásticos, conforme as necessidades dos clientes, precisam ser adequados a realidade dos clientes e às exigências das suas aplicações, e

precisam ser oferecidos em diversos locais. Tudo isso deve ser oferecido com segurança. A Figura 10 - ilustra estas características.

Figura 10 - Recursos essenciais de *Cloud*



Fonte: VERAS (2012, pag. 50).

Os aplicativos que estão indo para a nuvem ainda são de pouca confidencialidade, mas, com o aumento exponencial da base de informação digital, as empresas precisam considerar o fato de que respondem por boa parte destas informações em termos de segurança, privacidade e confidencialidade. Ainda Veras (2012) diz que o crescimento de uso da nuvem só será possível com o aumento da segurança. As empresas precisam assegurar a confidencialidade, a integridade e a disponibilidade dos dados no momento em que eles forem transmitidos, armazenados ou processados por terceiros na cadeia de serviços em nuvem.

Para garantir uma maior proteção na nuvem, VERAS (2012), cita os elementos principais, que são:

- **Segurança de identidade:** A segurança da identidade preserva a integridade e a confidencialidade dos dados e dos aplicativos enquanto deixa o acesso prontamente

disponível para os usuários apropriados. O suporte a esses recursos de gerenciamento de identidade para usuários e componentes da infraestrutura será um dos principais requisitos da *Cloud Computing* e a identidade precisará se gerenciada de maneira que gere confiança.

- **Segurança das informações:** no *Datacenter* tradicional, os controles sobre o acesso físico, o acesso a *hardware* e *software* e os controles de identidade se combinam para proteger os dados. Na nuvem, a barreira protetora que protege a infraestrutura é diluída. Para compensar, a segurança passará a ser centrada nas informações. Os dados precisam de segurança própria que os acompanhe e os proteja.

- **Segurança da infraestrutura:** a infraestrutura de base da nuvem deve ser inerentemente segura, independentemente de ser privada ou pública ou prover serviço SaaS, PaaS ou IaaS.

Outra forma de ver a segurança é utilizar o modelo de referência proposto anteriormente pela guia CSA versão 2.1. O documento elaborado pela *Cloud Security Alliance*, organização norte-americana sem fins lucrativos, com o objetivo de orientar sobre o uso de melhores práticas da prestação de serviços na área de segurança na nuvem.

Utilizando - se o modelo da CSA, podem ser feitos considerações importantes sobre os três modelos de serviços e a segurança.

- O modelo SaaS oferece funcionalidade mais integrada, construída diretamente baseada na oferta, com a menor extensibilidade para o cliente e um nível relativamente elevado de segurança.

- O modelo PaaS visa permitir que os desenvolvedores criem seus próprios aplicativos em cima da plataforma. Assim, é mais extensível que o modelo SaaS, a custas das funcionalidades disponibilizadas aos clientes. As capacidades de segurança são menos completas, mas há flexibilidade para adicionar uma camada de segurança extra.

- O modelo IaaS oferece pouca ou nenhuma característica típica de um aplicativo, mas permite muita extensibilidade. Significa ter menos recursos e funcionalidades integradas de segurança. Este modelo requer que o cliente proteja e gerencie os sistemas operacionais, aplicativos e conteúdo.

Veras (2012) cita um Artigo publicado na *Computerworld* americana, traduzido para o português com o título"Considere os riscos legais antes de contratar o serviço de *Cloud*", reforça dizendo que uma organização não deve assinar contrato de *Cloud Computing* sem levar em conta cinco questões fundamentais, as quais serão descritas a seguir:

- **Privacidade:** para se proteger, os clientes precisam conferir se os provedores são capazes de atender às regras a que estão submetidos e insistir que tudo seja descrito no contrato.

- **Conformidade com múltiplas jurisdições:** os clientes da nuvem devem saber a localização do fornecedor e os seus servidores para determinar onde poderiam sofrer com problemas jurídicos.

- **Mandados de busca:** dados de múltiplos clientes podem acabar no mesmo servidor. Caso um dos clientes sofra um processo que gere um mandado por buscas naquele servidor, todos os dados podem acabar se tornando inacessíveis para a outra companhia, que não tem nada a ver com aquilo. A empresa precisa ter um plano para minimizar esses riscos e garantias do provedor de que as informações estão particionadas de forma a não afetar os dados dos outros clientes, caso apenas um deles se envolva em uma questão judicial.

- **Informações legais:** o detentor de uma informação tem a obrigação de preservar qualquer dado que possa ser relevante em litígio, mantendo-o armazenado para propósitos legais. Um exemplo disso são as informações trabalhistas: se não tiver registro de todos os dados de seu funcionário, a empresa pode ser acionada legalmente para prestar informações, caso sofra ação. E a justiça pode ir diretamente ao provedor, com um mandado judicial, de forma que a empresa perde o controle de toda a situação. Além disso, buscar informações pode ser difícil se o provedor não tiver procedimentos muito bem documentados de armazenamento, facilitando a consulta futura. A empresa deve ter a capacidade de buscar os documentos exatos que importam ao pedido, para não sofrer com multas. E o contrato com o fornecedor de nuvem deve ser capaz de prever isso com exatidão.

- **Segurança da informação:** os métodos para proteger dados nas nuvens, como criptografia, estão bem documentados. Más há também riscos associados com a manutenção de todos os registros da empresa em uma dada localização.

3.9.1 Consolidação dos Riscos

Chaves (2011, apud VERAS, 2012, p. 54), apresenta a consolidação dos riscos inerentes a *Cloud Computing*:

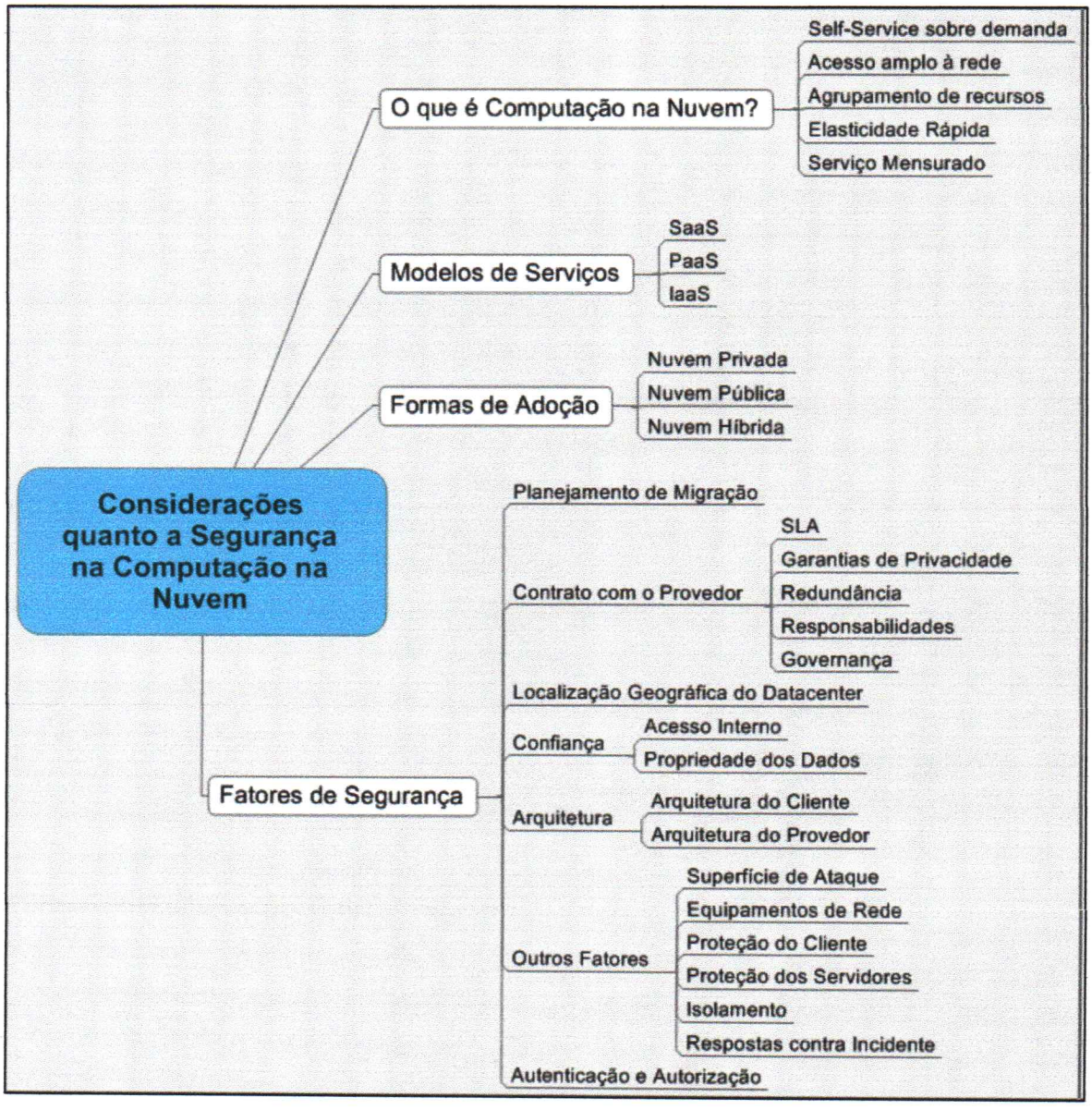
- Riscos operacionais: falta de privacidade devida, por exemplo, a deficiências de isolamento no ambiente de nuvem, falta de integridade que pode ser provocado por agentes de *software*, suporte inadequado por parte do provedor ocasionado por uma série de fatores incluindo pessoal mal preparado, baixo desempenho dos serviços contratados, ataques por saturação não detectados a tempo, dificuldades para provisionar ou liberar recursos e baixa ou nenhuma interoperabilidade entre aplicativos.

- Riscos de negócio: indisponibilidade temporária por parte do provedor e a não continuidade, que seria uma interrupção definitiva por parte do provedor.

- Riscos estruturais: não conformidade com padrões e legislação, limitações na forma de realizar o licenciamento de *software*, aprisionamento feito pelo provedor e má reputação do provedor, oriunda de baixa qualidade de serviços prestados.

A imagem da Figura 11 serve de modelo para revisar os principais pontos que foram abordados neste capítulo. Além dos conceitos básicos de Computação em Nuvem foram abordados também, os tipos de nuvem disponíveis e as formas de adoção de cada modelo.

Figura 11: Mapa de modelo para *Cloud Computing*.



