FACULDADE UNYLEYA

Naziro Hamed de Assis Lima

SEGURANÇA DA INFORMAÇÃO EM AMBIENTES CORPORATIVOS NA NUVEM

Vitória-ES
2018

Naziro Hamed de Assis Lima

SEGURANÇA DA INFORMAÇÃO EM AMBIENTES CORPORATIVOS NA NUVEM

Monografia apresentada à Faculdade UnYLeYa como exigência parcial à obtenção do título de Especialista em Cybercrime e Cybersecurity: Prevenção e Investigação de Crimes Digitais.

Nome do Orientador: Daniel Celestino de Freitas Pereira

Vitória-ES
2018

Naziro Hamed de Assis Lima

SEGURANÇA DA INFORMAÇÃO EM AMBIENTES CORPORATIVOS NA NUVEM

Monografia apresentada à Faculdade UnYLeYa como exigência parcial à obtenção do título de Especialista em Cybercrime e Cybersecurity: Prevenção e Investigação de Crimes Digitais.

Vitória-ES, ____ de _____ de 2018.

Nota de Aprovação: _____

_____

Professor Orientador

Prof. Esp. Daniel Celestino de Freitas Pereira.

Vitória-ES
2018

DEDICATÓRIA

Ao meu Deus que é Pai, Filho e Espírito Santo, aos meus amados pais, esposa, filha, irmão, tia e avó, aos meus amigos, professores e a todos que me auxiliaram de alguma forma ao longo do curso.

AGRADECIMENTOS

Ao Deus onipotente, onisciente e onipresente, por permitir a minha existência e suprir todas as minhas necessidades diariamente.

Aos meus pais, Salimi Hamed Deud de Assis e Francisco de Assis e à minha tia Nagibi Hamed Deoud, por se apresentarem como fonte de amor, apoio e incentivo constante.

Ao meu irmão, Nassif Hamed de Assis que, por meio da sua amizade e carinho fraternal, sempre me impulsionou em seguir adiante e superar as adversidades que se apresentaram ao longo da minha vida.

À minha esposa Ana Paula Lima Penha Hamed, pelo companheirismo, força, dedicação e amor.

À minha filha Diana Ayla Lima Penha Hamed de Assis, que com apenas um sorriso muda completamente o meu dia, a minha noite e o meu coração, inspirando constantemente a evolução do meu dom de ser pai e me possibilitando sentir um pouco daquilo que Deus sente por cada um de nós.

Ao meu amigo Lucas Prado Any, por toda a amizade, apoio e palavras de fé, desde o período do ginásio até os dias de hoje, e por toda a parceria e diversão durante as jogatinas da franquia *Resident Evil* ao longo de quase duas décadas.“*haaa muleke!*”.

“A vida é a infância da imortalidade.”

(Johann Wolfgang von Goethe)

RESUMO

Esta pesquisa constitui-se em uma revisão de literatura que apresenta a segurança da informação na computação em nuvem. Buscou-se evidenciar o valor da informação e a importância da tecnologia da informação para as corporações, assim como os conceitos de computação em nuvem, cibercrime e cibersegurança, seus aspectos técnicos e as formas de implementação de segurança na nuvem. Conclui-se que, embora a computação em nuvem ofereça muitas vantagens para as empresas, principalmente no quesito agilidade e economia, as corporações ainda apresentam resistência na adesão deste serviço por questões de privacidade e segurança. Considera-se que esta proposta de estudo possa expor formas de implementação de segurança para diferentes tipos e arquiteturas de nuvens, objetivando a proteção de dados e informações corporativas.

Palavras chave: Computação em Nuvem, Segurança da Informação, Tecnologia da Informação, Cibercrime, Cibersegurança, Ambientes Corporativos, Virtualização, Data Center, Arquitetura de Nuvem.

ABSTRACT

This research is a literature review that presents information security in cloud computing. The aim was to highlight the value of information and the importance of information technology for corporations, as well as the concepts of cloud computing, cybercrime and cybersecurity, its technical aspects and ways of implementing security in the cloud. It is concluded that, although cloud computing offers many advantages for companies, especially in agility and economy, the corporations still show resistance to adhere to this service due to privacy and security issues. It is considered that this proposal of study can expose forms of security implementation for different types and architectures of clouds, aiming at the protection of data and corporate information.

Keywords: Cloud Computing, Information Security, Information Technology, Cybercrime, Cybersecurity, Corporate Environments, Virtualization, Data Center, Cloud Architecture.

LISTA DE ABREVIATURAS E SIGLAS

AWS – *Amazon Web Services*

CMP – *Cloud Management Platform*

CRM – *Customer Relationship Management*

DC – *Data Center*

DDoS – *Distributed Denial of Service*

DNS – *Domain Name System*

DoS – *Denial of Service*

ERP – *Enterprise Resource Planning*

FTP – *File Transfer Protocol*

HIDS – *Host-based intrusion detection system*

IaaS – *Infrastructure as a Service*

IoT – *Internet of Things*

IP – *Internet Protocol*

NIDS – *Network-based intrusion detection system*

MAC – *Media Access Control*

PaaS – *Platform as a Service*

PDCA – *Plan-Do-Check-Action*

SLA – *Service Level Agreement*

SES – *Simple Email Service*

SGSI – Sistema de Gestão de Segurança da Informação

SI – Sistemas de Informação

SNS – *Simple Notification Service*

SO – Sistema Operacional

SQS – *Simple Queue Service*

SSL – *Secure Socket Layer*

TI – Tecnologia da Informação

TIC – Tecnologia da Informação e Comunicação

USC – *Unified Computing System*

VDI – *Virtual Desktop Infrastructure*

VPC – *Virtual Private Cloud*

LISTA DE GRÁFICOS

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

O tema a ser abordado nesta pesquisa é a segurança da informação em ambientes corporativos na nuvem, o qual não será esgotado durante a sua apresentação, a qual almeja tratar à problemática: quais formas de implementação de segurança são as mais indicadas para a proteção de dados corporativos nos diferentes tipos de computação em nuvem?

A escolha do tema segurança da informação em ambientes corporativos na nuvem se deu devido a sua crescente abrangência e relevância, tanto para as áreas de tecnologia da informação, quanto segurança e ambientes corporativos de todos os portes. As áreas de tecnologia porque enxergam a nuvem como uma oportunidade de se voltarem para a visão dos negócios das corporações, as áreas de segurança porque enxergam a nuvem como um grande desafio para atuação e por fim os ambientes corporativos que vislumbram a nuvem com o anseio de redução de custos associada a uma grande agilidade e praticidade.

Ainda que a computação em nuvem seja um termo que corresponde a um conceito recente, ela já apresenta um conjunto enorme de vantagens a serem fornecidas aos seus usuários, sejam pessoas físicas ou entidades jurídicas, desde a praticidade e de se armazenar uma foto até a agilidade do redimensionamento computacional escalável com considerável economia financeira.

Embora sejam diversos os benefícios que esta tecnologia pode trazer para as corporações, as mesmas ainda possuem resistência em aderi-la, pois em suma desconhecem as implicações de segurança as quais seus dados estariam submetidos em um ambiente em nuvem e destaca-se que as literaturas sobre nuvem ainda são poucas, principalmente as que abordam questões de segurança na proteção de dados. Como a segurança é um quesito complicador para adesão às tecnologias emergentes por parte das empresas, é importante analisar tais tecnologias sobre a ótica de segurança da informação e para isso torna-se necessário conhecer os riscos e brechas associados à tecnologia para se mapear medidas preventivas e reativas.

O objetivo geral desta pesquisa será apresentar as formas de implementação de segurança da informação nos diversos tipos e arquiteturas de nuvem, objetivando a proteção de informações corporativas, visando desta forma, garantir a continuidade

dos negócios da empresa ao passo que ela possa gozar de todas as vantagens da computação em nuvem.

Os objetivos específicos desta pesquisa serão:

- apresentar os conceitos relacionados à informação e aos recursos de tecnologia e suas importâncias para a continuidade dos negócios das empresas;
- apresentar os conceitos relacionados à computação em nuvem, assim como seus principais fornecedores e citar algumas ferramentas disponibilizadas em suas plataformas;
- apresentar os conceitos relacionados ao cibercrime e cibersegurança, os tipos de criminosos, ataques e fraudes presentes no ambiente virtual, os pilares, serviços e política de segurança da informação e as ferramentas de cibersegurança;
- apresentar a relação da política de segurança da informação com o uso de sistemas de gestão da segurança da informação, os conceitos de risco, ameaça, vulnerabilidade e a relação da gestão de riscos com a implementação da segurança em nuvem.

O capítulo 2 abordará o assunto: a importância da informação e tecnologia para as empresas, focando na apresentação dos conceitos de dado, informação, conhecimento, recursos de tecnologia da informação, a importância da informação para a continuidade de negócio, as consequências de perda de dados e a importância de se proteger informações corporativas.

O capítulo 3 abordará o assunto: computação em nuvem, focando na apresentação dos conceitos de virtualização, data centers, computação em nuvem, as vantagens da nuvem, as arquiteturas e tipos de nuvens, os principais fornecedores de serviços de nuvem e citação de algumas ferramentas disponibilizadas por estes fornecedores.

O capítulo 4 abordará o assunto: cibercrime e cibersegurança, focando na apresentação do conceito de cibercrime, tipos de criminosos virtuais, os tipos de ataques e fraudes, o conceito de cibersegurança, os pilares de segurança da informação, ferramentas, softwares, política e sistema de gestão de segurança da informação.

E por fim, o capítulo 5 abordará: a segurança da informação na nuvem, apresentando além da explanação da problemática da pesquisa, a relação da política de segurança da informação com o uso de sistema de gerenciamento de segurança da informação, o conceito de risco, ameaça, vulnerabilidade e a relação entre o gerenciamento de riscos e a segurança da informação na nuvem.

Conforme Vergara (2003, p. 46), “há dois critérios básicos para pesquisa, quantos aos fins e quanto aos meios. Quantos aos fins a pesquisa pode ser exploratória, descritiva, explicativa, metodológica aplicada e intervencionista”.

Esta pesquisa de caráter bibliográfico e na forma de procedimento monográfico por meio da metodologia indutiva de caráter descritivo e qualitativo, apresenta natureza básica ou pura, pois almeja gerar conhecimentos novos e úteis no campo científico, entretanto sem apresentar caráter de aplicação prática. Para Minayo (2002 apud Virtual UFC), esta forma de pesquisa possibilita articular conceitos e sistematizar a produção de determinada área de conhecimento visando criar questões num processo de incorporação e superação daquilo que já se encontra produzido.

Destaca-se que o pesquisador, com o intuito de embasar a revisão de literatura, utilizou fontes primárias de pesquisas, tais como: sites de tecnologia da informação, eletrônica, apostilas de cursos de informática diversos, artigos científicos, monografias para obtenção de título de tecnólogo, bacharel, especialista e dissertações de mestrados, além de sites de empresas da área de informática e sites de notícias, as quais associadas às suas experiências na área de tecnologia, possibilitaram uma apresentação objetiva e de fácil compreensão das formas de implementação de segurança na nuvem para a proteção de dados corporativos.

2 IMPORTÂNCIA DA INFORMAÇÃO E TECNOLOGIA PARA CORPORAÇÕES

A informação serve de guia para que as empresas possam alcançar as oportunidades que surgem no mercado atual, o qual impõe às organizações novos desafios frequentes devido a sua dinâmica global e uma competitividade acirrada em praticamente todos os ramos, o que torna as informações a propriedade de maior valor de mercado que uma entidade corporativa possui, as quais são utilizadas como ferramenta que possibilitam às corporações adquirirem vantagens competitivas em relação aos concorrentes.

> Nas diversas atividades da sociedade, sejam pertencentes aos setores de produção, de serviços, ou de governo, as informações armazenadas nos computadores têm um valor incalculável. Dependendo do objetivo organizacional, a falta dessas informações pode significar dificuldades administrativas e até a paralisação de atividades essenciais (MORAES, E. M., 2007, p. 13).

Destaca-se que muitas das vezes, as oportunidades se tornam imperceptíveis para as empresas devido ao nível deficiente de conhecimento que muitas apresentam ou mesmo à falta de qualidade das informações que chegam até os gestores.
A presença de dados, informações e conhecimentos associados ao uso da tecnologia, servem de suporte à tomada de decisão por parte da gestão.

> Sendo a informação um patrimônio, um bem que agrega valor e dá sentido às atividades que a utilizam, é necessário fazer uso de recursos de TI de maneira apropriada, ou seja, é preciso utilizar ferramentas, sistemas ou outros meios que façam das informações um diferencial. Além disso, é importante buscar soluções que tragam resultados realmente relevantes, isto é, que permitam transformar as informações em algo com valor maior, sem deixar de considerar o aspecto do menor custo possível (ALECRIM, E., 2011).

Desta forma, torna-se necessário que as empresas mantenham seus dados, informações e conhecimentos sempre muito bem estruturados, organizados e que contem com suporte de recursos de tecnologias da informação capazes de gerar relatórios de qualidade que apoiem à gestão nos momentos propícios.

2.1 Dado

O dado corresponde a fragmento ou unidade básica de informação em sua forma mais bruta. O dado não apresenta nenhum sentido quando analisado isoladamente, entretanto quando há um agrupamento de dados relacionados e o conjunto é analisado de forma ordenada, eis que dão origem à informação.

> Dados são códigos que constituem a matéria prima da informação, ou seja, é a informação não tratada que ainda não apresenta relevância. Eles representam um ou mais significados de um sistema que isoladamente não pode transmitir uma mensagem ou representar algum conhecimento (SILVA, 2007 apud REZENDE, 2015).

Em tecnologia da informação (TI), o dado comumente representa uma expressão básica de uma entidade ou evento, tais como: um caractere ou palavra de um texto, um valor de variável ou mesmo o resultado de uma medição.

Conforme Conceito.de (2012), na TI, dados são expressões que descrevem características das entidades sobre as quais operam os códigos computacionais. São expressões que devem ser apresentadas de maneira que possam ser tratadas por um computador. Neste caso, os dados por si só não constituem informação, a menos que esta surja do adequado processamento dos mesmos.

2.2 Informação

A informação pode ser entendida como o resultado ou produto da análise e processamento de um conjunto de dados agrupados que estão inter-relacionados, constituindo a representação de uma mensagem sobre uma determinada entidade ou evento. Cabe destacar que uma informação possui vida útil, que corresponde ao intervalo de tempo em que a mesma apresenta valor agregado.