Fonte: *DOCPLAYERS* (2016)

4 PROPOSTAS PARA A MELHORIA DA SEGURANÇA DA INFORMAÇÃO EM COMPUTACÃO NAS NUVENS.

Por meio da *Internet,* a computação em nuvem apresenta uma extensão de problemas. Para garantir que tais informações sejam acessadas através do ambiente de computação em nuvem, os próprios provedores de serviços devem estabelecer políticas de segurança coerente e eficaz para identificar e implementar métodos adequados que assegure os dados dos usuários.

Este capítulo tem por objetivo abordar as principais técnicas e ferramentas que profissionais da área de TI utilizam para garantir que usuários acessem seus dados com segurança em *Cloud Computing*.

4.1 Principais técnicas e ferramentas utilizada para garantir a segurança em *Cloud Computing*

Já citado anteriormente, confidencialidade, integridade e disponibilidade são uns dos elementos que precisam ser considerados para que tenhamos o privilégio de acessar as informações de forma segura.

A utilização da nuvem computacional aos poucos vem crescendo e tendo um alto índice de confiabilidade e produtividade. Parchen *et al* (2013), de uma forma resumida, destacam algumas medidas que devem ser adotadas pelos usuários para que possam usufruir dos serviços os quais a nuvem computacional oferece de forma segura.

A primeira delas é a contratação de um provedor de serviços consagrado no mercado, objeto de avaliações positivas por parte da comunidade científica e dos internautas.

A busca por uma empresa que efetivamente contribua para uma benéfica relação no uso da tecnologia é essencial. Procurar ver se a mesma conta com serviço de suporte integral, com planos de contingências para perda de dados (back-up ou cópias de segurança), com estrutura de servidores compatível com aquilo que divulga ao seu negócio.

A segunda é a busca pela tutela da confiança através da informação. Aquele que pretende contratar um serviço deve necessariamente informar-se com antecedência acerca dos benefícios e riscos que envolvem a nuvem, procurando saber ainda o histórico de acertos e de problemas que aquela determinada empresa de tecnologia tem ou teve, procurando valer-se ainda da experiência anterior de outros usuários que já utilizaram aquele serviço para, só então, munido dos elementos que precisa, sopesar a contratação.

A terceira é a adoção em conjunto da criptografia, das chaves públicas e privadas e dos certificados digitais. Sem este pacote de proteção, a nuvem fica à deriva em meio ao mar de ataques virtuais, de um universo de vírus de computadores, onde o resultado fatalmente será o da quebra da privacidade e idoneidade dos dados.

Se esta proposta for adotada toda vez que algum serviço em nuvem estiver sendo usado, não há como negar que esta proporcionará grandes benefícios quando aplicada às novas tecnologias atuais e às que surgirão, Parchen *et al* (2013).

Além das técnicas citadas anteriormente, no quadro seguinte, Moia (2016) faz um levantamento com relação a segurança em um provedor, que devemos levar em consideração seus requisitos e suas preocupações.

Quadro 1: A segurança num provedor

REQUISITO	PREOCUPAÇÃO
Segurança das chaves criptográficas	Gerenciamento correto das chaves criptográficas. São considerados fatores como o tempo de vida de uma chave e sua guarda correta.
Deduplicação segura	Garantir que técnicas de economia de espaço, usadas por provedores para evitar duplicação de dados que possam comprometer a privacidade dos usuários.
Alto nível de sigilo	Buscar modos de implementação de criptografia em serviços de nuvem, que possam trazer mais segurança e menos riscos à privacidade do usuário.
Trust no one (Não confie em ninguém)	Oferecer mais garantias de que o usuário seja o único capaz de acessar seus dados, através do uso exclusivo de uma chave criptográfica (senha) não compartilhada com o provedor da nuvem.
Sigilo dos atributos dos arquivos	Proteger os atributos de um arquivo (nome, datas de criação e última modificação, tamanho, etc.) contra acesso não autorizado por terceiros.
Open Source (Código fonte aberto)	Manter em domínio público o código fonte da aplicação de proteção a fim de evitar vulnerabilidades ou "portas dos fundos" que possam comprometer a segurança e privacidade dos usuários
Autenticidade do software	Permitir que usuários possam verificar a autenticidade de uma aplicação, isto é, que ela foi realmente gerada pelo seu desenvolvedor, a fim de evitar que atacantes possam alterá-la sem serem detectados.
Autenticação Multi-fator	Aumentar a segurança do processo de autenticação, utilizando dois ou mais fatores para este fim. Ex. de fatores de autenticação: algo que o usuário saiba (senha), algo que ele possua (smartphone ou cartão com chip) e algo que ele seja (características biométricas como digitais, íris, etc.).

Usabilidade	Reduzir a complexidade do software criptográfico a fim de facilitar sua utilização, exigindo um menor esforço sem o comprometimento da segurança

Fonte: MOIA (2016)

Levando em consideração todas essas medidas, para garantir um maior padrão de segurança ao armazenar, gerenciar e compartilhar os dados na Nuvem, existem empresas que fornecem serviços como segurança baseado em Nuvem e ferramentas que possam auxiliar para esses fins. Nesta secão irei abordar fornecedores de serviços que prometem garantir a segurança dos dados em *Cloud Computing* e métodos com o uso de *software* que tenham como principal característica criptografa-los os antes de enviar para o ambiente *(Cloud).*

4.2 Fornecedores de serviços como sergurança baseado em Nuvem

4.2.1 SiteLock: O SiteLock é uma das maiores soluções de segurança de sites. Esta solução permite verificar falhas de segurança do seu site bem como identificar e remover software malicioso utilizado por hackers. Não só protege contra ameaças como também identifica e corrige vulnerabilidades, DOT2WEB (2014).

No *SiteLock* hà integrações de aplicações *web* avançada baseado em Nuvem, chamados de *TrueShield, Web Application Firewall.* Os mesmos trabalham em conjunto com o objetivo de ajudar a proteger *websites* de tráfego malicioso. Ao utilizar o nosso *TrueShield* (WAF), também é possível diferenciar o tráfego humano a partir de tráfego de *bots*, e descobrir a origem dos ataques bloqueados através do endereço IP, *SITELOCK* (2016).

4.2.2 Benefícios da SiteLock, TrueShield, Web Application Firewall

De acordo com o que diz o site VALUEHOST (2016) os beneficios da *SiteLock,* juntamente com *TrueShield e Web Application Firewall* são:

- **Detecção de *Malware:*** Diagnóstico rápido de todas as infecções nocivas ou malware que podem estar no seu site.
- **Monitoramento de blacklist:** Verificação diária do seu site para mantê-lo fora da lista negra do Google e proteger a sua reputação.
- **Suporte expert sob demanda:** Equipe de experientes analistas de sites para reparar as infecções e bugs do seu site por completo.

- **Identificação de vulnerabilidade:** Um raio-X completo do seu site que descobre falhas de segurança, injeções de vírus e fraquezas.
- Com *Application Firewall SiteLock TrueShield Web*, o site vai estar a salvo de erros e *spammers* que tentam roubar o seu conteúdo e tráfego. Para os comerciantes, o firewall de aplicação web dá a você e seus clientes a tranquilidade de que o seu site está seguro, livre de invasores, fornecendo proteção ativa diariamente, *SITELOCK* (2016).

4.2.3 Como o SiteLock funciona

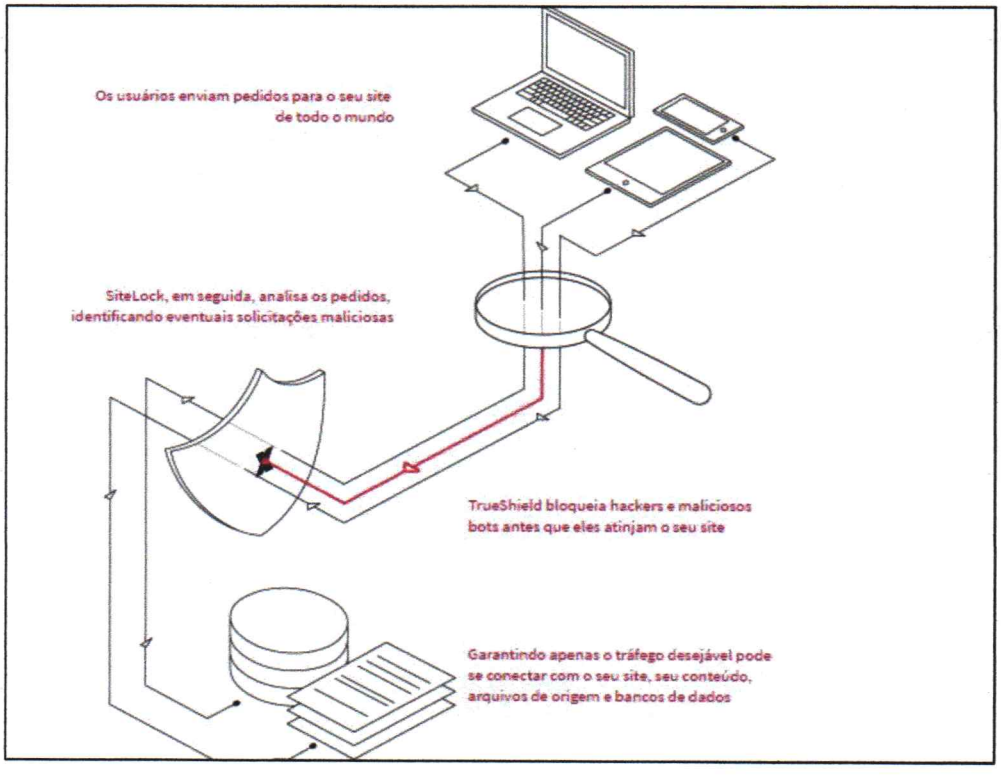
O *firewall* de aplicativo *web* (WAF) é uma camada avançada de proteção para o site, o qual determina quem é, ou não permitido acessá-lo.

O *TrueShield* (WAF) avalia o tráfego com base de onde ele está vindo, como ele está se comportando, e as informações que ele está pedindo, o que permitirá que os clientes usem mecanismo de busca para chegar ao seu site, e proteger seus arquivos, conteúdo e bancos de dados de tráfego ruim como spam ou *hackers*. *TrueShield* bloqueia tentativas de *bots* maliciosos ou *hackers* para invadir seu site- seu negócio *online*. A tecnologia avançada permite que um proprietário de site controle os tipos de interações os quais os visitantes podem ter em seu site, além de identificar e bloquear a maioria dos agentes de ataque, (*SITELOCK* 2016).