De acordo com Significados (2012) “Informação é a reunião ou o conjunto de dados e conhecimentos organizados, que possam constituir referências sobre um determinado acontecimento, fato ou fenômeno”.

Para *Wikipedia* (2018), a informação é proveniente da organização, processamento e manipulação de dados, de forma que represente uma modificação (quantitativa ou

qualitativa) no conhecimento do sistema (humano, animal ou máquina) a qual se destina.

2.3 Conhecimento

O conhecimento é o ato do saber e o saber é proveniente do aprendizado, sendo que este último é consequência da análise contínua de informações, ainda com vidas úteis, por um humano ou máquina. O conhecimento possibilita ao seu detentor inferir previsões sobre determinada entidade, assim como estabelecer medidas de segurança, com caráter preventivo, reativo e corretivo, em relação aos fenômenos que permeiam a entidade em questão.

Segundo Davenport e Prusak (1998), o conhecimento corresponde a um misto de experiência condensada, valores e informações contextuais, o qual proporciona uma estrutura para a avaliação e incorporação de novas experiências e informações. Ele tem origem e aplicação na mente dos conhecedores.

Segundo Conceito.de (2010), conhecimento é a capacidade para tomar ciência, por meio da razão, da natureza, das qualidades e das relações das coisas. É um conjunto de dados ou notícias relativos a uma pessoa ou a uma coisa.

Ilustração 01 – Dos dados ao conhecimento

Fonte: MORAES, L., 2014 [1]

[1-] Disponível em <https://pt.slideshare.net/leomoraes/informao-e-conhecimento-nas-organizaes-gesto> Acesso em 11 de fevereiro de 2018.

2.4 A necessidade da informação e do conhecimento para a continuidade dos negócios de uma corporação

Os dados, informações e conhecimentos são os bens mais importantes que uma empresa possui, correspondendo aos seus ativos intangíveis, os quais possuem valor inestimável. Essas três entidades constituem as ferramentas de base para a manutenção da continuidade dos negócios da empresa, possibilitando aos gestores tomarem decisões corretas no momento mais oportuno.

> [...] a informação é o item ideal e primário a que todos devem recorrer para antecipar decisões em todos os sentidos, pois não há tomada de decisão sem conhecimento antecipado, posto que tudo é baseado em conhecimento e este advém da informação. Ou seja, tudo o que acontece resulta em um conhecimento e este é a mola propulsora para, de acordo com as informações que o constitui, originar novas tomadas de decisão, novas informações e, consequentemente, novos conhecimentos (GONÇALVES, M. R.; GOUVEIA; PETINARI, 2008, p. 42/43 apud FURLAN; ASSIS, 2015, p. 37).

2.5 Recursos de tecnologia da informação

Os recursos de TI correspondem a uma variada gama de tecnologias de *hardware* e *software* desenvolvidos com funcionalidades diversas, mas com o intuito de realizar o processamento de dados e proporcionar saídas úteis na forma de informação para seus usuários, além de corresponder também a um conjunto de tecnologias que visa facilitar a comunicação entre dispositivos e sistemas, os quais muitas das vezes estão interconectados através da internet.

> O termo Tecnologia da Informação serve para designar o conjunto de recursos tecnológicos e computacionais para geração e uso da informação. Também é comumente utilizado para designar o conjunto de recursos não humanos dedicados ao armazenamento, processamento e comunicação da informação, bem como o modo como esses recursos estão organizados em um sistema capaz de executar um conjunto de tarefas (*WIKI*2, 2017).

Entre os recursos de TI, podemos destacar como exemplos: computadores, *smartphones*, *storages*, servidores, *e-mails*, aplicativos, sistemas operacionais (SO)s, bancos de dados, roteadores, *switches*, impressoras, telefones *Internet Protocol* (IP), redes cabeadas e *wireless* de computadores, a internet e uma

quantidade imensurável de *hardware* que está crescendo a cada dia, fora os conceitos de serviços de tecnologia de informação, os quais se moldam criando novas tecnologias da informação, tal como a virtualização e a computação em nuvem. Na modalidade de recursos de tecnologia muito utilizados por empresas, destacam-se sistemas de *Customer Relationship Management* (CRM), *Enterprise Resource Planning* (ERP), bancos de dados e sistemas diversos de mineração e análise de dados.

2.6 As consequências do comprometimento de informações corporativas

O comprometimento de informações varia, desde a indisponibilidade de acesso das informações devido à indisponibilidade de sistemas, até mesmo ao sequestro de informações ou ainda a perda total de informações por cibercrimes ou falhas humanas e neste ponto entra a cibersegurança, na tentativa de proteção dos dados e informações, por parte das pessoas ou empresas. O cibercrime e a cibersegurança serão abordados no Item 4 desta pesquisa. Os prejuízos do comprometimento de informações dependem do tipo da informação. Cabe destacar que este comprometimento diz respeito à perda, roubo, sequestro ou simples indisponibilidade por questões técnicas de *hardware* ou *software*.

Segundo Furlan e Assis (2015), em caso de indisponibilidade, por motivos diversos, de informações empresariais sobre legalização ou fiscalização, poderá haver o comprometimento jurídico da empresa perante as esferas do Governo Federal, Estadual e Municipal, perante seus clientes, seus fornecedores e até mesmo os seus funcionários, além dos riscos de prejuízos financeiros, por multas ou indenizações, ou até mesmo, denegrição da imagem da corporação.

Conforme Furlan e Assis (2015, p. 41):

> No caso de perda de dados e informações de negócios, as consequências podem variar desde retrabalho de funcionários e gestores para repor registros de atividades administrativas ou operacionais, conhecimentos e planejamentos (caso exista alguma possibilidade de repor tais informações), até a paralisação de atividades essenciais que comprometam moral e financeiramente a empresa, podendo levá-la à falência.

Ainda, segundo Furlan e Assis (2015, p. 40/41), “Em caso de falhas dos sistemas de TI [...], acarretaria em improdutividade provocada pela ociosidade de funcionários ou mesmo suspensão de atividades essenciais como venda e faturamento, com consequentes prejuízos financeiros ou danos morais, dependendo das atividades comprometidas e clientes e fornecedores afetados”.

2.7 Importância de se proteger informações corporativas

A necessidade de sobrevivência das empresas somada à necessidade de se obter vantagens no mercado visando à expansão empresarial, fez com que a busca por informações e geração de conhecimento se tornassem contínuas e cada vez mais acentuadas e para atender essa demanda as empresas estão se valendo cada vez mais da internet e da informatização dos seus ambientes, os quais muitas das vezes estão sendo migrados para a tecnologia em nuvem, seguindo uma nova tendência do mercado, objetivando gozar das diversas vantagens que este tipo de tecnologia proporciona, a qual será abordada no Item 3 desta pesquisa, sendo que no meio disso tudo, torna-se cada vez mais necessário tentar garantir a segurança das informações.
Conforme a ABNT NBR ISO/IEC 17799:2005 (2005, p. 9):

> Os ambientes informatizados das organizações estão expostos a uma grande diversidade de ameaças à segurança de seus dados e informações armazenadas digitalmente, desde falhas humanas na manipulação de dados, até roubos virtuais que comprometam a estrutura do software e incidentes naturais; que possam comprometer a estrutura de hardware.

Uma vez apresentada a importância da informação e do suporte das tecnologias para as empresas, visando a continuidade do negócio com praticidade, econômica e agilidade, assim como algumas consequências provenientes de um cenário hipotético de indisponibilidade de informações, torna-se perceptível a necessidade de se implementar segurança nos ambientes tecnológicos que irão armazenar, processar, trafegar, compartilhar e distribuir os dados e informações corporativas.

3 A COMPUTAÇÃO EM NUVEM

Os recursos de TI estão sendo aderidos e utilizados com maior frequência no mercado. A TI corresponde ao meio que as empresas da atualidade encontraram para disponibilizar o acesso aos seus serviços da forma dinâmica que o mercado exige.

Segundo Orlandini (2005), os recursos de TI são peça fundamental para as empresas, pois já fazem parte de todos os departamentos e atividades da companhia, desde o simples controle até a confecção de planos estratégicos complexos.

> As empresas utilizam os serviços e sistemas de informações (SI) como forma de disponibilizar seus serviços básicos, os quais se expandem conforme a demanda do mercado e para que seja possível suportar a crescente demanda dos serviços da corporação, os recursos de tecnologia precisam ser utilizados de forma otimizada, a qual permita sua realocação ou expansão de forma segura, monitorada e econômica, ou seja, os gestores devem saber exatamente em quais tecnologias investir para suportar suas demandas empresariais (HAMED, 2017, p. 16).

A computação em nuvem corresponde a um paradigma de TI no qual a infraestrutura é disponibilizada como um serviço que pode ser locado e que possibilita enorme escalabilidade, agilidade e desempenho com custo reduzido, o que a torna extremamente atrativa para as empresas da atualidade, uma vez que as mesmas buscam consolidação no mercado.

3.1 Definição de virtualização

A virtualização é um dos recursos de TI mais admirados e utilizados dentro das empresas da atualidade e seu conceito compõe grande parte das tecnologias de nuvem. A virtualização consiste na simulação via *software* de algo concreto, tais como: um computador, um servidor, um disco de armazenamento, SO e outros. A principal vantagem da virtualização é a possibilidade de alocar e realocar os recursos virtualizados de forma muito prática e ágil, aproveitando ao máximo possível os recursos que geralmente ficam ociosos nos servidores físicos, ou seja, seria possível executar diversos SOs simultaneamente, utilizando-se da capacidade computacional de uma mesma máquina física.

Segundo Choinacki (2012, pág. 14), “virtualização é o termo que define a abstração ou simulação de recursos computacionais. Em uma definição livre, é o processo de executar vários sistemas independentes em um único equipamento”.

> Virtualização é um processo de criar uma representação baseada em *software* de algo, em vez de um processo físico. A virtualização pode se aplicar a aplicativos, servidores, armazenamento e redes. É a maneira mais eficaz de reduzir as despesas de TI e ao mesmo tempo, aumentar a eficiência e a agilidade para empresa de todos os portes (ONE LINEA TELECOM, 2017).

3.2 Definição de data center

O *data center* (DC) corresponde à uma central de processamento e armazenamento de dados, informações, *softwares*, SOs e diversos serviços relacionados com a TI, os quais são disponibilizados através da rede ou internet. Geralmente o ambiente físico de um DC é projetado com um conjunto de servidores, discos de armazenamentos e diversos dispositivos que estão interligados em rede, com o propósito de oferecer serviços de forma ininterrupta, estando munidos de proteção contra falhas de *hardware* e *software* (através de *clusters*), *link* de dados (por meio da redundância de *link*), quedas de energia (com uso de *nobreaks* e geradores), incêndio (com gás e *sprinkler*), inundação (com elevação do piso e vedação da sala ambiente), superaquecimento (através da redundância de ares condicionados) e acesso não autorizado (através do uso de biometria conjugado com código de acesso). Destaca-se que os DCs podem estar interligados entre si, formando uma rede de DCs, desde que tenham sido configurados para este propósito.

> Um *Data Center* é uma modalidade de serviço de valor agregado que oferece recursos de processamento e armazenamento de dados em larga escala para que organizações de qualquer porte e mesmo profissionais liberais possam ter ao seu alcance uma estrutura de grande capacidade e flexibilidade, alta segurança, e igualmente capacitada do ponto de vista de *hardware* e *software* para processar e armazenar informações (PINHEIRO, 2004).

3.3 Conceito de computação em nuvem

A computação em nuvem pode ser entendida como um conjunto de serviços de TI disponibilizado por meio de um conjunto de *hardwares* e *softwares*, concentrados

em DCs, os quais utilizam o conceito de virtualização para fornecer o escalonamento de recursos de forma rápida e sob demanda. Os acessos aos serviços são feitos por meio da internet ou intranet de acordo com a arquitetura de nuvem, por usuários de todos os tipos e perfis, desde que possuam as devidas permissões e credenciais.
Segundo Alves et al. (2013), as nuvens encontram-se disponibilizadas em centrais de processamento de dados que podem abrigar milhares de máquinas de pequeno porte físico e com enorme capacidade de processamento e que utilizam os mais recentes *softwares* definidos como *Web* 2.0, além do uso dos conceitos de virtualização e código aberto.

> Computação em nuvem é um paradigma de computação em larga escala que possui foco em proporcionar economia de escala, em que um conjunto abstrato, virtualizado, dinamicamente escalável de poder de processamento, armazenamento, plataformas e serviços são disponibilizados sob demanda para clientes externos através da internet. (FOSTER, s/d, s/p. apud MULLER, 2010 p.18 apud ALVES et al., 2013, p. 3).

Outra definição para a computação em nuvem é que a mesma corresponde a um enorme grupo de serviços de TI, disponibilizados via *web*, o qual pode assumir o papel parcial ou quase que integral do ambiente de TI de uma empresa.

3.4 Benefícios da computação em nuvem

O advento da computação em nuvem provê muitas vantagens para as entidades empresariais, dentre elas podem ser destacados: custo, agilidade, escala global, produtividade, desempenho e confiabilidade.

3.4.1 Redução de custo

Na computação em nuvem os recursos são provisionados de acordo com a demanda da empresa. Em relação à redução de custos, para Taurion (2009, p. 40):

> O fator redução de custos aparece devido ao compartilhamento de recursos, economias de escala e maior padronização arquitetônica. A computação em nuvem implementa na prática o conceito de computação sob demanda, no qual os serviços computacionais são alocados à medida que a demanda aparece.

Como na computação em nuvem os serviços de TI são disponibilizados via internet e não há necessidade dos mesmos serem implementados dentro da empresa em questão, poupa-se recurso, pois muitas das vezes não há necessidade de: montagem de DCs locais, gasto com energia elétrica, climatização e profissionais para a manutenção dos mesmos, aquisição de *racks* e servidores, aquisição de licenciamento de diversos *softwares* e sistemas diversos, ou ainda atualização de *hardwares* e *softwares*.

> No caso dos custos de manutenção, a computação em nuvem reduz vertiginosamente os custos de manutenção de *hardware* e de *software*. Com a necessidade de menos servidores físicos na empresa, os custos de manutenção são imediatamente reduzidos e, como as aplicações em nuvem estão na nuvem, não há *software* em computadores da organização para manter (PINTO, 2012).