4.2.4. Como funciona o scan de vírus do SiteLock

De acordo com o que diz E-DOMÍNIOS (2016), o sistema de escaneamento de vírus compara seus arquivos com um banco de dados de vírus para determinar se há alguma semelhança entre o código de seu site e os códigos maliciosos conhecidos. Para evitar prejuízos à performance de seu website. O *download* das informacões é feito de maneira periódica, scaneando uma parte de seu site a cada dia. Para a maioria dos sites, a varredura completa leva até 30 dias.

Figura 12: Como funciona o *scan SiteLock*

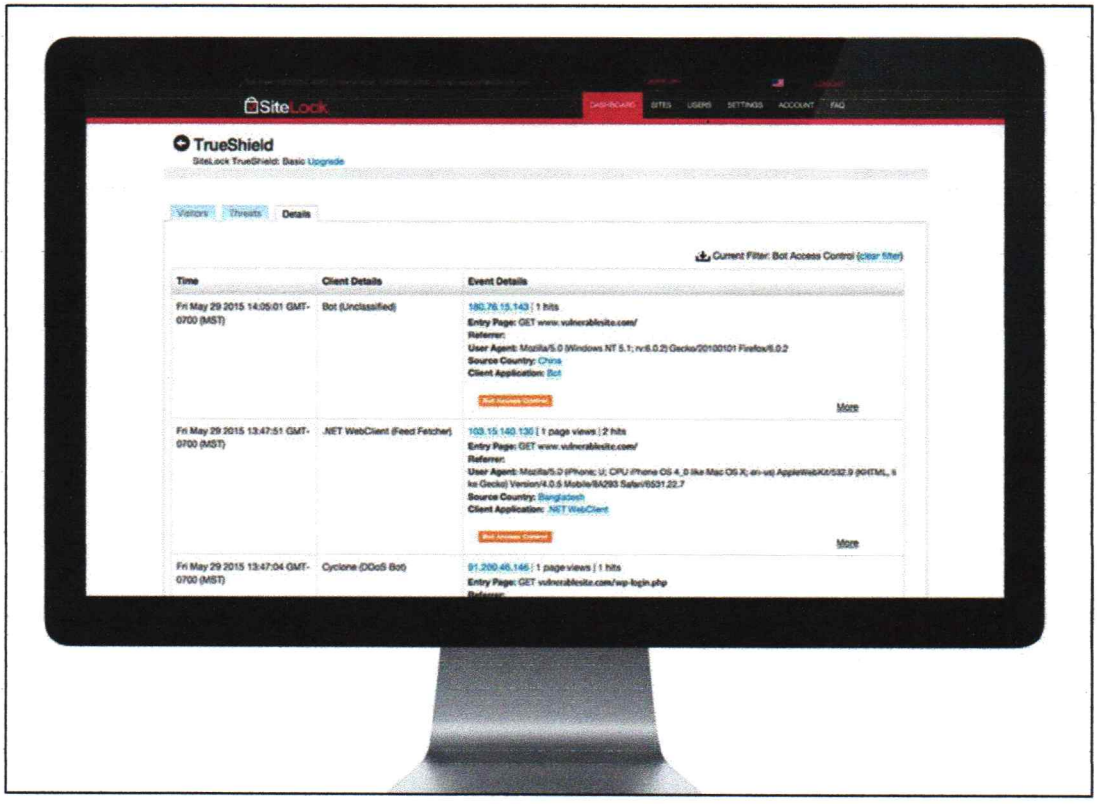


Fonte: *SITELOCK*

4.2.5 Como o SiteLock notifica o proprietário do site quando encontra um problema.

O *SiteLock* informa o *webmaster* através de e-mail e de um alerta no Painel de Controle *SiteLock*. O aviso oferece informações completas sobre o problema e ajuda para solucioná-lo, (E-DOMÍNIOS, 2016).

Figura 13: exemplos de endereços IP bloqueados por TrueShield



Fonte: *SITELOCK*

4.2.6 Plano SiteLock

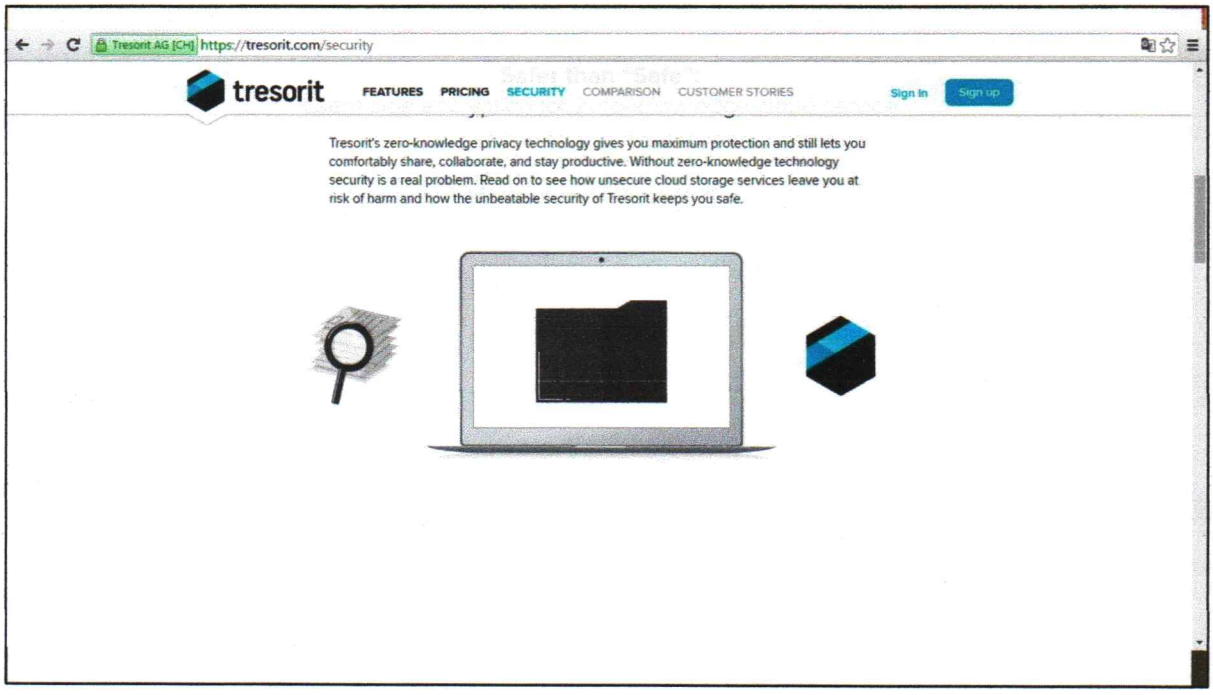
O *SiteLock* disponibiliza planos de pagamento, tendo você, o critério de escolher o que se ajuste melhor ao seu negócio mantendo o seu site seguro e livre de software malicioso.

SITELOCK BASIC	***SITELOCK BUSINES***	***SITELOCK PREMIUN***
Sites que precisam de verificações diárias de software malicioso.	Verificação e remoção automática de software malicioso.	Verificação contínua de vulnerabilidades
✓ Verificação até 25 páginas ✓ 1 verificação de vulnerabilidades ✓ Verificação diária de Malware ✓ Selo SiteLock Trust	✓ Verificação até 100 páginas ✓ 1 verificação de vulnerabilidades ✓ Verificação diária de Malware ✓ Remoção automática de Malware ✓ Verificação de alteração de ficheiros ✓ Selo SiteLock Trust Sea	✓ Verificação até 500 páginas ✓ Verificação continua de Vulnerabilidades ✓ Verificação diária de Malware ✓ Remoção automática de Malware ✓ Verificação de alteração de ficheiros ✓ Selo SiteLock Trust Sea
1,47€ /mês	3,68€ /mês	6,51€ /mês

Fonte: DOT2WEB.PT (2014)

4.3 *Tresorit*

Figura 14: Tela inicial *Tresorit*



Fonte: *TRESORIT* (2016)

Tresorit é um provedor de armazenamento em nuvem onde o recurso de segurança inclui criptografia do lado do cliente, o que se leva a entender que *Tresorit* protege seus arquivos em seu dispositivo com alguns dos maiores métodos de criptografia de grau disponíveis, e seus arquivos não pode ser descriptografado na nuvem. *Tresorit* é uma nuvem de armazenamento criptografado *end-to -end.* Usuários podem compartilhar seus arquivos usando *links* codificados com uma opção adicional de proteção por senha (BICAKCI, 2016).

Usando *Tresorit*, seus arquivos permanecem criptografados, para que ninguém, nem mesmo a equipe *Tresorit* e nem poderes govenamentais seja capaz de descriptografar os arquivos para ver, roubar ou modificá-los. Mesmo que o sistema cause algum tipo de falha, os dados os tornaram seguros, pois o que se pode ver nos servidores são apenas bits aleatórios de dados *TRESORIT* (2016).