Os computadores locais não exigem um *hardware* robusto, o que também reduz o custo, uma vez que as aplicações serão processadas na nuvem e não nos computadores dos usuários.

Conforme Pinto (2012), não há necessidade de um computador de última geração para executar as aplicações que estão na nuvem [...], dessa forma, podem ser adquiridos computadores de menor custo, com capacidade para executar, basicamente, o SO e o navegador *web*.

Os *softwares* e aplicações também são disponibilizados na nuvem por valores muito inferiores ao valor do licenciamento clássico, por usuário ou computador, o qual está cada vez mais elevado, fora que muitos *softwares* possuem licenciamento que não permitem suas atualizações para versões posteriores, o que acaba obrigando as empresas a adquirirem novos licenciamentos, enquanto na grande gama dos serviços de nuvem, os *softwares* são disponibilizados em suas versões mais atuais, sem que isso acarrete uma onerosidade demasiada ao cliente do serviço de computação em nuvem.

Segundo Pinto (2012), não é necessária a aquisição dos *softwares*, já que as empresas de computação em nuvem cobram um valor para disponibilizá-los como serviço. E ainda há empresas que estão oferecendo aplicações baseadas na *web* de graça, o que torna muito mais atrativo do que pagar os altos valores de licenciamento de *software* cobrados tradicionalmente.

3.4.2 Acesso

A questão do acesso está associada à facilidade e praticidade que o usuário possui disponíveis para solicitar os serviços de computação em nuvem. Como todo tipo de solicitação de serviço de nuvem começa pela internet, basta que o usuário possua um dispositivo conectado para que possa solicitar serviços, desde acesso a um arquivo qualquer armazenado à solicitação de um novo servidor de banco de dados.

3.4.3 Agilidade

A agilidade relaciona-se com o período de tempo necessário para que uma solicitação de serviço seja registrada e atendida. É comum que no serviço de nuvem o usuário registre a demanda, a qual é atendida automaticamente (autosserviço) e que de acordo com a necessidade provisione recursos de TI em questão de minutos.

3.4.4 Escalabilidade

A escalabilidade da tecnologia de nuvem permite provisionar grandes ou pequenas quantidades de recursos de TI de acordo com a necessidade momentânea da empresa ou usuário.

> Este cenário de escalabilidade de serviços, processos e infraestrutura quase ilimitados não possui precedentes e efetivamente melhora a flexibilidade relacionada a estruturas de tecnologia de informação (TI) bem como pode diminuir o custo total dos negócios pelo provimento de serviços sob demanda (BORGES et al., 2011, p. i).

Segue exemplo dos recursos que podem ser provisionados conforme necessidade: capacidade de processamento, armazenamento de dados, largura de banda, memória, SOs e outros.

> Enfim, para os usuários, os recursos parecem ser ilimitados e podem ser adquiridos em qualquer quantidade, ou seja, a demanda do usuário deve determinar a liberação e aquisição dos recursos e isto deve ser executado de forma rápida, transparente e sem intervenção humana (BORGES et al., 2011, p. 6).

Destaca-se que o pagamento dos serviços é proporcional à quantidade de recursos utilizados por tempo de uso. Desta forma, a empresa economiza em não ter que adquirir recursos para atender uma demanda temporária, os quais ficariam ociosos após a demanda se extinguir.

> Não é necessário contratar uma capacidade máxima antes mesmo de a empresa precisar por conta do aumento da demanda. Quando chegar o momento, fazer *upgrades* (memória, espaço de disco etc.) é fácil e rápido – gerando, inclusive, mais previsibilidade de investimento (SOARES, 2016).

3.4.5 Produtividade

Uma vez que a base crítica da infraestrutura de TI está montada fora da empresa e as atividades de manutenção estão ao encargo da nuvem, as equipes de tecnologia das empresas podem focar sua visão na obtenção de metas de negócios e aplicação das mesmas.

3.4.6 Desempenho

Os DCs que suportam os serviços de nuvem são sempre equipamentos e atualizados com as mais novas gerações de *hardware* e *software*, sendo que os DCs de um mesmo fornecedor geralmente estão interligados em uma rede mundial de DCs, o que permite ao fornecedor garantir um enorme desempenho dos seus serviços de computação em nuvem.

3.4.7 Confiabilidade

A confiabilidade refere-se à garantia de manutenção dos serviços disponibilizados e dos dados empresarias que estão armazenados na nuvem.
Conforme apresentado no item 3.2, os DCs estão interligados em rede e desta forma, quando há um problema com um DC específico ou com um componente de *hardware*, outro similar assume a atividade de forma a evitar falhas na prestação do serviço.
“Um sistema é dito confiável se ele não falha com frequência e, mais importante, se ele não perde os dados ao falhar” (SUN, 2009a apud CHIRIGATI, 2009).

Quanto ao *backup* dos dados, há possibilidade de configurar a redundância do mesmo em outro DC do fornecedor, ou ainda, há serviços em que a redundância do *backup* já é padrão e não necessita de qualquer intervenção do usuário para que ocorra. Segundo *Data Science Academy* (2017), a computação em nuvem proporciona facilidade e redução de custos de *backup*, recuperação de desastre e continuidade dos negócios, uma vez que dados podem ser espelhados em sites redundantes na rede do provedor de nuvem.

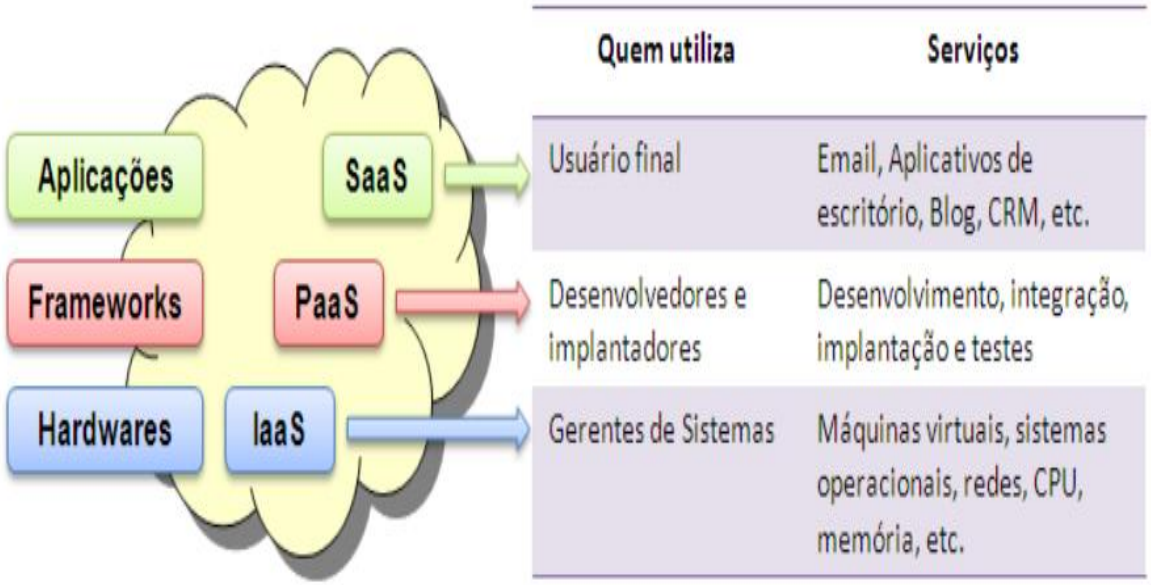
3.4.8 Colaboração

Esta característica possibilita que os arquivos sejam acessados e editados simultaneamente de diferentes localidades geográficas, enquanto às atualizações são exibidas na tela de cada usuário que esteja executando o arquivo, facilitando a execução de atividades de projetos por exemplo. Assim, a colaboração se torna um fator consideravelmente positivo para as empresas.

3.5 Arquiteturas de serviços de nuvem

As arquiteturas de serviços de nuvem, também denominados modelos, ou pilhas, são divididos em três grupos básicos: o IaaS, o PaaS e o SaaS. Esta divisão em grupos pode ser entendida como uma representação modular dos meios como a computação em nuvem é oferecida. Segue representação da arquitetura de serviços em nuvem:

Ilustração 02 – Arquiteturas de nuvem x usuário x serviço



Fonte: BORGES et al., 2011, p. 8 [2]

3.5.1 A arquitetura IaaS

A arquitetura *Infrastructure as a Service* (IaaS), em português: Infraestrutura como Serviço, disponibiliza recursos como máquinas virtuais, SOs, processadores, memórias, discos e outros, como serviços que são gerenciados através de um sistema *web* ou plataforma, os quais são acessados pelos gerentes de sistemas. Através da internet os usuários conseguem efetuar as operações, tais como provisionamento de recursos, gerência e monitoramento dos serviços contratados.

Segundo ASCHOFF (2016), “Significa Infraestrutura como um Serviço e engloba os *hardwares*, como componentes de rede, discos, dispositivos de armazenamento, servidores e outros elementos físicos do sistema”.

O IaaS representa a primeira camada do modelo conceitual de arquitetura de serviços em nuvem e desta forma corresponde ao serviço mais básico da modalidade. No IaaS o usuário contrata/aluga os recursos que irá utilizar conforme a demanda.

Conforme Borges et al. (2011, p. 8), “A infraestrutura é baseada na virtualização dos recursos computacionais que pode ser dinamicamente escalada para aumentar ou diminuir os recursos de acordo com as necessidades das aplicações”.

[2-] BORGES, Hélder Pereira; MURY, Antonio Roberto; SCHULZE, Bruno; SOUZA, José Neuman de Souza. Computação em nuvem. Artigo científico, Brasil, 2011.

Em relação às vantagens do IaaS podem ser destacadas: redução de investimentos em *hardware* e *software*, bem como a preocupação com a depreciação dos mesmos, eliminação de custos com configuração inicial, manutenção e segurança de DCs, otimização do desempenho, disponibilização de espaço físico na empresa e flexibilidade para ampliar e reduzir a capacidade de processamento e/ou armazenamento.

Segundo Souza S. F. (2009 apud Borges et. al., 2011), o IaaS possui como principal objetivo tornar mais fácil e acessível o fornecimento de recursos, como servidores, redes, armazenamento e outros que são fundamentais na construção de um ambiente sob demanda podendo ser tanto SO quanto aplicativos.

> Nesse cenário o serviço possui uma infraestrutura de *hardware*, que é responsável pelo processamento e armazenamento de dados. Nessa infraestrutura é presente a tecnologia de virtualização. O princípio básico da virtualização é o compartilhamento da mesma máquina física por diferentes máquinas virtuais. Pode-se oferecer essas máquinas virtuais para diversos clientes, dividindo seus recursos de máquina entre eles. Esses clientes utilizam esses recursos virtualizados para oferecer seus serviços. Por exemplo, é oferecida para o cliente uma máquina virtual com um sistema operacional instalado e o cliente irá usa-la para executar as suas aplicações (VAQUERO et al. 2008 apud GONÇALVES, 2011, p. 25).

Quanto à delegação de responsabilidades, na arquitetura IaaS o usuário/cliente deverá focar, a equipe de TI da empresa, em toda a estrutura de aplicações e *softwares*, ferramentas e *frameworks* de desenvolvimento, sistemas de banco de dados e SOs em casos diversos, enquanto todos os outros aspectos, tais como, rede e *link* de dados para a disponibilização da infraestrutura, *storage*, servidores, máquinas virtuais e outros, ficaram ao encargo da fornecedor do serviço de nuvem.

Segue a representação da delegação de responsabilidades no IaaS:

Ilustração 03 – Delegação de responsabilidades no IaaS

Fonte: Página do Geraldo Loureiro no *Wiki* [3]

3.5.2 A arquitetura PaaS

A arquitetura *Platform as a Service* (PaaS), em português: plataforma como serviço, é composta por um conjunto de *frameworks*, modelos de projetos, desenvolvimento, implantação, teste, hospedagem, integração de banco de dados e serviços *web*, segurança e outros similares que possibilitam aos usuários desenvolverem suas próprias aplicações de forma a abstrair toda a configuração e gerenciamento da infraestrutura necessárias para suporte do ambiente, sendo todos estes serviços disponibilizados através da internet, sem necessidade de aquisição de licenciamento de ferramentas de desenvolvimento e *softwares* afins.

> Uma plataforma de nuvem com a capacidade de construir, testar, implementar, executar e gerenciar aplicativos na nuvem. Plataformas de *Cloud* oferecem alternativas a essas ações, por exemplo, a experiência de construir pode ser apenas online ou apenas *off-line*, ou uma combinação dos dois (CHANTRY, 2009 apud GONÇALVES, 2011, p. 25).

[3-] Disponível em:<http://www.geraldoloureiro.com/wiki/index.php?title=1o_Fórum_IBGP_de_Debates> Acesso em 15 de fevereiro de 2018.

O PaaS, segundo Carvalho (2017), é um ambiente de desenvolvimento e implantação completo na nuvem, com recursos que permitem fornecer tudo, de aplicativos simples baseados em nuvem a sofisticados aplicativos empresariais habilitados para a nuvem.

O PaaS representa a camada intermediária do modelo conceitual, e fornece as mesmas vantagens que o IaaS. A vantagem adicional é a disponibilidade de todo um ambiente robusto de desenvolvimento sem a necessidade de pagar por licenciamento das ferramentas do ambiente e sem a necessidade de manutenção da infraestrutura e outro detalhe é que a equipe de desenvolvimento pode estar distribuída geograficamente sem que isso gere impactos aos projetos.

> As arquiteturas *platform-as-a-service* (PaaS) têm surgido nos últimos anos para aliviar os encargos da gestão de recursos. Este fator aumentou a produtividade para desenvolvedores e suas respectivas organizações. Os desenvolvedores não precisam mais se preocupar com detalhes de nível inferior, como o consumo de CPU, as limitações de largura de banda, o consumo de memória e uso de disco, como era comum no passado. A escala de aplicações é agora o ônus do sistema da plataforma. Sistemas PaaS se tornaram os sistemas operacionais do *datacenter* (ALMEIDA, 2014, p. 53).

Na arquitetura PaaS, quanto à delegação de responsabilidades, o usuário/cliente deverá focar, a equipe de TI da empresa, em toda a estrutura de aplicações e *softwares* e ferramentas analíticas para análise de negócios, enquanto SOs e sistemas de banco de dados, rede e *link* de dados para a disponibilização da infraestrutura, *storage*, servidores, máquinas virtuais e outros, ficaram ao encargo da fornecedor do serviço de nuvem.

Segue a representação da delegação de responsabilidades no PaaS:

Ilustração 04 – Delegação de responsabilidades no PaaS

Fonte: Página do Geraldo Loureiro no *Wiki* [4]

3.5.3 A arquitetura SaaS

A arquitetura *Software as a Service* SaaS), em português: *software* como serviço, entrega o *software* produto final. Disponibiliza para os usuários, conjuntos de aplicações completas, as quais podem ser contratadas conforme a demanda. As aplicações disponibilizadas nesta arquitetura são todas processadas no ambiente de nuvem e sua personalização é regulada por modelos de negócios que geralmente são previamente definidos pelos fornecedores do serviço, embora alguns serviços sejam altamente customizáveis.

> Os sistemas de *software* devem estar disponíveis na internet através de uma interface com um navegador *web*, logo devem ser acessíveis de qualquer lugar a partir dos diversos dispositivos dos usuários. Desta forma, novos recursos podem ser adicionados aos sistemas de forma transparente aos usuários, tornando-se assim a manutenção e evolução dos sistemas tarefas bem mais simples (BORGES et al., 2011, p. 10).

O SaaS representa a última camada do modelo conceitual, e suas principais vantagens são o fornecimento de aplicativos corporativos sofisticados, tais como

[4-] Disponível em:<http://www.geraldoloureiro.com/wiki/index.php?title=1o_Fórum_IBGP_de_Debates> Acesso em 15 de fevereiro de 2018.

CRM e ERP, por valores muito mais acessíveis, uma vez que não se paga por licenciamento das ferramentas, mas sim por locação das mesmas, segundo Borges et al. (2011, p. 10), “A aquisição de licenças para uso é dispensada para a utilização do SaaS, reduzindo-se então custos operacionais”. Todas as ferramentas são disponibilizadas via internet sem necessidade de atualização, aplicação de *patches* de segurança e compatível para diversas plataformas de SOs.

Quanto à questão da delegação de responsabilidades na arquitetura SaaS, o usuário/cliente deverá focar, a equipe de TI da empresa, nas metas de negócios e nas formas de aplicação das mesmas, uma vez que, quase toda a infraestrutura de TI, tais como rede e *link* de dados para disponibilização da infraestrutura, *storage*, servidores, máquinas virtuais, SOs e banco de dados, ferramentas e *frameworks* de desenvolvimento, *softwares* e aplicativos estarão ao encargo do fornecedor do serviço de nuvem. Segue a representação da delegação de responsabilidades no PaaS:

Ilustração 05 – Delegação de responsabilidades no SaaS

Fonte: Página do Geraldo Loureiro no *Wiki* [5]

[5-] Disponível em:<http://www.geraldoloureiro.com/wiki/index.php?title=1o_Fórum_IBGP_de_Debates> Acesso em 15 de fevereiro de 2018.

3.6 Tipos de nuvens

Os tipos de nuvens estão relacionados à forma como os serviços ou recursos de nuvem encontram-se implantados. As literaturas pertinentes, em suma, apontam três formas básicas de implantação do serviço, as quais dão origem aos termos: nuvem privada, pública e híbrida. Há um quarto tipo de nuvem chamada de comunitária, entretanto não é tão popular ou abordada quanto às outras três formas convencionais.

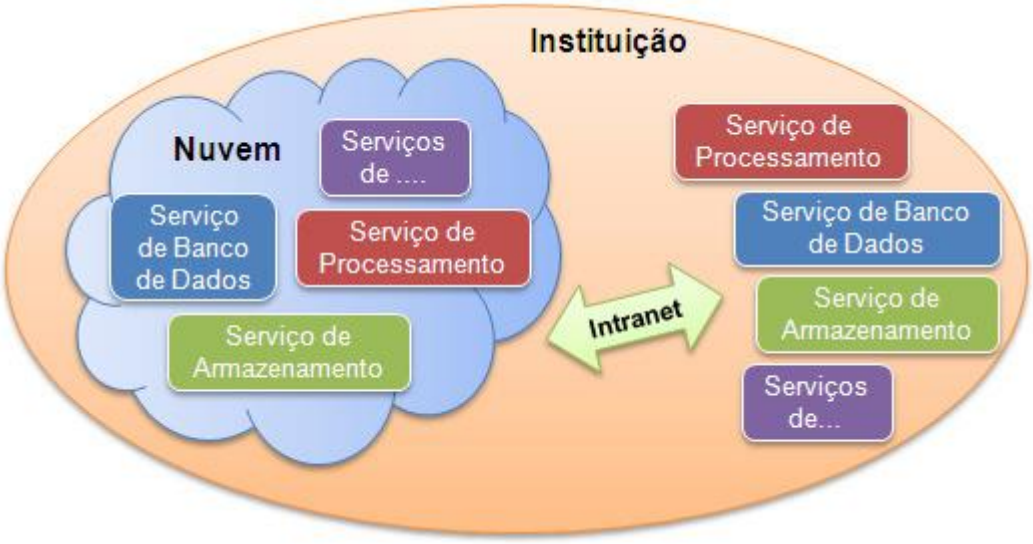
3.6.1 Nuvens privadas

As nuvens privadas correspondem a um grupo de nuvens em que cada qual possui seus recursos de TI dedicados exclusivamente a uma única empresa ou entidade. A nuvem privada pode estar localizada fisicamente em um DC interno da empresa ou por um DC dedicado à mesma.
Conforme Chirigat (2009):

> As nuvens privadas são aquelas construídas exclusivamente para um único usuário (uma empresa, por exemplo). Diferentemente de um *data center* privado virtual, a infraestrutura utilizada pertence ao usuário, e, portanto, ele possui total controle sobre como as aplicações são implementadas na nuvem. Uma nuvem privada é, em geral, construída sobre um *data center* privado.

Ainda, segundo Almeida (2014, p. 55) “É a infraestrutura operada apenas por uma organização, podendo ser gerenciada pela própria organização ou eventualmente por terceiros e pode tanto existir dentro como fora dos limites da organização”.
A grande vantagem deste tipo de implementação de nuvem é a segurança, uma vez que toda a infraestrutura está sob o controle de acesso físico da instituição e suas implementações de segurança são personalizadas conforme a política de segurança da empresa. A desvantagem é a expansão da estrutura que geralmente fica ao encargo da empresa, obrigando-a a efetuar investimentos robustos na aquisição de *hardware* e *software*. Segue representação da nuvem privada:

Ilustração 06 – Representação de nuvem privada



Fonte: BORGES et. Al., 2011, p. 11 [6]

3.6.2 Nuvens públicas

As nuvens públicas correspondem aos serviços de nuvem que são prestados por um provedor de serviços de nuvem, o qual mantém a infraestrutura e fornece os serviços para as empresas, através de DCs que disponibilizam recursos que são utilizados de forma compartilhada.

> A nuvem pública é fornecida por um prestador de serviços para o público geral usando como base a computação utilitária que tem o modelo de consumo *pay-per-use*. Os recursos da nuvem são geralmente hospedados nas instalações do prestador de serviços, mas estes *data centers* podem estar em qualquer lugar do mundo. Exemplo de nuvens públicas são *Amazon* (EC2), *Google gmail,* e *Azure da Microsoft* (MOHAN, 2011 apud GOLÇALVES, 2011, p. 27).

A vantagem deste tipo de nuvem é que as empresas possuem mais facilidade para realizar o redimensionamento de recursos, uma vez que as mesmas simplesmente alugam os serviços necessários enquanto há demanda e pagam por tempo de utilização sem a necessidade de adquirir *hardware* e licenciamento de *software*. Neste tipo de nuvem, os fornecedores são responsáveis pela manutenção de toda a infraestrutura. A desvantagem é a questão da segurança, a qual geralmente é implementada pelo fornecedor, não possibilitando às empresas uma implementação personalizada. Segue representação da nuvem pública:

[6-] BORGES, Hélder Pereira; MURY, Antonio Roberto; SCHULZE, Bruno; SOUZA, José Neuman de Souza. Computação em nuvem. Artigo científico, Brasil, 2011.

Ilustração 07 – Representação de nuvem pública

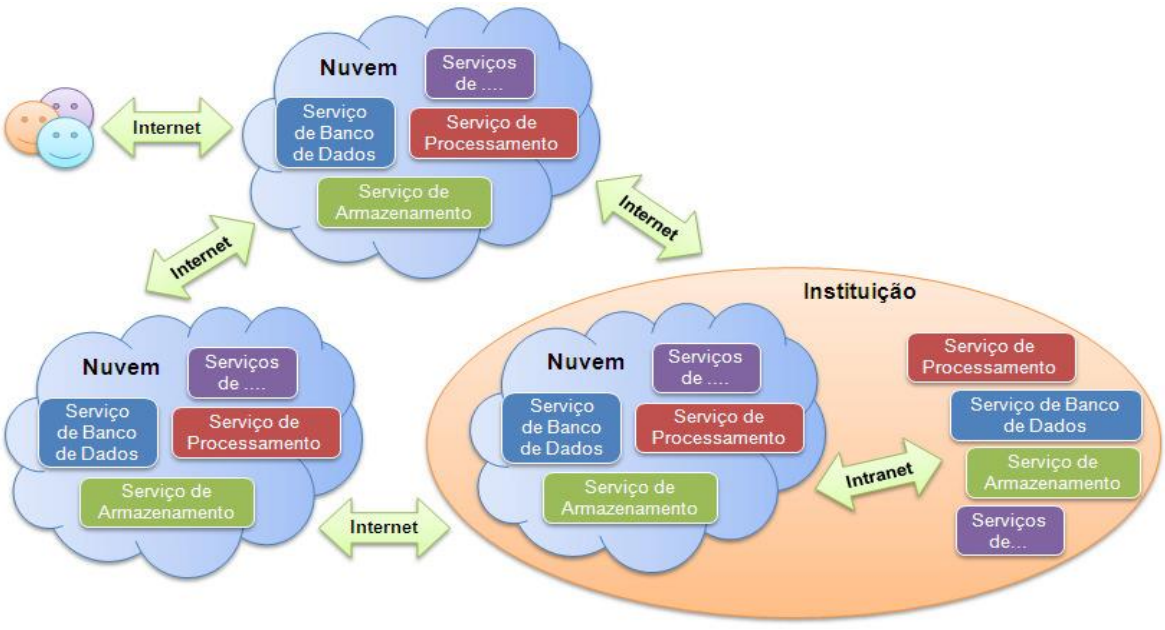
Fonte: BORGES et. Al., 2011, p. 12 [7]

3.6.3 Nuvens híbridas

As nuvens híbridas, como o próprio nome sugere, faz uma combinação de implantação entre nuvem privada e nuvem pública, o que proporciona maior flexibilidade para o usuário. Ressalta-se que este tipo de nuvem aumenta a complexidade de implementação, uma vez que torna necessário definir quais recursos e serviços serão disponibilizados pela nuvem pública e quais serão disponibilizados pela nuvem privada.

Para Mohan (2011 apud Gonçalves, 2011), A nuvem híbrida é constituída por duas ou mais nuvens (sendo que pelo menos uma possui arquitetura diferente das demais) que permanecem únicas e estão unidas por tecnologia padronizada que permite a portabilidade de dados e de aplicativos.

Ilustração 08 – Representação de nuvem híbrida



Fonte: BORGES et. Al., 2011, p. 13 [8]

[7 e 8-] BORGES, Hélder Pereira; MURY, Antonio Roberto; SCHULZE, Bruno; SOUZA, José Neuman de Souza. Computação em nuvem. Artigo científico, Brasil, 2011.

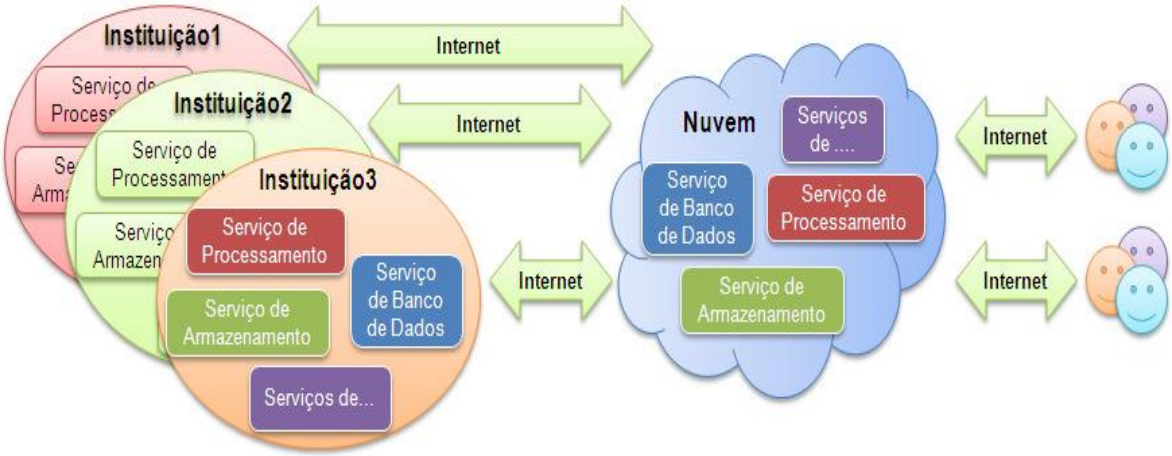
3.6.4 Nuvens comunitárias

A nuvem comunitária introduz o conceito de compartilhamento de dados, recursos e serviços de uma mesma nuvem por duas ou mais empresas ou entidades, as quais possuem atividades e finalidades em comum ou também compartilhadas.

> No modelo de implantação de nuvem comunidade ocorre o compartilhamento por diversas empresas de uma nuvem, sendo esta suportada por uma comunidade específica que partilha interesses, tais como a missão, os requisitos de segurança, política e considerações sobre flexibilidade. Este tipo de modelo de implantação pode existir localmente ou remotamente e geralmente é administrado por alguma empresa da comunidade ou por terceiros (SOUSA, 2011 apud NUBLING, 2011, p. 24).

Ainda, segundo Nist (2011 apud GOLÇALVES, 2011, p. 27). “A infraestrutura da nuvem é compartilhada por várias empresas e suporta uma determinada comunidade que visam o mesmo objetivo [...]. Pode ser gerenciada pela empresa ou por um terceiro e pode existir no local ou fora do local”.