4.3.1 Caracteristicas

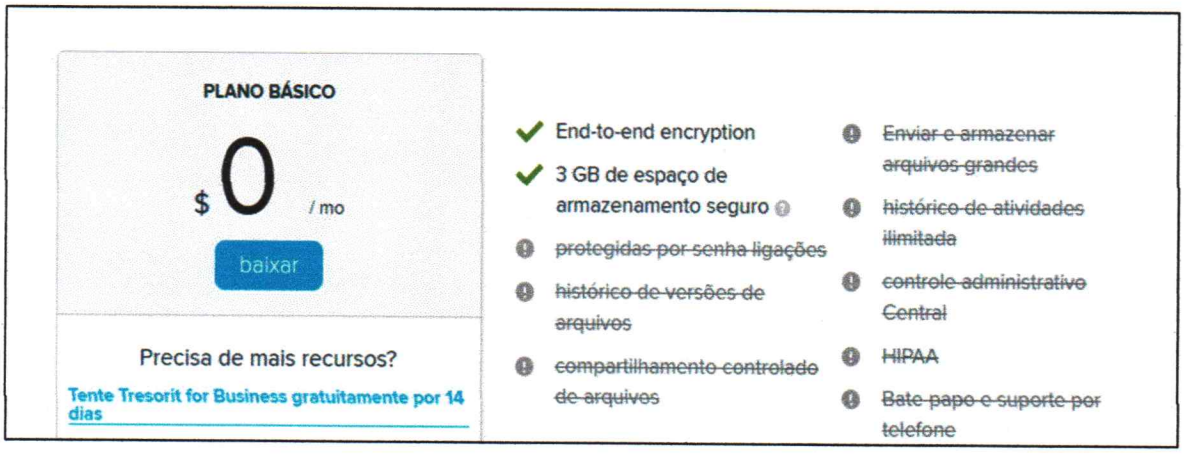
O site *TRESORIT* (2016) destaca suas principais características e funcionalidades, que são elas:

- **Criptografia *end-to-end*:** arquivos criptografados, para que ninguém, nem mesmo a equipe *Tresorit* e nem poderes govenamentais seja capaz de descriptografar.
- **Segurança:** *Tresorit* desafiou hackers com uma recompensa de US $ 50.000 para quem conseguisse invadir seu sistema, 1000 *hackers* de 49 países tentaram, mas ninguém conseguiu.
- **Privacidade Suiça:** *Tresorit* manipula dados sob as leis de privacidade suíças, que assegurem uma protecção mais forte do que leis semelhantes a do Estados Unidos ou até mesmo da União Europeia.
- ***Backup* criptografado:** Cada arquivo adicionado ao *Tresorit* é automaticamente criptografado e enviado para a nuvem, onde todas as alterações são constantemente submetidas a backup.
- **Até 1TB de armazenamento criptografado (negócio):** *Tresorit* para negócios vem com armazenamento suficiente para cada usuário de trabalho a fim de armazenar arquivos de trabalho sensíveis e documentos.
- **Aplicativos móveis e de *desktop*:** Usuários acessam seus arquivos em dirversos tipos de plataformas como, por exemplo: *Windows, Mac, Linux, iOS, Android, Windows Phone* ou *Blackberry*.
- **Segurança da conta e dispositivo:** Com a autenticação de duas etapas e bloqueio do dispositivo, seus dados estão seguros se a sua senha ou o dispositivo é roubado.
- **Apagamento remoto de dispositivo:** Com *Tresorit* você pode apagar todos os arquivos protegido caso perca seu dispositivo ou se alguêm venha a roubá-lo.
- **Trabalhar seus arquivos e pastas da maneira que quiser:** Não há necessidade de mover arquivos. Arrastar e soltar qualquer pasta ou arquivos existentes para sincronizá-lo com segurança para a nuvem.

- **Sem anexo de *E-mail*:** Trabalhar com outros em documentos sensíveis, como apresentações ou relatórios sem a necessidade de anexos de email tudo isso é possível realizar dentro do ambiente *Tresorit*.
- **Versões de atividade e histórico (negócio):** Veja o que seus colaboradores estão fazendo. Acesso and roll de volta para versões anteriores de qualquer documento.
- **Enviar arquivos de forma segura:** Enviar arquivos para qualquer pessoa via *link* criptografado. O acesso requer apenas um navegador.
- **Niveis de Acesso (negócio):** Decidir se o seu documento compartilhado pode ser copiado, enviado, impresso, compartilhado.
- **Segurança da conta executada (negócio):** Faça duas etapas de verificação obrigatória, para garantir que os padrões de segurança são elevados em toda a empresa.
- **Politica de acesso (negócio):** Restringir o acesso ao escritório ou outras instalações da empresa. Limitar o acesso a partir de dispositivos móveis, se necessário.

4.3.2 Planos Tresorit

Figura 15: planos *Tresorit*



Fonte: *TRESORIT* (2016)

	PREMIO	P/EMPRESAS	G/EMPRESAS
PREÇO	10 € /MÊS	20 € /MÊS	40 € /MÊS
Criptografia			
Sistema de conhecimento nulo	✓	✓	✓
Proteção de canal TLS	✓	✓	✓
Compartilhamento criptografado	✓	✓	✓
Privacidade Suiça	✓	✓	✓
Armazenamento seguro de rede			
Datacenters certificados	✓	✓	✓
Armazenamento redundante na Europa	✓	✓	✓
Estatísticas de acesso	✓	✓	✓
Autenticação em duas etapas	✓	✓	✓
Pastas seguras ilimitadas	✓	✓	✓
Espaço de armazenamento	100GB	100 GB	Personalizado
Tamanho máximo de arquivo	5GB	10GB	10GB
Histórico de atividades	90 dias	Ilimitado	Ilimitado
Número de dispositivos	5	10	Ilimitado
HIPAA		✓	✓
Acesso a arquivo e sicronização			
Clientes de *desktop*	✓	✓	✓
Histórico de versões de arquivos	✓	✓	✓
Aplicativos móveis	✓	✓	✓
Acesso seguro à *Web*	✓	✓	✓
Sincronização criptografado automático	✓	✓	✓
Gerenciamento de dispositivo	✓	✓	✓
Histórico de versões de arquivos	10 versões	Ilimitado	Ilimitado
Copartilhamento e cololaboração			
Permissões de compartilhamento granulares	✓	✓	✓
Compartilhar com qualquer número de pessoas	✓	✓	✓
Envio de ficheiros através de *links*	✓	✓	✓
Numeros de *Link* que usuários pode criar	50/ mês	Ilimitado	Ilimitado
Tamanho máximo de *links*	500MB	1000MB	1000MB
Definir a data de expiração para os *links*	Até 30 dias	Até 90 dias	Até 90 dias
Definir o limite de download para os *links*	Até 50	Até 1000	Até 1000

Proteção os *links* com senhas		✓	✓
DRM proteção dos direitos de acesso avançado			
Limitar cópia, edição, impressão, criação de imagens e *e-mail*		✓	✓
Arquivos protegidos no dispositivo, e na nuvem		✓	✓
Controle administrativo e de gerenciamento usuário			
Estatísticas de arquivo e de usuário		✓	✓
Gerenciamento de usuários		✓	✓
Os grupos de usuários		✓	✓
Autenticação verificação de dois Passos		✓	✓
Políticas de dispositivo		✓	✓
Filtragem de IP		✓	✓
Políticas de armazenamento e compartilhamento		✓	✓
Controles de administração personalizada			✓
Apoio			
Base de conhecimento	✓	✓	✓
Fórum da comunidade	✓	✓	✓
Resposta de *E-mail*	Normal	Prioridade	Prioridade Máxima
Suporte por telefone		✓	✓
Suporte de desenvolvimento		✓	✓
Formação Personalizada de pessoas			✓

Fonte: *TRESORIT* (2016)

4.4 *BoxCryptor*

Figura 16: Tela Inicial *BoxCryptor*

Fonte: *BOXCRYPTOR* (2016)

BoxCryptor faz parte de módulos criptográficos que podem ser acoplados com um provedor de serviço em nuvem existente, como por exemplo, o *Dropbox, Google Drive, Microsoft OneDrive,* dentre outros. Os dados são encriptados antes de serem enviados para nuvem. Com *BoxCryptor* é possivel manter o controle total do conteúdo de sua nuvem, uma vez que é criptografada com as principais criptografias *AES-256 e †RSA antes da sincronização. Devido ao padrão de conhecimento nulo, *BoxCryptor* não pode acessar seus dados, (MOIA 2015).

Além de ser compatível com os sistemas operacionais como, por exemplo: *Windows, Windows Chrome (beta)* e *Mac OS X, BoxCryptor* também suporta as plaformas que é utilizada nos dispositivos móvel, como: *Android, IOS, Windows Phone, Windows RT,* e *BlackBarry* permitindo que você acesse seus arquivos criptografados em movimento. A versão gratuita do *BoxCryptor* é limitada a 2GB de arquivos criptografados (LATHA 2014).

*O algoritmo AES (Advanced Encryption Standard), do tipo block cipher, possui tamanho de bloco de 128 bits e chaves de 128, 192 e 256 bits. Já RSA (Data Security INC) É um tipo e cifra onde permite a utilização de chaves de tamanho variados para proporcionar velocidade na criptogarafia de grandes quantidades de dados, (DA COSTA CARMO, 2009).

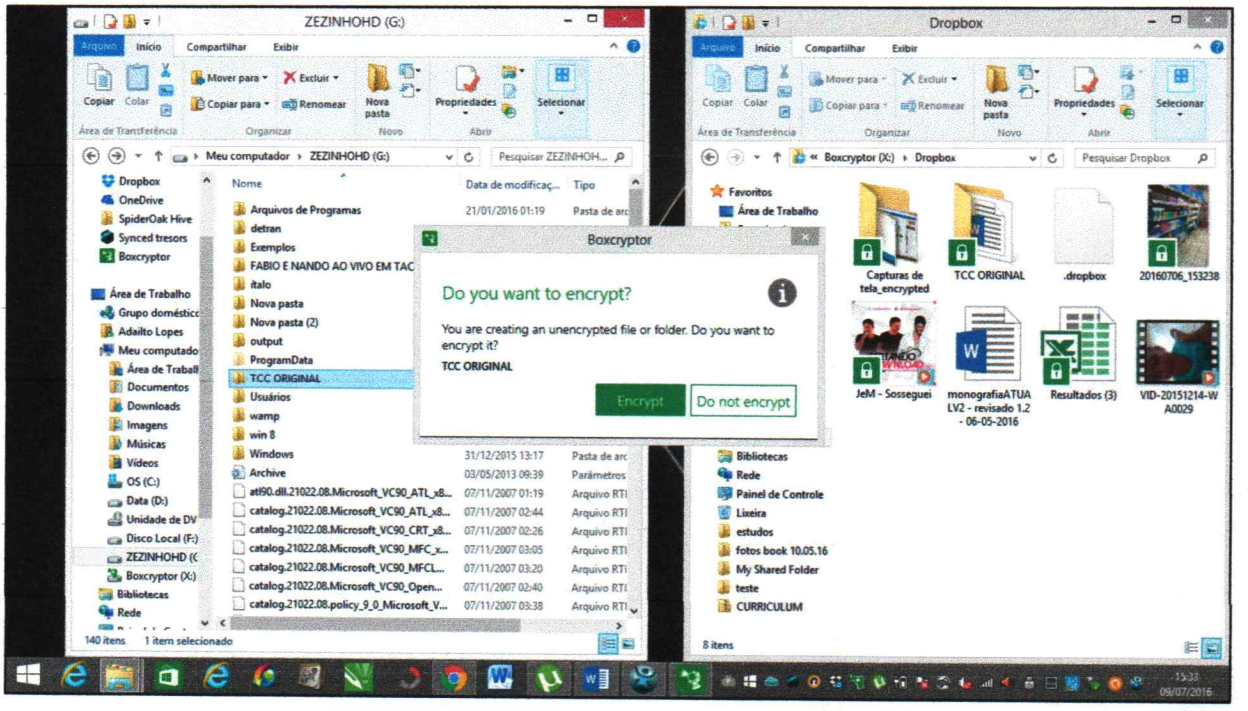
4.4.1. Criptografar e descriptografar arquivos e pastas no BoxCryptor, Passo a passo.