Ilustração 09 – Representação de nuvem comunitária



Fonte: BORGES et. Al., 2011, p. 12 [9]

3.7 Grandes fornecedores de serviços de nuvem da atualidade

Há fornecedores que se destacam pela abrangência dos serviços disponibilizados, pela liderança do mercado e até mesmo pelo pioneirismo. Destacam-se as seguintes empresas:

[9] BORGES, Hélder Pereira; MURY, Antonio Roberto; SCHULZE, Bruno; SOUZA, José Neuman de Souza. Computação em nuvem. Artigo científico, Brasil, 2011.

3.7.1 Amazon

Em 2016 o *Amazon* iniciou a oferta de infraestrutura como serviço, através da plataforma *Amazon Web Services* (AWS) sendo uma das pioneiras na modalidade, e a parte central da sua plataforma de nuvem é o EC2, o qual corresponde a um serviço *web* que disponibiliza capacidade computacional redimensionável.

> A interface de serviço da *Web* simples do *Amazon* EC2 permite que você obtenha e configure a capacidade com mínimo atrito. Oferece um controle completo de seus recursos computacionais e permite que você trabalhe no ambiente computacional comprovado da *Amazon*. O *Amazon* EC2 reduz o tempo exigido para obter e inicializar novas instâncias do servidor em minutos, permitindo que você escalone rapidamente a capacidade para mais e para menos, à medida que os requisitos de computação são alterados. O *Amazon* EC2 muda a economia da computação ao permitir que você pague somente pela capacidade que realmente usa. O *Amazon* EC2 fornece aos desenvolvedores as ferramentas para criar aplicações resistentes a falhas e isolá-las de cenários comuns de falhas (AWS *AMAZON*, 2017).

O *Amazon* fornece diversos serviços de nuvem, tais como: computação escalável, armazenamento, serviços de hospedam, integração, multimídia, desenvolvimento de aplicações e jogos, banco de dados, análise de dados e migração, segurança e internet das coisas. Seguem exemplos de ferramentas/serviços:

- Para computação escalável – *Amazon EC2, Amazon Elastic Container Registry, Amazon Elastic Container Service, Amazon Lightsail, Amazon VPC, AWS Batch, AWS Elastic Beanstalk, AWS Lambda* e *Auto Scaling;*
- Para armazenamento – *Amazon S3, Amazon EBS, Amazon Elastic File System, Amazon Glacier, AWS Storage Gateway, AWS Snowball, AWS Snowball Edge* e *AWS Snowmobile;*
- Para banco de dados – *Amazon Aurora, Amazon RDS, Amazon DynamoDB, Amazon DynamoDB Accelerator, Amazon ElastiCache, Amazon Redshift* e *AWS Database Migration Service;*
- Para migração – *AWS Application Discovery Service, AWS Database Migration Service, AWS Migration Hub, AWS Server Migration Service, AWS Snowball, AWS Snowball Edge* e *AWS Snowmobile*;
- Para redes e entrega de conteúdos – *Amazon VPC, Amazon CloudFront, Amazon Route 53, AWS Direct Connect* e *Elastic Load Balancing*;

- Para desenvolvimento – *AWS CodeStar, AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy, AWS CodePipeline, AWS X-Ray* e Interface da linha de comando da *AWS*;
- Para gerenciamento – *Amazon CloudWatch, Amazon EC2 Systems Manager, AWS CloudFormation, AWS CloudTrail, AWS Config, AWS OpsWorks, AWS Service Catalog, AWS Trusted Advisor* e *AWS Personal Health Dashboard;*
- Para multimídia – *Amazon Elastic Transcoder, AWS Elemental MediaConvert, AWS Elemental MediaLive, AWS Elemental MediaPackage, AWS Elemental MediaStore, AWS Elemental* e *MediaTailor*;
- Para análise de dados – *Amazon Athena, Amazon EMR, Amazon CloudSearch, Amazon Elasticsearch Service, Amazon Kinesis, Amazon Redshift, Amazon Quicksight, AWS Data Pipeline* e *AWS Glue*;
- Para inteligência artificial – *Amazon Lex, Amazon Polly, Amazon Rekognition, Amazon Machine Learning, AMIs do AWS Deep Learning, Apache MXNet* na *AWS* e *TensorFlow* na *AWS*;
- Para aplicações – *Amazon Sumerian for AR and VR; AWS Step Functions* e *Amazon API Gateway*;
- Para sistemas de mensagens – *Amazon Simple Queue Service (SQS), Amazon Simple Notification Service (SNS), Amazon Pinpoint* e *Amazon Simple Email Service (SES);*
- Para streaming de desktop e aplicações – *Amazon Chime, Amazon WorkDocs, Amazon WorkMail;*
- Para produtividade empresarial – *Amazon WorkSpaces* e *Amazon AppStream 2.0*;
- Para central de atendimento baseada em nuvem – *Amazon Connect*;
- Para internet das coisas – Plataforma do *AWS Internet of Things (IoT), AWS Greengrass* e *AWS IoT Button*;
- Para desenvolvimento de jogos – *Amazon GameLift* e *Amazon Lumberyard*;
- Para segurança, identidade e conformidade – *Amazon Cloud Directory, AWS Identity & Access Management, Amazon Inspector, Amazon Macie, AWS Certificate Manager, AWS CloudHSM, AWS Directory Service, AWS Key Management Service, AWS Organizations, AWS Shield, AWS WAF, AWS Single Sign-On, Amazon GuardDuty* e *Amazon Cognito*;

3.7.2 Google

A *Google* oferta uma variedade de recursos e serviços em nuvem. Os mais conhecidos pelos usuários são *Gmail*, *Google Docs, Google Spreadsheets* e *Google Play*, entretanto há muitas outras soluções disponíveis, principalmente para ambientes corporativos. A *Google Cloud Platform* fornece serviços de computação, armazenamento e banco de dados, rede, ferramentas de gerenciamento, ferramentas de desenvolvedor e de segurança. Seguem exemplos de ferramentas/serviços:

- Para computação em nuvem – *Computer Engine, App Engine, Container Engine e Cloud Functions;*
- Para armazenamento e banco de dados – *Cloud Storage, Cloud SQL, Cloud Bigtable, Cloud Spanner* e *Cloud Datastore*;
- Para nuvem virtual privada – *Virtual Private Cloud (VPC), Cloud Load Balancing, CDN do Cloud, Cloud Interconnect* e *Domain Name System (DNS) do Cloud*;
- Para grande volume de dados – *BigQuery, Cloud Dataflow, Cloud Dataproc, Cloud Datalab, Cloud Dataprep, Cloud Pub/Sub, Genomics* e *Google Data Studio*;
- Para internet das coisas – *Cloud IoT Core*;
- Para aprendizado de máquina – *Cloud Machine Learning Engine, Cloud Jobs API, Cloud Natural Language API, Cloud Speech API, Cloud Translation API, Cloud Vision API* e *Cloud Video Intelligence API*;
- Para identidade e segurança – *Cloud IAM, Cloud Identity-Aware Proxy, Cloud Data Loss Prevention API, Cloud Key Management Service, Cloud Resource Manager* e *Cloud Security Scanner*;
- Para gerenciamento – *Cloud Deployment Manager, Cloud Endpoints, Cloud Console, Cloud Shell, Cloud Mobile App* e *Cloud Billing API;*
- Para desenvolvimento – *Cloud SDK, Container Registry, Container Builder, Cloud Source Repositories, Clout Tools para Android Studio, Cloud Tools para IntelliJ, Cloud Tools for PowerShell, Cloud Tools para Visual Studio, Cloud Tools para Eclipse* e *Cloud Test Lab*;

3.7.3 Microsoft

A *Microsoft* é outro dos grandes fornecedores de nuvem, embora não seja pioneira. Apresenta grande potencial de atrair os clientes para a nuvem, uma vez que detém a patente das soluções *off-line* que apresentam os maiores índices de utilização no mundo. Possui soluções diversificadas na nuvem, sendo uma das mais conhecidas o *Hotmail/Outlook*. Atualmente a *Microsoft* tem diversificado ainda mais seus recursos e dentre eles podem ser destacados algumas soluções. Seguem exemplos de ferramentas serviços:

- Para PaaS – *Windows Azure*;
- Para IaaS – *Windows Azure* Controlador
- Para SaaS – *SharePoint, Office 365, CRM Online, Bing* e outros.
- Para virtualização em nuvem – *Hyper-V*.

3.7.4 VMware

A *VMware Foundation* surgiu com a ferramenta de virtualização *VMware*, a qual provocou muitas mudanças nos ambientes empresariais de corporações em diversas localidades do mundo, com uma ferramenta de *software* que permitia reduzir significativamente os gastos com investimentos em infraestrutura de TI. Há algum tempo, a *VMware Foudation* lançou os conceitos de sua ferramenta principal na nuvem, o que gerou toda a sua plataforma de serviços de nuvem, oferecendo recursos como: DC e infraestrutura em nuvem, virtualização de funções de rede na nuvem, espaço de trabalho, virtualização de *desktops* e aplicativos, gerenciamento da mobilidade corporativa, virtualização de *desktop* pessoal e segurança. Seguem exemplos de ferramentas/serviços:

- Para infraestrutura em nuvem e DC – *vSphere with Operations Management, vSphere, vCenter Server, vCloud Director* e *vCloud Availability for vCloud Director;*
- Para armazenamento e disponibilidade – *vSAN e Site Recovery Manager*;
- Para rede e segurança – *NSX, AppDefense e vRealize Network Insight*;
- Para gerenciamento em nuvem – *vCloud Suite, vRealize Suite, vRealize Operations, vRealize Automation, vRealize Business for Cloud, Wavefront by*

VMware, are Integrated OpenStack, vRealize Log Insight, vRealize Code Stream, vRealize Orchestrator e *vRealize Hyperic*;

- Para virtualização e funções de rede – *vCloud NFV* e *VMware Integrated OpenStack Carrier Edition*;
- Para internet das coisas – *Pulse IoT Center*;
- Para virtualização de *desktops* e aplicativos – *Workspace One* e *Workspace One App Express*;
- Para espaço de trabalho digital – *Horizon 7, Horizon Apps* e *Horizon Cloud*;
- Para gerenciamento da mobilidade corporativa – *VMware AirWatch*;
- Para *desktop* pessoal – *Horizon Flex, Fusion, Workstation Pro* e *Workstation Player*;
- Para uso gratuito com finalidades diversificadas – *vShere Hypervisor, vCenter Converter* e *Software Manager*.

3.7.5 Salesforce

A *Salesforce* é uma das empresas líderes em SaaS e está aperfeiçoando a sua plataforma em nuvem também na disponibilização de PaaS. No geral, os serviços disponibilizados incluem ferramenta CRM, ferramentas de suporte aos usuários, ferramentas analíticas de negócios, repositório de aplicações, *framework* para desenvolvimento de aplicativos em nuvem e *IoT Cloud*. Seguem exemplos de ferramentas:

- Para vendas – *Sales Cloud* e *Salesforce CPQ*;
- Para atendimento – *Service Cloud* e *Desk*.com;
- Para *marketing – Marketing Cloud* e *Pardot*;
- Para desenvolvimento – *Salesforce Platform, Light* e *Heroku Enterprise*;
- Para comércio – *Commerce Cloud Digital* e *Commerce Cloud Order Management*;
- Para plataforma de colaboração – *Quip*;
- Para análise de dados – *Einstein Analytics, Sales Analytics* e *Service Analytics*;
- Para comunidades – *Community cloud* e *Chatter*;
- Para internet das Coisas – *IoT Cloud* e *Thunder*;

- Para Produtos por indústria - *Financial Services Cloud* e *Health Cloud*.

3.7.6 Citrix

A Citrix é uma empresa de norte americana *de software*, com foco em virtualização de aplicativos e *Virtual Desktop Infrastructure* (VDI), e atualmente está disponibilizando serviços de gerenciamento de mobilidade corporativa, armazenamento e sincronização de arquivos e de ferramentas de redes em nuvem. Seguem exemplos de ferramentas/serviços:

- Para virtualização de aplicativos e VDI – *XenApp, XenDesktop* e *XenServer*;
- Para gerenciamento de mobilidade corporativa – *XenMobile*;
- Para armazenamento e compartilhamento de arquivos – *ShareFile*;
- Para rede e segurança de rede – *NetScaler ADC, NetScaler AppFirewall, NetScaler Secure Web Gateway, NetScaler Unified Gateway, NetScaler Management & Analytics System* e *NetScaler SD-WAN*.

3.7.7 AT&T

A AT&T é uma empresa norte americana de telecomunicações e possui ponto forte no fornecimento de IaaS, como hospedagem e gerenciamento de serviços e atualmente também oferta PaaS, direcionada à profissionais. Já apresenta uma base sólida de clientes corporativos e possui centros de dados interligados em rede mundial. A empresa está tentando integrar seus serviços de nuvem aos serviços de telefonia móvel, através de aplicativo de armazenamento em nuvem para seus clientes que utilizam smartphone com SO *Android*.

3.7.8 Outros fornecedores de computação em nuvem

Há diversos outros fornecedores de computação em nuvem, mas ainda destaca-se a *Rackspace*, a Verizon e a Cisco.
A *Rackspace* está se dedicando ao contínuo desenvolvimento do *OpenStack*, desde 2010, o qual corresponde a um padrão aberto para construção de nuvens.

A *Verizon* é uma operadora de telefonia móvel que após a aquisição da *Terremark*, aprimorou seus serviços de IaaS e fornece serviços de segurança e gerenciamento de identidade e está em busca de alianças com empresas como a Cisco e IBM para expandir seu portfólio de serviços de computação em nuvem.

A Cisco, com a ferramenta *WebEx*, é um dos fornecedores SaaS mais representativos e sua estratégia é a plataforma que integra perfeitamente servidor e funções de rede utilizando-se do conceito de *Unified Computing System* (USC). A Cisco possui parcerias com a EMC, *VMware* e Intel com o propósito de desenvolver seus serviços de computação em nuvem.

4 CIBERCRIME E CIBERSEGURANÇA

A era da tecnologia da informação e comunicação (TIC) provocou alterações e difusão das relações sociais e culturais através da internet e suas redes de relacionamento, mas não obstante a isso, a evolução da TIC também alavancou o desenvolvimento global através da diversidade de tecnologias que foram inseridas nos ambientes empresariais, as quais proporcionaram às empresas uma enorme facilidade, agilidade e redução de custos na execução de atividades corporativas em diversos campos de atuação.