Criptografar arquivos e pastas:

Quando iniciado pela primeira vez, *BoxCryptor* não criptografa seus arquivos automaticamente. Você pode salvar seus arquivos direto do *software* que você usa (por exemplo, *Word, Excel, PowerPoint*, entre outros) para o local dentro do seu *BoxCryptor Drive.*

Outra opção é criar novos arquivos ou pastas através do botão direito do mouse e escolha a opção Novo, ou simplesmente na guia superior "novo item" para criar um novo item no local atual. Uma caixa de diálogo irá aparecer dando-lhe a escolha, para simplesmente salvá-lo ou para criptografar o arquivo ou pasta recém-criada.

Figura 17- Criptografar arquivos e pasta



Fonte: AUTORIA PRÓPRIA

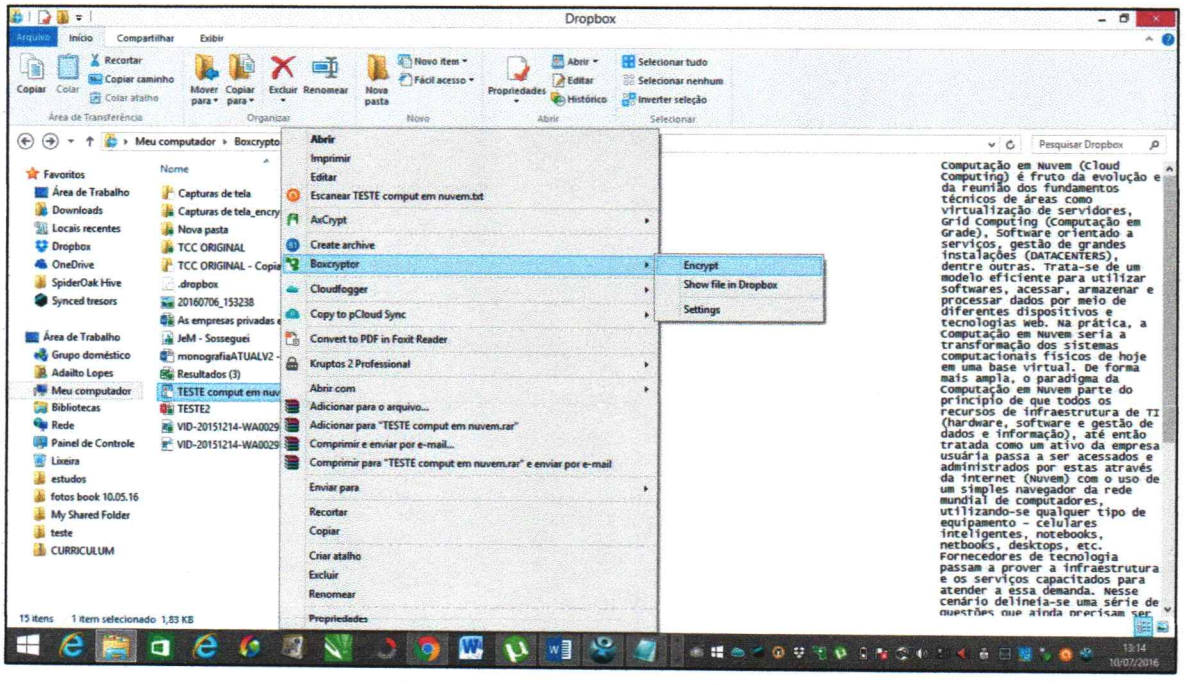
Criptografar pastas e arquivos existentes:

Para criptografar itens e pastas é muito fácil. Você apenas tem que seguir os seguintes passos:

- Selecione o arquivo ou pasta que você deseja criptografar dentro do *BoxCryptor Drive.*
- Botão direito do mouse no item, e selecione *BoxCryptor*
- Em seguida escolha a opção *encrypt*,

Feito isso, agora, seu arquivo está criptografado.

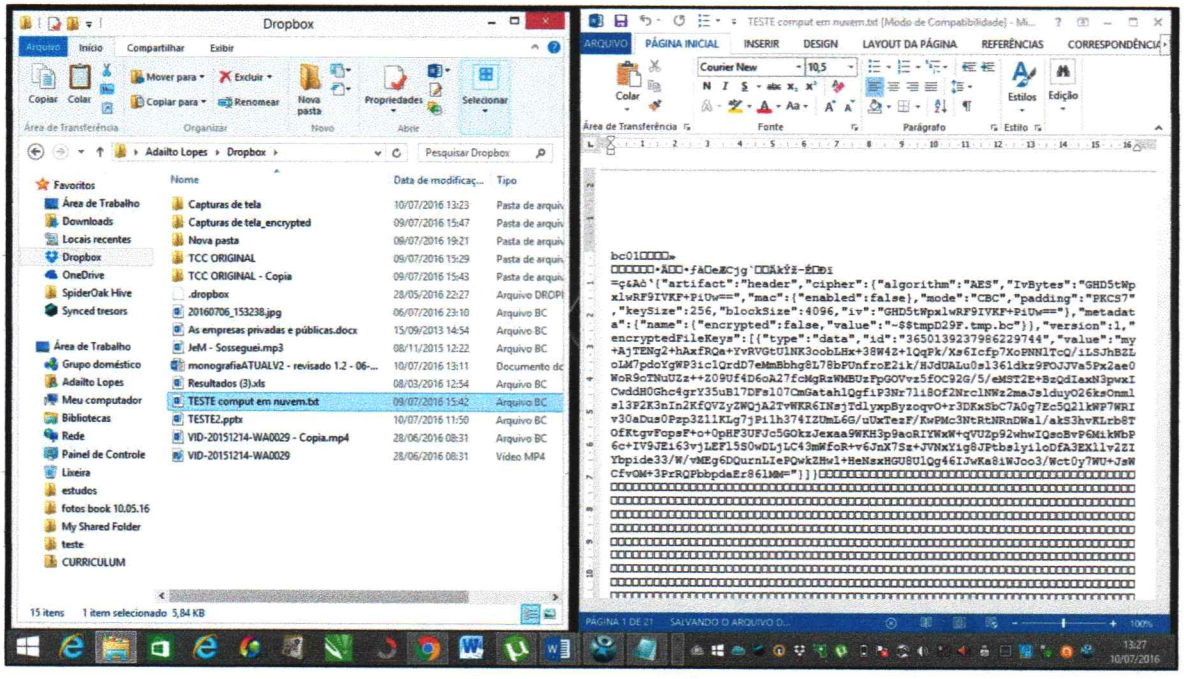
Figura 18- Criptografar arquivos e pasta existente



Fonte: AUTORIA PRÓPRIA

Depois dos arquivos criptografados dentro do *BoxCryptor Drive* a vizualização dos arquivos dentro da pasta *Dropbox* aparecerá ilegivel de forma que ninguem consiga decifrar, de acordo com o que mostra a próxima figura.

Figura 19- Vizualização de arquivos encriptado



Fonte: AUTORIA PRÓPRIA

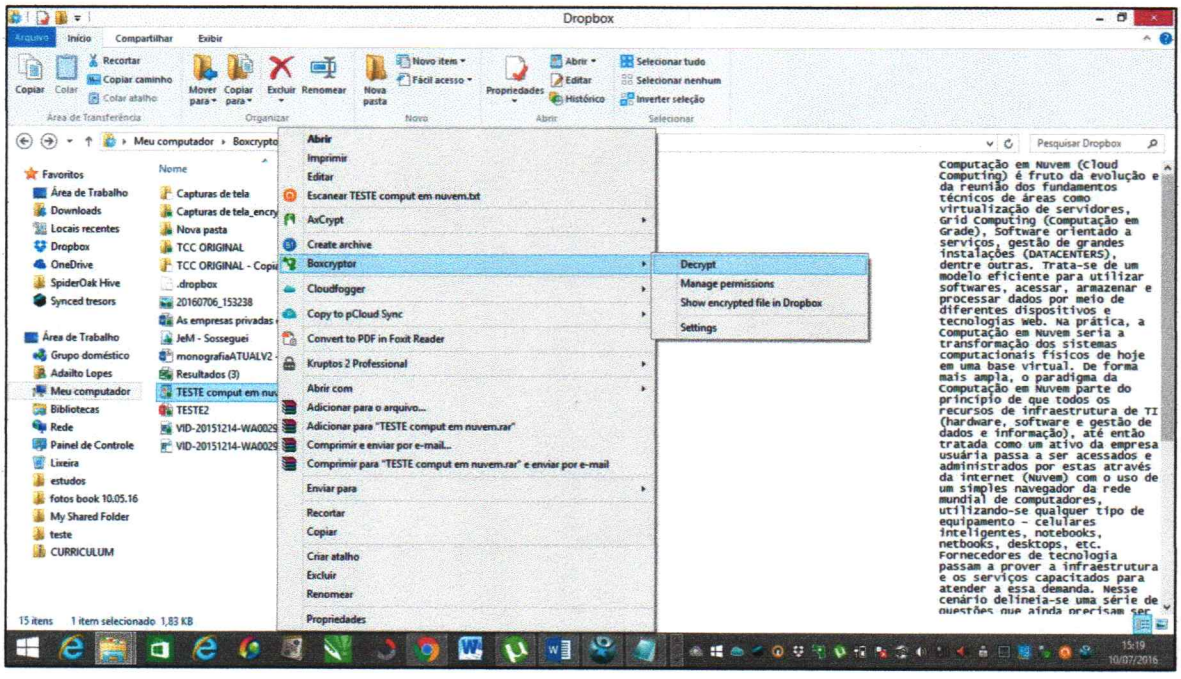
4.4.2. Como descriptografar os arquivos e pastas no BoxCtyptor

Descriptografar arquivos e pastas é tão fácil quanto o processo de criptografar. Você apenas tem que realizar os seguintes passos:

- Selecione o arquivo ou pasta criptografada que você quer decifrar através do *BoxCryptor Drive*.
- Botão direito do mouse no item e selecione *BoxCryptor*
- Em seguida escolha a opção *decrypt*

Feito! Seu arquivo ou pasta estar descriptografado.

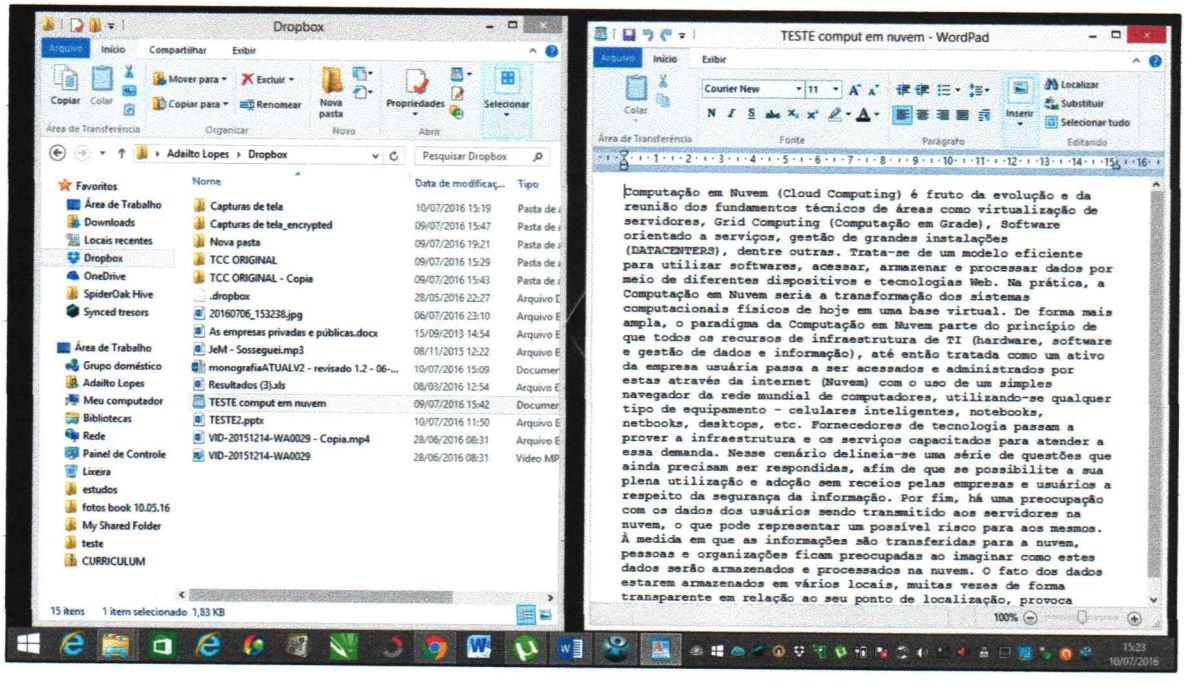
Figura 20 - decriptando arquivo



Fonte: AUTORIA PRÓPRIA

Depois dos arquivos descriptografado dentro do *BoxCryptor Drive* a vizualição dos arquivos dentro da pasta *Dropbox* aparecerá legivel de forma que todos consigam decifrar o que está contido no arquivo, de acordo com o que mostra a figura 21.

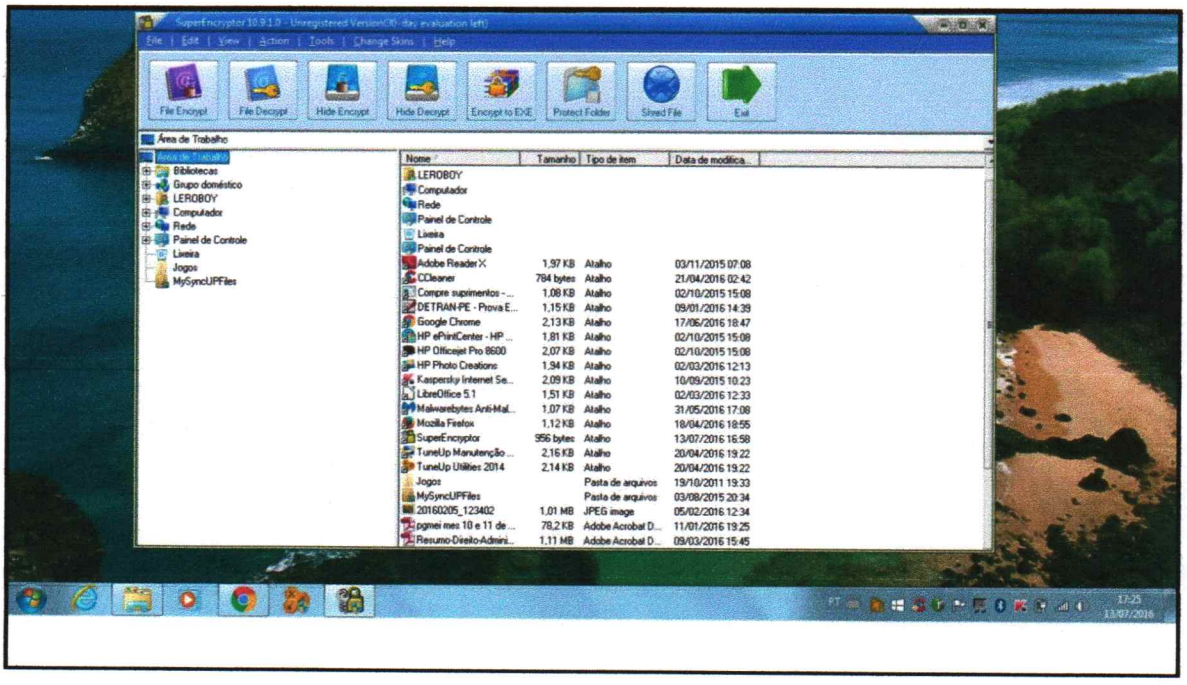
Figura 21 - Vizualização de arquivo descriptografado



Fonte: AUTORIA PRÓPRIA

4.5 SuperEncryptor

Figura 22 - Tela inicial SuperEncryptor



Fonte: AUTORIA PRÓRPIA

Yiyou Software foi fundada por um grupo de desenvolvedores de *software* em 2001. Especializando-se em desenvolvimento de segurança e privacidade. Desenvolveram uma ferramenta com soluções simples, confiável e fácil de usar. O *software* pode ser utilizado em Desktop para uso pessoal ou em pequenas empresas. *SuperEncryptor* é uma poderosa ferramenta de criptografia, com interface de usuário amigável e fácil de usar, tendo como caractéristicas únicas, além da criptografia de arquivos de qualquer tipo e comprimento, também fornece armazenamento de dados abrangente e proteção para seus arquivos e pastas, YIYOU ENCRYPTION SOFTWARE (2001-2014).

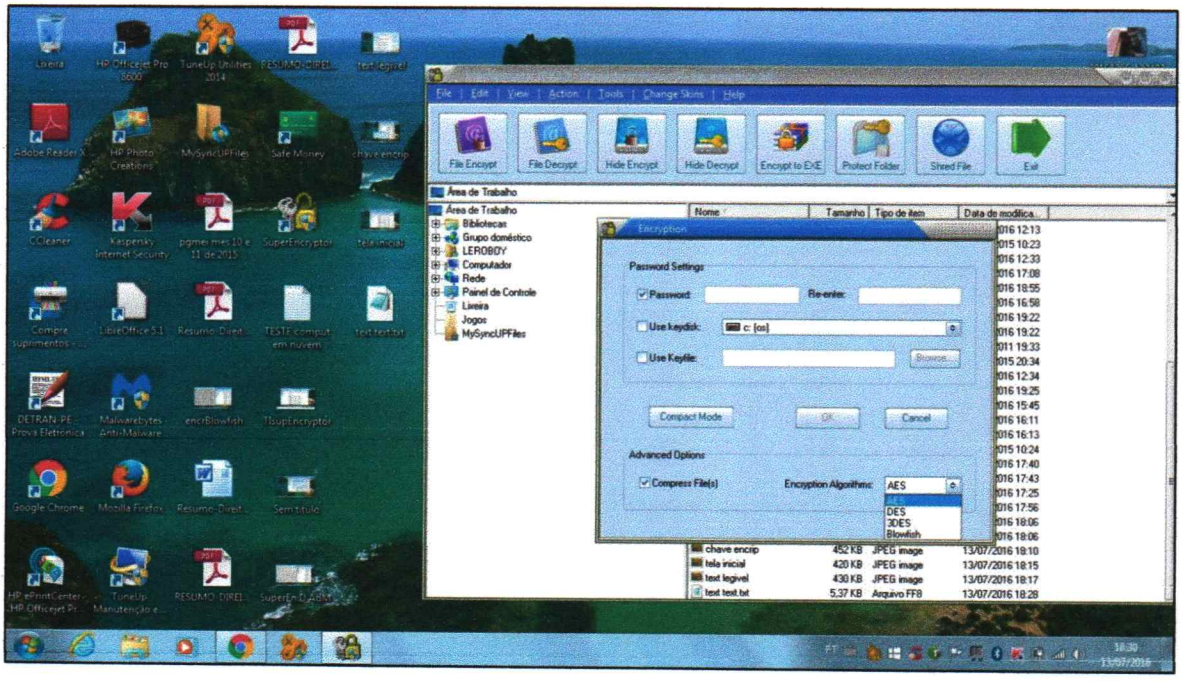
4.5.1. Criptografar e descriptografar arquivos e pastas no SuperEncryptor, Passo a passo.

Criptografar arquivos e pastas no *SuperEncryptor*:

- Selecione um tipo de arquivo ou pasta;

- Clique no icone "*File Encrypt*", em seguida, uma caixa de entrada de senha irá aparecer, local onde irá escolher uma chave para encriptar o arquivo;
- Clique em "OK", pronto! Seu arquivo está encriptado.