Como consequência da evolução das tecnologias e das formas de comunicação, a criminalidade se expandiu e alcançou o ambiente virtual, através dos cibercriminosos ou criminosos digitais, afetando tanto o usuário de perfil comum quanto grandes corporações, e como resposta imediata emergiu a cibersegurança que trata das questões relacionadas à segurança e permeia todo o ambiente virtual e os ativos que o integram: físicos (*hardwares*) e lógicos (*softwares*).

> A realidade das novas tecnologias trouxe ao mundo um novo universo de potencialidades de crime. E os criminosos não se fizeram rogados e o aparentemente inócuo mundo da Internet é hoje um campo de batalha onde se travam intensas batalhas (PEREIRA, 2013).

4.1 O cibercrime

O cibercrime corresponde à modalidade de crime que é iniciada, intermediada ou concretizada no ambiente virtual/digital, no qual o cibercriminoso se valendo de técnicas de computação ou persuasão, busca vantagem, geralmente técnica ou psicológica, sobre a sua vítima, com o intuito de obter alguma informação privilegiada ou acesso indevido no ambiente virtual ou real, que o leve a algum benefício próprio, seja financeiro, moral, físico e/ou psicológico, em detrimento do bem estar financeiro, moral, físico e/ou psicológico de sua vítima, dependendo da intensão do crime e da vítima (pessoa física ou entidade jurídica). Há casos em que o cibercriminoso aborda um ponto vulnerável, pessoa física, para obter informações que facilitem a execução do crime em um ambiente empresarial por exemplo.

Conforme Moreira (2017) cibercrime é o nome de crimes cibernéticos que envolvam atividade ou prática ilícita na rede. As práticas podem abranger invasões de

sistemas, disseminação de vírus, roubo de dados pessoais, falsidade ideológica, acesso a informações confidenciais e outros. O cibercrime compreende também crimes convencionais realizados por meio de dispositivos eletrônicos ou que incluam a utilização de alguma ação digital como instrumento para a prática do crime.

4.1.1 Os tipos de cibercriminosos

O cibercrime pode variar conforme a intensão do criminoso e também conforme o nível de conhecimento do mesmo. Pautando-se nessa mesma ideia de nível de conhecimento e intensão, surgiram várias classificações para os criminosos virtuais. Seguem as mais comuns: *hacker, cracker, phreakers, lammer, newbies (nub* ou *noob), carders* ou *carding, coders, virri* e/ou *wares, defacer* e *cyberpunks*.

4.1.1.1 Os hackers

No geral, os *hackers* possuem conhecimentos técnicos de nível avançado em computação e afins e buscam exercita-los e aprimora-los em diversos domínios da informática, sempre com o auto desafio de fazerem melhor e com mais perfeição. Os crimes cometidos não possuem a intenção final de lesar a vítima em si, mas de conseguirem efetuar algum procedimento de forma mais eficiente e eficaz do que o último realizado.

4.1.1.2 Os crackers

Os *crackers* por sua vez são proporcionais aos *hackers* em questão de conhecimento técnico, sendo peritos em romper sistemas de segurança, tais como: senhas de sistemas. Com relação à intensão em cometer crimes, são inversamente proporcionais aos *hackers*. Os *crackers* cometem os crimes objetivando o ato criminoso a todo instante, com o intuito de obter benefícios, que na maior parte das vezes são financeiros.

> O termo *cracker* é utilizado para pessoas que utilizam suas habilidades para a prática de quebra de um sistema de segurança. Ambos os termos são utilizados para definir pessoas que possuem habilidades com

> computadores, mas uma se difere da outra em termos de utilização de tais dotes (GOMES, 2014, p. 18).

4.1.1.3 Os phreakers

Os *phreakers* ou *phone freak* correspondem aos criminosos virtuais de sistemas de telefonia e são como os *crackers*, ou seja, possuem como finalidade o ato criminoso, entretanto se diferem no quesito campo de atuação. O objetivo específico dos *phreakers* está em utilizar de forma diversificada os recursos das linhas telefônicas de suas vítimas e sem restituí-las de forma alguma pelos serviços utilizados. Este grupo de criminosos possuiu maior notoriedade na década de 80, quando este tipo de crime alcançou o seu ápice de destaque na sociedade. Atualmente os *phreakers* correspondem aos criminosos que invadem celulares com o objetivo de clonar linhas, interceptar ligações comuns e provenientes de telefonia IP e diversas outras atividades ilegais relacionadas à comunicação fixa e móvel.

4.1.1.4 Os lammers

Os *lammers* correspondem a um grupo de criminosos virtuais que apresentam grande deficiência de conhecimento técnico quando comparado aos demais grupos. Desta forma, para se apoderarem de vantagens técnicas nos ambientes virtuais, estes criminosos se apropriam do conhecimento de especialistas, conhecimentos estes que se encontram disponíveis e acessíveis de alguma plataforma, site, mercado negro ou até mesmos cursos básicos de *hackers*, os quais não passam orientações éticas sobre a utilização das técnicas que ensinam. Uma vez que este grupo possui conhecimentos técnicos básicos, os transtornos que conseguem causar às suas vítimas possuem impactos mais moderados, com exceção de alguns casos bem específicos. Os *lammers* são conhecidos também como *script kids* devido ao nível de precariedade (“imaturidade”) que suas técnicas apresentam e principalmente pelo fato de que a maior parte das pessoas que constituem este grupo é composta por jovens entre 20 e 30 anos de idade. Cabe destacar que quase todo *cracker* começou como um *lammer*, desta forma, torna-se importante não subestimá-los.

Com relação ao *lammer*, segundo Dornbusch (2002, p. 10), “É o que se pode chamar de pseudo *hacker*, eles são os aspirantes a *hacker*, são motivo de piada e gozações. São pretensos *hackers* sem conhecimento técnico para superar as defesas das redes, estão tentando se tornar um *hacker*.

4.1.1.5 Os newbies

Os *newbies* correspondem a um grupo específico de *lammers*, ou seja, detém pouco ou quase nenhum conhecimento técnico de computação, mas se aventuram em atividades similares às fraudes ou roubos, por meio de trapaças em jogos digitais online. Por exemplo: conseguem itens de jogos de forma gratuita, os quais somente são comercializados. Realizando esta atividade através da instrução de outros *newbies* mais experientes ou através de pesquisas na internet sobre como burlar a segurança de determinado jogo.

4.1.1.6 Os carders ou carding

Os *carders* correspondem a um grupo de *cracks* que são especializados no roubo de informações de cartões de compras de todos os tipos, mas focam principalmente em cartões de crédito/débito. Logo após obterem as informações e credenciais para uso dos cartões, obviamente os utilizam para efetuar compras indiscriminadamente que em suma são efetuadas pela internet. Suas vítimas podem ser pessoas físicas ou jurídicas. Geralmente estes criminosos costumam focar seus ataques nas operadoras de cartões, entretanto podem atacar diretamente os usuários. Como defesa contra este tipo de ataque, as operadoras entram em contato com o cliente para confirmar a compra antes de liberar o pagamento e utilizam *secure socket layer* (SSL) para o envio de dados criptografados durante a comunicação do cartão/máquina com a operadora.

4.1.1.7 Os coders

Os *coders* correspondem a um grupo de *crackers* que possuem conhecimentos técnicos avançados em computação e que desenvolvem em uma, duas ou diversas linguagens de programação, as quais permitem escrever códigos maliciosos e

ferramentas de segurança e invasão, assim como examinar códigos fonte em busca de vulnerabilidades que lhes permitam planejar seus ataques direcionados.

4.1.1.8 Os virris e wares

Os *virri* e *wares* por sua vez, também representam um grupo de criminosos virtuais em que alguns possuem conhecimento de programação e realizam alterações em códigos fonte de programas de terceiros sem a devida autorização e em alguns casos desenvolvem ativadores de *softwares* proprietários e outras ferramentas similares com propósito de venda ou com o intuito de disseminação de códigos maliciosos inseridos de forma oculta em ativadores ou *softwares crackeados*. Geralmente disponibilizam repositórios de *software* piratas e *cracks*, através de sites clandestinos não seguros, ou ainda, por *links File Transfer Protocol* (FTP) provenientes de seus próprios computadores pessoais.

4.1.1.9 Os defacers

Os *defacers* correspondem a um conjunto de *cracks* também denominados pichadores de sites. Os criminosos virtuais deste grupo, ao realizarem um delito de invasão, buscam alterar a interface do *site* ou página da empresa ou entidade invadida como forma de apresentar o seu feito para os demais *crackers* e obter notoriedade e respeito na comunidade de criminosos virtuais. O ato da pichação pode representar também uma afronta direta à equipe de segurança que mantém o ambiente da instituição que sofreu o delito. A pichação digital pode vir acompanhada de outras consequências provenientes da invasão, pois geralmente quando este tipo de ataque ocorre, o criminoso dissemina códigos maliciosos dentro da rede invadida e pode roubar informações corporativas capturadas na rede da empresa.

4.1.1.10 Os cyberpunks

Os *cyberpunks* correspondem a grupo pessoas que utilizam ferramentas para ocultar seus rastros enquanto navegam no espaço virtual, ainda que seja um ato ilegal navegar por determinados ambientes virtuais, o que os configura como criminosos. Há *cyberpunks* que realizam invasões de *sites* e fazem pichações dos

mesmos, geralmente como uma crítica a ideologia da entidade a qual invadem. São considerados tecno-anarquistas com o ideal de manutenção da privacidade e disseminam programas de criptografia na tentativa de proteger pessoas contra a espionagem governamental e empresarial.

4.1.2 Tipos de ataques na internet

No ambiente virtual, o criminoso possui liberdade para rastrear e escolher alvos para tentativas de ataques. Geralmente buscam por vulnerabilidades em sistemas de segurança e assim que as detectam, as exploram para conseguirem efetivar um ataque com sucesso. Os ataques podem ter objetivos diversos: roubo ou sequestro de informações, roubo de contas bancárias de empresas e pessoas físicas, paralização de serviços de uma determinada empresa ou até mesmo vandalismo virtual por notoriedade e reconhecimento na comunidade *hacker*. A seguir será descrito alguns dos principais ataques cometidos pelos criminosos virtuais.

4.1.2.1 Negação de serviço

O ataque de *denial of service* (DoS), ou em português: negação de serviço, representa uma forma de ataque no qual o cibercriminoso tenta provocar a interrupção de um serviço ofertado no mundo real ou virtual, mas que é mantido no ambiente virtual. A parada da oferta do serviço é provocada ou por sobrecarga de solicitações a um determinado sistema/servidor ou por sobrecarga no tráfego da rede.

> Um método que os *hackers* usam para impedir ou negar a usuários legítimos o acesso a um computador. Os ataques de DoS são executados normalmente usando ferramentas de DoS que enviam muitos pacotes de pedidos a um servidor de destino da Internet (geralmente *Web*, FTP ou servidor de e-mail). O ataque inunda os recursos do servidor e torna o sistema inutilizável. Todo sistema conectado à Internet e equipado com os serviços de rede com base no TCP está sujeito ao ataque (*SYMANTEC*).

Há também o ataque *distributed denial of service (*DDoS*)*, no qual o ataque DoS ocorre de forma distribuída, por meio de um grupo de computadores ligados à internet, os quais são controlados por uma máquina mestre, a qual se encarrega de

passar os comandos para os computadores que estão na ponta, denominados “zumbis” ou “escravos”.

4.1.2.2 Ataques de força bruta

Os ataques de forma bruta ocorrem quando algum criminoso virtual tenta acessar um sistema, no qual é solicitada autenticação com senha. O criminoso executa manualmente ou através de *software* várias tentativas de *login*, por meio da tentativa e erro. Quando a tentativa é realizada através de *software*, são testadas todas as combinações possíveis de senha até que a mesma seja encontrada e o criminoso consiga acesso interno ao sistema, considerando que o *software* continue em execução e o serviço de *login* não fique indisponível durante as tentativas.
Segundo Cruz (2014, p. 40):

> Ataque de força bruta (*brute force*) consiste em forçar a quebra de uma senha de um determinado usuário de um sistema. É utilizado um dicionário de palavras mais comuns e suas combinações. Quando as combinações de uma senha são descobertas, o atacante consegue utilizá-las para acessar o sistema de modo legítimo.

4.1.2.3 Ataques por malwares

Os *malwares* são códigos de instrução maliciosos criados com a intensão de gerar prejuízos às suas vítimas. Os *malwares* geralmente se aderem aos sistemas e conseguem gerar danos ao computador ou dependendo do tipo espionam a máquina infectada, ou ainda, conseguem se espalhar pela rede e contaminar outras máquinas “saudáveis”. Geralmente os *malwares* conseguem acesso a um computador através da abertura de um *e-mail* desconhecido, ou de um *site* fraudulento e afins. Dentro da classificação de *malwares* podem ser encontrados, os vírus de computador, *worms*, cavalos de troia e *spywares*.

4.1.2.4 Ataques de defacement

O *defacement* corresponde ao ataque e invasão, alteração e pichação do conteúdo de *sites*. Conforme apresentado no item “Os tipos de cibercriminosos”, os indivíduos

que realizar este tipo de ataque geralmente deixam alguma espécie de identificação para que possam ser reconhecidos na comunidade *hacker*.

4.1.2.5 Ataques de e-mail spoofing

No ataque de *e-mail spoofing*, a conta de *e-mail* da vítima encontra-se comprometida, uma vez que serão encaminhados *e-mails* falsificados, através da alteração do cabeçalho, para os contatos presentes na lista de contatos da vítima, contendo códigos maliciosos ou *links* de páginas falsas para aplicação de golpes no ambiente virtual.

4.1.2.6 Ataques de escuta clandestina

O *sniffing* é um mecanismo de *software* que apresenta a função de interceptar dados que trafegam na rede e são utilizados com muita frequência com intuitos comerciais, buscando por preferências do usuário para compras e outros, mas a tecnologia do *sniffing* pode ser utilizada para o ataque de escuta clandestina, no qual um indivíduo não autorizado consegue acesso à rede e dissemina seus *sniffings* com o intuito de captar informações que lhes permitam praticar fraudes, espionagens ou outros. Os ataques possibilitam desde o furto de credenciais de acesso a sistemas, até senhas de cartões e outros similares.
Segundo Medeiros (2008, p. 35):

> Neste tipo de exploração também pode ocorrer o ataque de *eavesdropping*, do inglês, “escuta clandestina”, que ocorre através da interceptação do tráfego de uma rede. Esta situação particularmente prevalece quando as redes incluem conexões sem fio e dispositivos de acesso remoto. Assim, o atacante pode obter senhas, números de cartões de crédito e outras informações confidenciais que os usuários enviam pela rede.