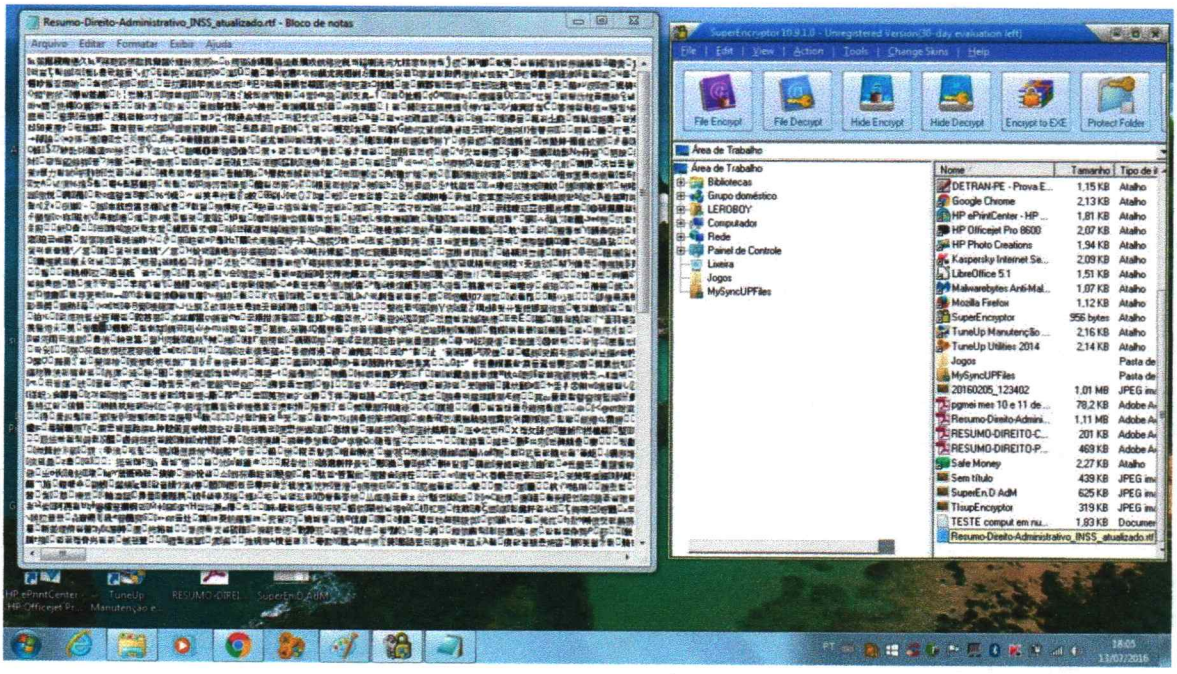
Figura 23 - Inserindo chave no SuperEncryptor



Fonte: AUTORIA PRÓPRIA

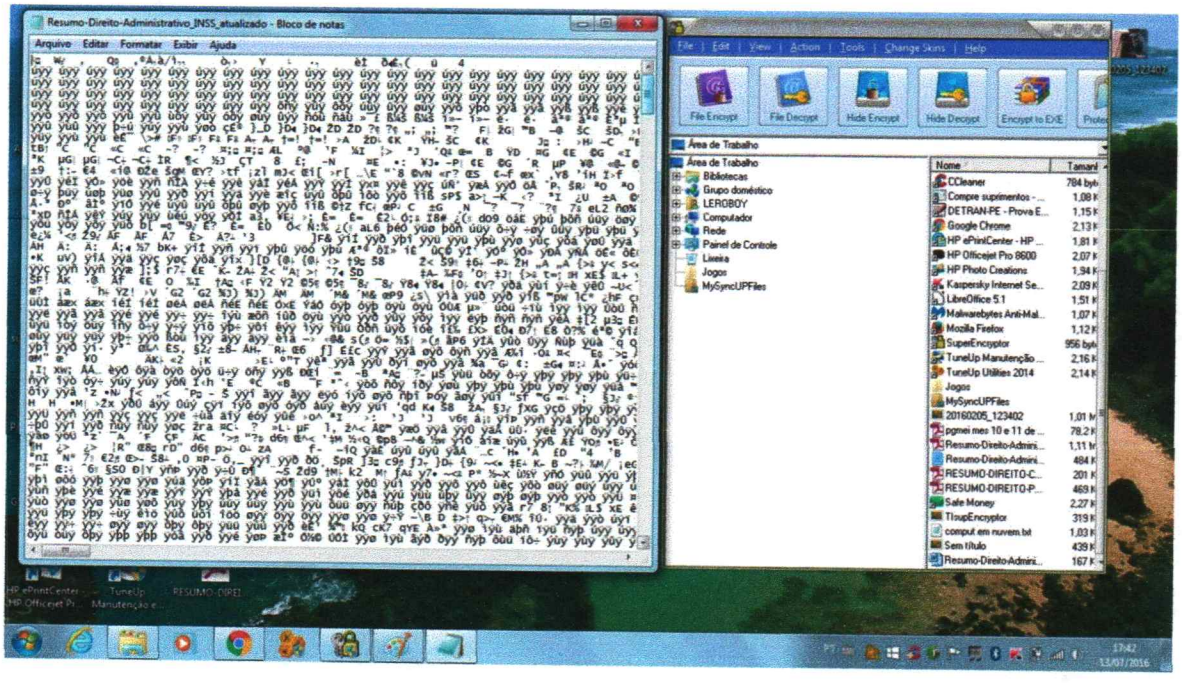
Caso ocorra de alguém com más intensões tentar visualizar alguns dos arquivos os quais estejam encriptados, a tentative será em vão, pois, e le pode até ter acesso ao arquivo, mão não terá o privilégio de destinguir o que está contido nele.

Figura 24 - Visualização de um arquivo Encriptado no método BlowFish



Fonte: AUTORIA PRÓPRIA

Figura 25 - Visualização de um arquivo Encriptado no método AES 256

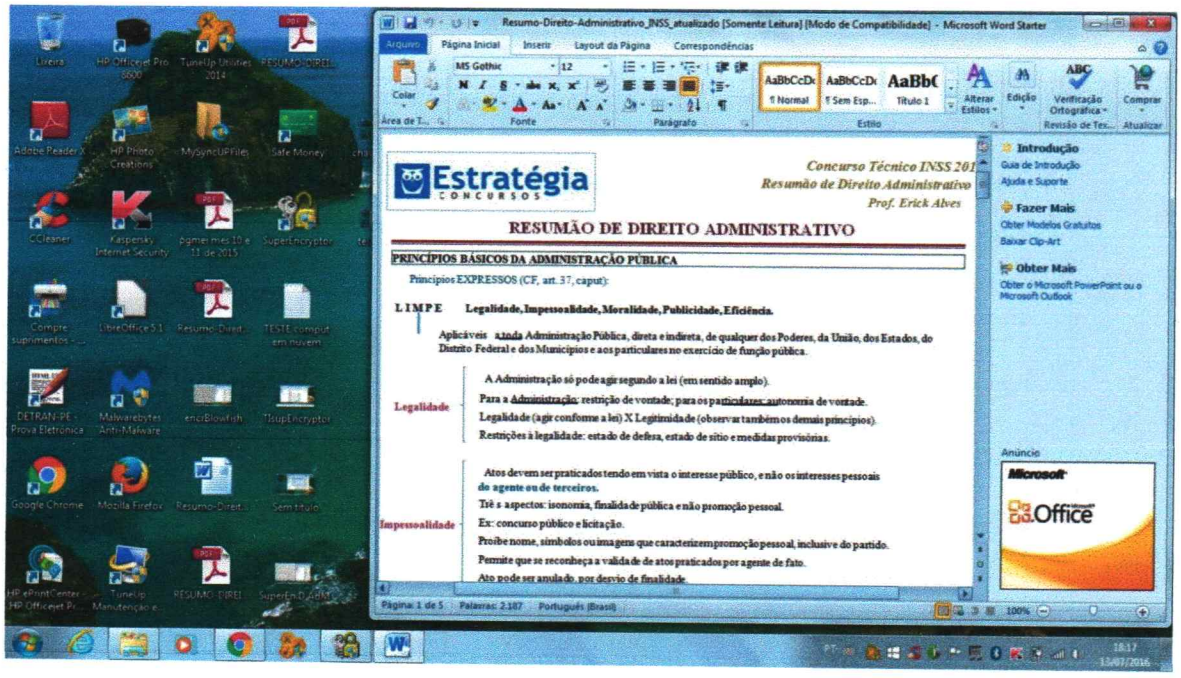


Fonte - AUTORIA PRÓPRIA

Descriptografar arquivos e pastas no *SuperEncryptor*:

- Selecione o arquivo o qual deseja descriptografar;
- Clique no ícone "*File Decrypt*", em seguida, uma caixa de entrada de senha irá aparecer, local onde irá colocar a mesma chave utilizada ao encriptar o arquivo;
- Clique em "OK", pronto! Seu arquivo está descriptado. Após digitar a senha correta, você pode abrir, editar ou salvar o arquivo. Depois de fechar, ele ainda está em estado criptografado, e não há necessidade de criptografá-lo novamente.

Figura 26 - Visualização do arquivo Descriptado



Fonte: AUTORIA PRÓPRIA

5 CONCLUSÃO

O presente trabalho possibilitou uma análise onde empresas e usuários se restringem ao uso da nova tecnologia, tendo como principal receio, o fato em não ter um total conhecimento de como os dados são transmitidos e armazenados aos servidores na nuvem.

A contribuição dos autores frente aos conceitos sobre segurança da informação em nuvem foi de grande importância para a melhor compreensão a respeito dos avanços tecnológicos de forma específica da computação em nuvem que trata em armazenar e assegurar os dados por tempo indeterminado sem o risco de vazamento ou até mesmo a perca definitiva desses dados.

De modo geral empresas e usuários tem razão em ter um certo receio em migrar seus dados para *DATACENTERS* na grande Nuvem, pelo fato de que as informações estarão hospedadas por fornecedores de serviços desconhecidos, pois para empresas e usuários o ideal seria os mesmos terem o privilégio em saber e principalmente ver como de fato seus dados estão sendo armazenados.

De acordo com os objetivos que foram traçados, a questão em relação ao presente trabalho é de fato apresentar aos usuários meios ferramentais que possibilitem que os dados passem por um processo de criptografia mesmo antes de serem enviados para nuvem, possibilitando que usuários tenham maior confiança em saber que terceiros possam até ter acesso aos dados, porém não terá o privilégio de decifrar e modificar e destruir as informações as quais estarão armazenadas em Nuvem.

No decorrer do trabalho foram citados provedores de segurança em computação em nuvens chamado *tresorit*, onde a empresa desenvolvedora destaca como uma das principais características a Criptografia end-to-end, (ponta a ponta), essa tecnologia tem como objetivo manter arquivos criptografado onde nem mesmo a equipe *tresorit* e nem poderes governamentais sejam capazes de decifrar as informações, pois o que se pode ver nos servidores são apenas bits aleatórios.