4.1.2.7 Ataques de scan

O *scan* corresponde a um mecanismo de *software* que possibilita a varredura das redes e a identificação de *hosts* e serviços ativos. Embora este mecanismo seja muito utilizado pelos responsáveis pela rede e segurança com o ideal de encontrar vulnerabilidades, são também utilizados por cibercriminosos, os quais selecionam

potenciais alvos, associam vulnerabilidades aos serviços que conseguiram identificar e desta forma escolhem o melhor alvo possível para realizar a invasão.

4.1.3 As fraudes mais comuns

Os tipos de fraudes mais comuns que comumente ocorrem por meio do ambiente virtual são: fraude com uso de engenharia social, fraude de furto de identidade, fraude de antecipação de recurso, fraude de *phishing*, fraude de *pharming* e fraude de boato. A seguir seguem as respectivas descrições das fraudes.

4.1.3.1 A fraude com uso de engenharia social

A engenharia social corresponde a uma das principais técnicas utilizadas em fraudes que ocorrem no meio virtual, ou que tem início através dele e são concretizadas no mundo real. Por meio da engenharia social, o criminoso persuade sua vítima, através de intimidação ou sedução, a lhe conceder informações privilegiadas que podem lhe trazer algum benefício. Geralmente as outras fraudes do mundo virtual se iniciam através do uso de engenharia social.

4.1.3.2 A fraude de furto de identidade

Na fraude de furto de identidade o cibercriminoso assume a identidade de outra pessoa com o objetivo de se passar por ela, cometendo estelionato. Pode, por exemplo, criar um perfil falso, em uma rede social, com foto e todos os outros dados da vítima.
Segundo Hamed (2017, p. 31):

> Os objetivos são dos mais diversos. Geralmente o furto de identidade é utilizado em conjunto com a engenharia social para aplicação de fraudes financeiras, extorsão e roubo de informações privilegiadas que geralmente ocorrem por meio do ambiente virtual, sendo que outros crimes acabam transcendendo as barreiras do ambiente virtual, tais como: sequestro, estupro, pedofilia e até mesmo assassinato.

4.1.3.3 A fraude de antecipação de recurso

A fraude de antecipação de recurso corresponde a um conjunto de fraudes nas quais o cibercriminoso ludibria suas vítimas, por meio de páginas *web*, *e-mail*, mensagens instantâneas e outros, a conceder-lhes dinheiro ou informações confidenciais com a promessa de retorno de algum benefício fantasioso em um breve período de tempo.

4.1.3.4 A fraude de phishing

A fraude de *phishing* ocorre quando os criminosos virtuais utilizam mensagens instantâneas, *e-mails*, bate papo e outros para divulgar promoções enganosas, as quais podem ser acessadas por um *link* em anexo à mensagem, o qual redireciona os usuários para uma página falsa que irá coletar dados de compras, caso os usuários tentem preencher qualquer formulário que nela exista.

4.1.3.5 A fraude de pharming

A fraude de *pharming* corresponde a um tipo bem específico de *phishing*, no qual o usuário acessa o site legítimo e é direcionado para sites falsos.

> *Pharming* é uma prática fraudulenta semelhante ao *phishing*, com a diferença que, no *pharming*, o tráfego de um site legítimo é manipulado para direcionar usuários para sites falsos, que vão instalar *softwares* maliciosos nos computadores dos visitantes ou coletar dados pessoais, tais como senhas ou informações financeiras. Este tipo de ataque é particularmente traiçoeiro porque, se um servidor de DNS for comprometido, mesmo os usuários com aparelhos protegidos e livres de *malwares* podem se tornar vítimas (AVAST).

4.1.3.6 A fraude de Boato

A fraude de boato se desenvolve por meio de *e-mails* e redes sociais, com mensagens de teor sensacionalista. Geralmente os usuários se sentem estimulados a abrir a mensagem e ao fazerem isso, logo em seguida algum *software* ou código malicioso invade o dispositivo de acesso para torna-lo vulnerável a invasões posteriores, nas quais os criminosos efetuam o ato do crime.

4.2 A cibersegurança

A cibersegurança corresponde à área do conhecimento que almeja a proteção de pessoas, corporações, *hardwares*, *softwares*, dados, informações e outros ativos que estejam em contato contínuo ou permanente, ou ainda, que possam estar expostos de alguma maneira no ambiente virtual, em outras palavras, a cibersegurança é uma ciência que busca prever, neutralizar e tratar a ocorrência ou reincidência de cibercrimes.

Quando a cibersegurança é focada na proteção de dados e informações corporativas, ela é arquitetada de forma a garantir os três pilares da segurança da informação: disponibilidade, integridade e confidencialidade; e utiliza-se dos serviços de controle de acesso, autenticidade, não repúdio e auditoria para assegurar que os pilares da segurança não estão sendo violados.

4.2.1 Pilares da segurança da informação

Os pilares da segurança da informação buscam garantir a qualidade da informação, uma vez que a mesma está disponível sempre que necessária, está íntegra, ou seja, completa e sem alterações não autorizadas pela sua fonte/proprietário e confidencial, o que significa que o valor dela se conserva, pois não foi utilizada por terceiros, dado que somente as entidades com permissões possuem acesso a ela. Desta forma, a informação pode ser utilizada para a geração de conhecimento e em diversas outras atividades que agreguem valores ou vantagens para as empresas.

Ilustração 10 – Triângulo da segurança da informação

Fonte: ABREU, 2011, p. 13 [10]

[10-] ABREU, Leandro Farias dos Santos. A Segurança da Informação nas Redes Sociais. Monografia, Brasil, 2011.

4.2.1.1 Disponibilidade

A disponibilidade de uma informação está associada à condição da mesma de se encontrar sempre disponível para acesso ou edição, por pessoas ou programas com as devidas autorizações, conforme definição da política de segurança. A disponibilidade vai além da informação, chegando também aos sistemas, dado que, uma vez que um sistema apresente falhas/paradas em seu serviço, as informações por ele apresentadas ficarão indisponíveis, ou seja, quando se trata questões de disponibilidade, tanto as informações, quanto sistemas devem ser tratados.
A disponibilidade da informação é, conforme Freitas (2009, p. 22), “propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada”.

4.2.1.2 Integridade

A integridade está associada à condição dos dados e informações estarem protegidos contra exibição parcial, alteração ou mesmo exclusão por entidades que não possuam autorização para executar tais ações.
Conforme Hamed (2017), a integridade consiste na proteção dos dados e informações contra modificações sem a autorização formal do proprietário dos mesmos. A segurança da integridade inclui proteção contra a escrita, ou seja, alterações de status, conteúdo, remoção e atrasos durante a sua transmissão ou retransmissão. Destaca-se que quando a informação não possui garantia de que está atualizada, a integridade não se mantem.
Ainda, segundo Abreu (2011, p. 13):

> A integridade dos dados refere-se à certeza de que os dados não são adulterados, destruídos ou corrompidos. É a certeza de que os dados não serão modificados por pessoas não autorizadas. Existem basicamente dois pontos durante o processo de transmissão no qual a integridade pode ser comprometida: durante o carregamento de dados e/ou durante o armazenamento ou coleta do banco de dados.

4.2.1.3 Confidencialidade

A confidencialidade de uma informação está associada à condição da mesma de estar segura contra acessos não autorizados, ou seja, somente entidades com as

devidas permissões podem tomar posse ou copiar os dados e informações em sua totalidade ou parcialidade.

A confidencialidade, para Abreu (2011, p. 13):

> A confidencialidade dos dados significa que estes estão disponíveis apenas para as partes apropriadas, que podem ser partes que requerem acesso a dados ou partes que são confiáveis. Os dados que têm sido mantidos confidenciais são aqueles que não foram comprometidos por outras partes; dados confidenciais não são divulgados a pessoas que não necessitam ou que não deveriam ter acesso a eles.

4.2.2 Serviços de segurança

Os serviços de segurança da informação trabalham como ferramentas de apoio aos pilares da segurança, em suma, são responsáveis por garantir que a disponibilidade, integridade e confidencialidade estão sendo mantidas.

4.2.2.1 Controle de acesso

No controle de acesso o serviço é responsável por permitir ou negar que alguma entidade solicitante tenha acesso a um dado, informação ou sistema. Para isso, o controle realiza a comparação entre as credenciais do solicitante e as entidades pertencentes ao grupo com autorização para acesso. Cabe destacar que o controle de acesso não faz somente a verificação se o solicitante está na lista de autorizados, mas utiliza o serviço de autenticidade para comprovar que o solicitante é realmente quem diz ser, antes de permitir o acesso.

4.2.2.2 Autenticidade

Na autenticidade o serviço é encarregado de identificar a origem de uma solicitação/mensagem, com o intuito de comprovar que o remetente real é exatamente o mesmo indivíduo cujas credenciais foram informadas no início de um processo de autenticação, em outras palavras, o serviço de autenticidade é responsável por comprovar a genuinidade de uma identificação apresentada a um sistema ou serviço, como o controle de acesso por exemplo. Desta forma, para Silva

S. S. (2014), autenticidade reflete à certeza que uma ação refletida sobre uma informação foi exposta ao conhecimento e há registros do fato, ou seja, autenticidade se dá quando o usuário almeja manipular uma informação e antes de realizá-la, é anunciado e sobre isso há um registro.

Com o serviço de controle de acesso trabalhando em conjunto com o serviço de autenticidade, a segurança é ainda mais reforçada com o intuito de garantir que somente indivíduos com autorização tenham acesso às informações, contribuindo com os pilares da segurança, uma vez que a disponibilidade, a integridade e confidencialidade não serão comprometidas por um acesso indevido.

4.2.2.3 Irretratabilidade

A irretratabilidade é um serviço que assegura que um indivíduo/entidade que tenha realizado uma comunicação, como o envio de mensagem ou solicitação, não tenha como negar que realizou tal ação. A irretratabilidade utiliza-se muito dos *logs* de sistemas de controle de acesso e autenticidade, para comprovar as ações efetuadas por determinadas entidades, comprovações estas utilizadas em auditorias e na investigação de crimes virtuais.

Segundo Abreu (2011, p. 14), “A irretratabilidade pode ser vista como a combinação da autenticidade com a integridade da informação [...]”.

4.2.2.4 Auditoria

A auditoria é um serviço de grande importância, pois permite realizar a análise detalhada de várias atividades com o intuito de se identificar regras e procedimentos que não estão sendo seguidos e quem não está seguindo e com o auxílio da irretratabilidade o infrator não possui meios de negar a sua ação.

O serviço de auditoria permite a análise detalhada de atividades mapeadas em um sistema informatizado, possibilitando identificar o que foi feito e afetado, quando, quem executou a ação entre outras. O serviço de irretratabilidade auxilia a auditoria no sentido de que os erros e ações maliciosas executadas por pessoas e sistemas autorizados, não poderá ser negada pela entidade.

4.2.3 Política de segurança da informação

A política de segurança da informação de uma corporação é responsável pela definição, planejamento, implementação, manutenção, revisão, atualização, auditoria e governança de um conjunto de documentos, regras, métodos, processos, serviços, pessoas, treinamentos e ferramentas de segurança virtual, os quais são agrupados de forma arquitetônica para compor o corpo da segurança da informação. A política para ser aplicada e mantida, utiliza-se de um conjunto de ferramentas de cibersegurança.

Segundo Hamed (2017), na política de segurança da informação há muitas questões que devem ser tratadas, tais como: política de *backup* dos dados, restrição de acesso ao DC ou salas de centrais de comunicação, testes contínuos de vulnerabilidades nos ativos de rede, política de atualização de vacinas do antivírus e da solução *antispam*, assim como troca periódica das senhas de acesso aos recursos da rede, treinamento de funcionários para combate às técnicas de engenharia social e revisão da política de segurança da informação a cada seis ou doze meses.

4.2.4 As ferramentas de cibersegurança

Na tentativa de prover segurança no ambiente virtual, a cibersegurança conta com o apoio de um conjunto de ferramentas, sem as quais não seria possível bloquear as ações dos cibercriminosos, tais como: treinamentos de pessoas, sistemas de gestão de segurança da informação (SGSI)s e softwares de segurança.

4.2.4.1 Treinamento de pessoas

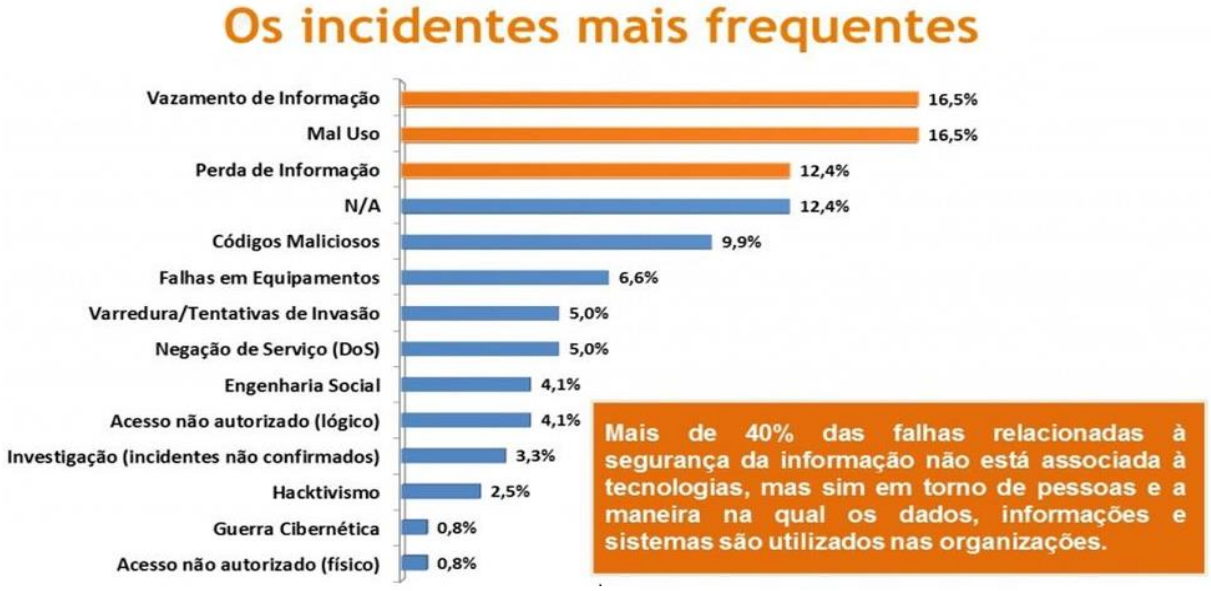
Quando se trata da proteção de ambientes virtuais corporativos ou mesmo da segurança da corporação como um todo, o ponto mais vulnerável para a ação de criminosos e cibercriminosos são as pessoas, as quais geralmente desconhecem o valor das informações corporativas e da privacidade das empresas e acabam deixando vazar informações privilegiadas, geralmente induzidas por terceiros, informações estas que na mão de criminosos podem representar um grave risco

para as empresas. As pessoas vinculadas às atividades da organização, e que possuem acesso às informações privilegiadas, são também chamadas de *insiders*. Segundo o *Gartner Group* (s/a, s/p apud *PROOF, 2017, s/p)*:

> 70% dos incidentes de segurança que realmente causam prejuízos financeiros para as empresas, envolvem *insiders*. No caso da *Yahoo!*, que perdeu milhões de dólares em negociações devido à um vazamento de dados, tudo começou com um *e-mail phishing*, um dos golpes que usa táticas de engenharia social para atingir seus objetivos.