Para trabalhos futuros, pode ser interessante uma análise mais detalhada de como os dados são armazenados nestes servidores nas nuvens, de forma a contribuir no entendimento de como é possível implementar de forma mais segura métodos que possam garantir uma maior segurança dos dados dos seus clientes.

REFERÊNCIAS

ARRUDA, Felipe. **Os 9 maiores roubos de dados da Internet**. Disponivel em: < http://www.tecmundo.com.br/seguranca/26476-os-9-maiores-roubos-de-dados-da-internet.htm >. Acesso em: 10 Mai 2016.

ARRUDA, Leoclides Milton. **A Terceirização e a Segurança da Informação e Comunicações no Serviço Público.** Era da Tecnologia da Informação, v. 1, n. 1, 2014. Disponivel em: https://repositorio.ufsc.br/bitstream/handle/123456789/84431/188664.pdf?sequence=1 Acesso em: 18 Mai 2016.

BICAKCI, Kemal; YAVUZ, Davut Deniz; GURKAN, Sezin. TwinCloud: A Client-Side Encryption Solution for Secure Sharing on Clouds Without Explicit Key Management. **arXiv preprint arXiv:1606.04705**, 2016. Disponivel em: < http://arxiv.org/pdf/1606.04705v1.pdf > Acesso em 30 Jun 2016.

CASTRO, R. C. C., Pimentel de Sousa, V. L., **Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança**, In: III Congresso Tecnológico de TI e Telecom InfoBrasil 2010, Anais Eletrônicos; Fortaleza, CE, 2010. Disponível em: <http://www.infobrasil.inf.br/userfiles/26-05-S5-1-68740Seguranca%20em%20Cloud.pdf >Acesso em 20 Nov 2015.

CLOUD SECURITY ALLIANCE. **"Guia de Segurança para Áreas Críticas Focado em Computação em Nuvem V2.1"** (2009) Disponivel em: < https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf > Acesso em 05 Mai 2016.
DA COSTA CARMO, Luiz Fernando Rust; CORRÊA, André Sion Fernandes Muniz. **Algoritmos Simétricos para Software Embarcado.** Rio de Janeiro - 2009. Disponivel em: < http://equipe.nce.ufrj.br/rust/Mestrado%202009/SionSimetricAlg2009_SR.pdf> Acesso em 11 Set 2016.

DA CUNHA, Amanda Souza et al. **Relevância da Educação Física na Escola Inclusiva para o Individuo com Síndrome de Down**. Disponivel em: < http://www.pucrs.br/edipucrs/XSalaoIC/Ciencias_da_Saude/Educacao_Fisica/71054-AMANDA_SOUZA_CUNHA.pdf > Acesso em: 17 Mai 2016.

DANTAS, Marcus Leal (2011). **"Segurança da Informação: uma abordagem focada em gestão de riscos."** *Recife: Livro Rápido-Elógica.*

DIAS, Jean Miguel; RITA DE CÁSSIA, M. C.; PIRES, Daniel Facciolo. **A segurança de dados na computação em nuvens nas pequenas e médias empresas.** Revista Eletrônica de Sistemas de Informação e de Gestão Tecnológica, v. 2, n. 1, 2012.
DOCPLAYER: Capítulo 17 – **Considerações quanto à Segurança na Computação na Nuvem:** Disponivel em: http://docplayer.com.br/926759-Capitulo-17-consideracoes-quanto-a-seguranca-na-computacao-na-nuvem-consideracoes-quanto-a-seguranca-na-computacao-na-nuvem.html> Acesso em: 17 Mai 2016.

E-DOMÍNIOS (2016), Disponivem em :< http://www.e-dominios.com.br/sitelock > Acesso em 07 Jun 2016

FILHO, Antonio Mendes da Silva. Segurança da Informação: **Sobre a Necessidade de Proteção de Sistemas de Informações.** Disponível em: < http://espacoacademico.com.br/042/42amsf.htm > 11/2004. Acesso em 06 Dez 2015.

Folha de S.Paulo: **Praias da Tailândia afetadas por Tsunami em 2004 ainda falham em Segurança**. Disponvel em: < http://www1.folha.uol.com.br/turismo/1179058-praias-da-tailandia-afetadas-por-tsunami-em-2004-ainda-falham-em-seguranca.html > Acesso em: 11 Mai 2016

GARCIA, Marco A.B.A **Definição, funcionamento e aplicações da computação em nuvem (cloud computing).** 2009. 08f. Artigo. Universidade Estadual Paulista " Júlio de Mesquita Filho" (UNESP), São José do Rio Preto – SP, 2009: Disponivel em < api.ning.com/files/...nBFVtyHGYlzS/**computacao_em_nuvem**.pdf> Acesso em 05 Abr 2016.

GODOY, Arlida Schmidt. **Introdução à pesquisa qualitativa e suas possibilidades**. Revista de administração de empresas, v. 35, n. 2, p. 57-63, 1995.

GOOGLE. (s.d.). GoogleCareers. Disponivel em: <http://www.google.com/about/careers/lifeatgoogle/a-rare-inside-look-at-google-data-centers.html> Acesso em: 04 Mai 2016

GUERRA, Fernando CGD; VELOSO, Marcelo de Alencar; MASSENSINI, Rogério Luís. **Cloud Computing:** questões críticas para a implementação em organizações públicas. 2012.Disponivel em: < http://repositorio.fjp.mg.gov.br/consad/bitstream/123456789/638/1/C5_TP_CLOUD%20COMPUTING%20QUEST%C3%95ES%20CR%C3%8DTICAS%20PARA.pdf> Acesso em 16 Mai 2016.

GUGELMIN, Felipe.**Os maiores ataques hackers da história**. Disponivel em: < http://www.tecmundo.com.br/seguranca/9971-os-maiores-ataques-hackers-da-historia.htm >. Acesso em: 10 Mai 2016.

JUNIOR, C. (17 de Dezembro de 2014). *conexaosystem*. Fonte: conexaosystem Gestão de TI e Impressã: Disponivel em < http://www.conxaosystem.com.br/blog/2014/12/17/82423/> Acesso em 25 Abr 2016.

LATHA, S. Raju1 K. Santhi2 S.; RAJU, K.; SANTHI, S. **Overview of dropbox encryption in cloud computing**. Transactions on Engineering and Sciences, v. 2, n. 3, p. 27-32, 2014. Disponivel em: **< http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.641.4824&rep=rep1&type=pdf** > Acesso em 07 Jul 2016.

MACHADO, Cesar de Souza et al. **Gerenciamento da segurança da informação em sistemas de teletrabalho**. 2002. Disponivel em:< https://repositorio.ufsc.br/bitstream/handle/123456789/84431/188664.pdf?sequence=1 > Acesso em: 18 Mai 2016.

MELL, Peter, and Tim Grance. **"The NIST definition of cloud computing**." (2011):20-23.Disponivel em: < http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf > Acesso em 03 Mai 2016.

MIGUEL, Paulo Augusto Cauchick. **Estudo de caso na engenharia de produção**: estruturação e recomendações para sua condução. Revista Produção, v. 17, n. 1, p. 216-229, 2007: Disponivel em: < http://www.scielo.br/pdf/%0D/prod/v17n1/14.pdf> Acesso em: 17 Mai 2016.

MOIA, Vitor Ugo Galhardo (2016). **Estudo propõe técnicas para a segurança de dados em nuvens**. Disponivel em:

http://www.unicamp.br/unicamp/sites/default/files/jornal/paginas/ju_652_paginacor_07_web.pdf Acesso em: 27 Mai 2016.

MOIA, Vitor; HENRIQUES, Marco Aurélio Amaral. Cloud Privacy Guard (CPG): Security and Privacy on Data Storage in Public Clouds. In: **VIII Congreso Iberoamericano de Seguridad Informática**. 2015. Disponivem em: <http://www.dca.fee.unicamp.br/~vhgmoia/papers/artigo_CIBSI.pdf > Acesso em 06 Jul 2016.

NEULS, Karina. **A atuação do Ministério Público no Processo Civil**. 2012. Disponivel em: http://dspace.idp.edu.br:8080/xmlui/bitstream/handle/123456789/311/Monografia_Karina%20Neuls.pdf?sequence=1 Acesso em: 17 Mai 2016.

OFICINADANET. (24 de novembro de 2008). ***Segurança da informação, conceitos e mecanismos***. Fonte: oficinadanet: Disponivel: em: <https://www.oficinadanet.com.br/artigo/1307/seguranca_da_informacao_conceitos_e_mecanismos> Acesso em 28 Abr 2016

PARCHEN, Charles Emmanuel; FREITAS, Cinthia Obladen Almendra; EFING, Antônio Carlos. **Computação em nuvem e aspectos jurídicos da segurança da informação**. Revista Jurídica Cesumar-Mestrado, v. 13, n. 1, 2013.

REICHER, Cristiano. **Segurança da informação no acesso à internet banking**. 2011.

SÊMOLA, Marcos et al. **Gestão da segurança da informação**. Elsevier Brasil, 2003

SILVA, Cristiane Débora; Nogueira Augusto. (2015, Janeiro, 1). **Cloud Computing: o reflexo das políticas de segurança nas organizações de.** ***Cloud Computing:*** *the reflection of the security policies in large organizations*, p. 10. Disponivel em: http://revistapensar.com.br/tecnologia/pasta_upload/artigos/a92.pdf >Acesso em 31 Dez 2015

SITELOCK (2016), Disponivel em:<https://www.sitelock.com/web-application-firewall.php> Acesso em 07 Jun 2016

SOUSA, Flávio RC, Leonardo O. Moreira, and Javam C. Machado. "**Computação em nuvem: Conceitos, tecnologias, aplicações e desafios.**" *II Escola Regional de Computação Ceará, Maranhão e Piauí (ERCEMAPI)*(2009): 150-175: Disponivel em<https://www.researchgate.net/profile/Javam Machado/publication/237644729 Computao em Nuvem Conceitos Tecnologias_Aplicaes_e_Desafios/links/56044f4308aea25fce3121f3.pdf> Acesso em 01 Mai 2016.

TRESORIT (2016), Disponivel em: < https://tresorit.com/features > Acesso em 01 Jul 2016

TRESORIT (2016), Disponivel em: < https://tresorit.com/pricing/basic > Acesso em 03 Jul 2016

VALUEHOST (2016), Disponivel em :< https://www.valuehost.com.br/sitelock-seguranca > Acesso em 07 Jun 2016

VERAS, M. (2012). ***Cloud Computing Nova Arquitetura da TI***. SãoPaulo: Eletronica: Abreu'sytem LTDA