Com a inserção das tecnologias IoT nas empresas, motivada pela agilidade e eficiência que as mesmas proporcionam aos negócios, também ampliaram a superfície de ataque, aumentando, consequentemente, o êxito dos ataques cibernéticos, principalmente utilizando os *insiders* como ponto vulnerável. Desta forma, é de extrema importância que as corporações realizem companhas de conscientização e capacitação com treinamentos frequentes, com seus funcionários e *insiders* diversos, sobre segurança da informação corporativa e políticas de segurança da empresa voltada para colaboradores, explicando as práticas de engenharia social, os tipos de ataques mais comuns utilizados enquanto se navega na internet e as formas gerais de prevenção de ataques, dado que a maioria dos incidentes de segurança estão relacionados aos *insiders*.

Gráfico 01 – Os incidentes mais frequentes



Fonte: Página do *Exin* no *Slideshare* [11]

[11-] Disponível em: <https://pt.slideshare.net/Exin/exin-daryus-apresentacao-pesquisa> Acesso em 17 de fevereiro de 2018.

4.2.4.2 Sistema de gestão de segurança da informação

O SGSI corresponde a um sistema de gestão corporativo direcionado a segurança da informação, o qual apresenta toda a abordagem da corporação, a qual é utilizada para proteger os aspectos de confidencialidade, integridade e disponibilidade das informações.

Segundo GSW (2011):

> A implantação do SGSI envolve primeiramente a análise de riscos na infraestrutura de TI para identificar os pontos vulneráveis e as falhas nos sistemas que deverão ser corrigidos. Em seguida, são definidos processos para detectar e responder aos incidentes de segurança e procedimentos para auditoria.

Segundo Palma (2016), “O SGSI inclui estratégias, planos, políticas, medidas, controles, e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação”.

Ainda segundo Palma (2016), “A norma ISO 27001 adota o modelo *Plan-Do-Check-Act* (PDCA) para descrever a estrutura de um SGSI”.

A implementação do SGSI segue alguns passos: definição da política de segurança da informação, definição do escopo do SGSI, executar avaliação do SGSI, gerenciamento de riscos, seleção de controles a serem implementados e preparação da declaração de aplicabilidade. Destaca-se que uma vez implementado, é necessário monitorar o SGSI constantemente, aprimorá-lo/atualizá-lo conforme as mudanças organizacionais ou alterações da política de segurança da corporação e realizar novas avaliações de risco.

Quadro 01 – Implementação e manutenção de um SGSI

Fonte: ADÃES, 2010 [12]

[12-] Disponível em: <https://tecnoativa.wordpress.com/category/seguranca-da-informacao/> Acesso em 19 de fevereiro de 2018.

4.2.4.3 Softwares de segurança para o ambiente virtual

Os *softwares*, para a proteção de um ambiente virtual, formam uma enorme gama de recursos virtuais que almejam a proteção de toda a estrutura lógica do ambiente virtual da corporação, com o intuito de tratar as vulnerabilidades e reduzir os riscos de invasão/contaminação da rede e suas inúmeras consequências.

4.2.4.3.1 Firewall

O *firewall* é implementado tanto em servidores, quanto em computadores e roteadores. O *firewall* dos roteadores geralmente são implementados via *hardware*, enquanto dos servidores e computadores via *software*. De forma geral, o *firewall* gerencia o controle do fluxo de solicitações que saem da rede/nuvem da empresa, assim como filtra todas as solicitações externas de acesso aos serviços do ambiente virtual da empresa, deixando passar somente as comunicações/requisições que estejam autorizadas/permitidas. A tabela de regras do *firewall* é configurada/personalizada conforme a necessidade e a política de cada empresa e implementada pela equipe responsável pela segurança da rede da corporação.
Segundo Jesus (2016, p.17):

> A política de segurança implementada por um *firewall* é composta exatamente por essas regras, as quais definem que tipo de tráfego é permitido ou não na rede, atuando como uma porta que se abre ou fecha para determinados fluxos de dados de acordo com as características específicas de cada um. Sempre que um fluxo chega ou parte da rede, o *firewall* verifica as características deste fluxo, comparando-as sequencialmente com várias regras até encontrar uma regra na qual todas as características definidas por ela correspondem às características do fluxo em questão. Encontrada tal regra, é aplicada ao fluxo a ação definida por essa regra.

4.2.4.3.2 Proxy

O *proxy* corresponde a um *software* que realiza o filtro de conteúdo. Ele limita o acesso dos usuários aos conteúdos que estão disponíveis fora da rede/nuvem da empresa. O *proxy* também é configurado pelos responsáveis pela segurança da rede e em conformidade com a política de segurança da empresa. Uma vez que o conteúdo ao qual o usuário poderá acessar está limitado, reduz também a chance

de que o mesmo acesse conteúdo indevido de forma premeditada ou não intencional e desta forma o computador da empresa não será submetido ao aceso de páginas que são consideradas um risco para a segurança da rede, conforme especificado na política de segurança.

4.2.4.3.3 Sistemas de detecção de intrusão

Sistemas de detecção de intrusão podem apresentar três formas de arquiteturas diferentes:

- Arquitetura de *host*, recebendo o nome *Host-based intrusion detection system* (HIDS) – não realizam o monitoramento do que passa pela rede, mas verificam as informações de eventos e *logs* relacionados ao *host* no qual se encontra instalado, alertando sobre tentativas de acesso não autorizado à máquina e bloqueando novas tentativas de acesso não autorizado;
- Arquitetura de rede, recebendo o nome *Network-based intrusion detection system* (NIDS) – monitora o tráfego e os pacotes que passam pela rede e são instalados em diversas máquinas específicas que monitoram atividades de rede, na tentativa de identificar atividades maliciosas baseadas em serviços, portas e outros. O NIDS não busca somente identificar tentativas de acesso não autorizados, mas também se algum acesso legítimo está executando alguma atividade que não deveria;
- Arquitetura híbrida, recebendo o nome *Hybrid-base intrusion detection system* – nesta arquitetura o sistema possui função completa, trabalhando diretamente nos *hosts* e em toda a rede.

Segundo Júnior (2016, p. 4): “Sistemas de detecção de intrusão são projetados para reconhecerem tentativas de intrusão, bloquearem ataques e produzirem alertas que podem ser analisados posteriormente”.

4.2.4.3.4 Scanners de vulnerabilidades

Os *scanners* de vulnerabilidades analisam a fundo toda a estrutura dos pacotes que recebem como resposta da sua atividade de enviar pedidos para portas variadas. Com a análise, identificam portas ativas e abertas, assim como as aplicações que

estão associadas a cada porta ativa e fazem recomendações para correção de problemas identificados.

Conforme Buzzatte (2014, p. 27), ”Os *Scanners* de vulnerabilidade têm como objetivo procurar por falhas em serviços, aplicativos, sistemas operacionais que representam um risco à segurança de uma rede quando utilizado por pessoas não autorizadas”.

Segundo Ulbrich (2004, apud BUZZATTE, 2014, p. 28):

> Através de uma lista de falhas conhecidas, o *scanner* de vulnerabilidade verifica se o sistema está ou não executando um serviço com problemas. O *scanner* é capaz de detectar erros comuns de configuração, configuração e senhas-padrão como, por exemplo, *softwares* com configuração de fábrica, combinações obvias de usuários e senha e vulnerabilidades divulgadas.

4.2.4.3.5 Antivírus

O *software* antivírus é uma ferramenta sofisticada na detecção, eliminação e prevenção de *malwares* de diferentes tipos. Seus fabricantes possuem equipes especializadas em segurança virtual e laboratórios sofisticados para criação e testes de vacinas para combate às pragas virtuais mais recentes que surgem no mercado. As novas vacinas são disponibilizadas na forma de *patches* de atualização para a ferramenta antivírus do fornecedor. É de vital importância para a segurança da rede de uma corporação, que a mesma mantenha a sua ferramenta antivírus sempre atualizada.

4.2.4.3.6 Antispam

O *antispam* corresponde a um *software* que efetua o bloqueio de mensagens com teor indesejado, tais como: promoções e propaganda de produtos diversos, e que apresentam riscos à segurança, tais como: mensagens *phishing* ou mesmo mensagens com códigos maliciosos inseridos em arquivos anexos ou no corpo da própria mensagem.

O *antispam* apresenta um conjunto de filtros que devem ser configurados/calibrados de acordo com a política de segurança da empresa e demanda do usuário, sempre mantendo a comodidade de ambos. Geralmente o próprio usuário possui acesso ao

filtro de *spam*, quando não é o caso, o administrador da rede efetua as configurações do filtro, os quais podem apresentar bloqueios por assuntos, remetentes, palavras estrangeiras, tamanhos de anexo e outros.
Segundo Hamed, (2017, p.36)

> Geralmente as ferramentas *antispam* possuem filtros de bloqueio para assunto, texto no corpo do *e-mail*, remetente, domínio, IP, *links* e apresenta o recurso de lista branca, pois sempre há exceções de mensagens desejadas no meio de mensagens catalogadas como indesejadas.

4.2.4.3.7 Backup

O *software* de *backup* corresponde a uma ferramenta que realiza cópias de segurança de arquivos, de forma gerenciável, personalizada e atualizada, sendo que as diferentes versões dos mesmos arquivos são mantidas por determinado período de tempo, conforme definido na política de segurança da empresa. A ferramenta de *backup* geralmente possibilita guardar cópias dos dados, diretamente em discos rígidos comuns, *storages*, fitas, fitas virtuais, disco ópticos e dispositivos de armazenamento em memória *flash*, ou seja, em locais lógicos e físicos diferentes do ambiente de produção dos dados. Em caso de perda das informações que estão nos servidores da empresa, seja proveniente de ato criminoso, falha humana ou catástrofe natural, os dados armazenados pelo *backup* podem ser restaurados diretamente em nova base de dados, possibilitando que a empresa retome os serviços de TIC e disponibilize novamente as informações corporativas em ambiente de produção, desde que sua infraestrutura não esteja comprometida.

4.2.4.3.8 Criptografia

Os *softwares* de criptografia tem a função de cifrar as mensagens que vão trafegar por um meio não seguro. Caso a mensagem seja interceptada no tráfego entre a origem e o destino, o interceptador não conseguirá visualizar as informações contidas na mensagem de forma inteligível, para isso ele deverá desencriptar a mensagem e somente com a chave de desencriptação ele poderá realizar o feito, a qual fica em posse somente do destinatário. A mensagem é encriptada na origem e desencriptada no destino, geralmente sem nenhuma ação por parte do usuário, ou

seja, toda a atividade da criptografia fica por conta da aplicação. A criptografia auxilia na manutenção da confidencialidade da informação, de forma que entidades não autorizadas não conseguem acesso à informação presente no conteúdo da mensagem.

5 SEGURANÇA NA COMPUTAÇÃO EM NUVEM

A computação em nuvem está em fase de desenvolvimento contínuo e expansão de serviços de forma constante, e a cada dia que se passa, mais aumenta a diversidade de produtos ofertados nos *sites* dos grandes provedores de nuvem, produtos estes que passam a agregar novos recursos e a abranger uma área ainda maior de atuação em demandas de negócios de empresas de todos os ramos e portes. Considerando toda a praticidade, agilidade, dinamismo e economia proporcionadas pela computação em nuvem, os gestores estão se sentindo cada vez mais seduzidos pela possibilidade de migrar a infraestrutura e sistemas de suas empresas para o novo ambiente, entretanto, ainda que exista resistência na adoção da nuvem por diversas corporações, há outras que migram sem que a gestão possua conhecimentos dos aspectos envolvendo a segurança dos dados corporativos na nuvem, muita das vezes motivada por deficiência técnica da equipe de TI responsável pela assessoria.
Segundo Castro e Sousa V. L. P (2010, p. 3):

> Computação em Nuvem, tais como, *e-mails*, desenvolvimento de aplicativos personalizados, armazenamento de dados e gestão de infraestrutura, podemos considerar que esses são concentrações maciças de recursos e dados. A percepção de que a nuvem é um aglomerado de informações pode caracterizá-la como sendo um alvo propício a ataques por potenciais invasores. Ameaças como esta podem afetar diretamente os pilares da segurança da informação: disponibilidade, confidencialidade e integridade, e consequentemente comprometer toda a nuvem.

Quando se trata da segurança de dados e informações corporativas é essencial que a proteção seja implementada de forma a tentar garantir o valor da informação ainda em seu ciclo de vida, por meio da manutenção das propriedades de segurança da informação: disponibilidade, integridade e confidencialidade.

5.1 A política de segurança da informação e o uso do SGSI

A segurança da informação, assim como qualquer outra área de conhecimento, necessita ser trabalhada de forma organizada e estratégica, ou seja, requer a definição de uma política bem estruturada e geralmente implementada sobre um

SGSI, que permitirá maiores facilidades na atividade de monitoramento, controle e atualização da mesma.

De acordo com a norma ABNT NBR ISO/IEC 27002:2005 (2005):

> "A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio".

No geral, a política de segurança da informação estará pautada em conformidade com os objetivos estratégicos da corporação e com o auxílio do SGSI e de seu método PDCA, buscará adequação e melhoria contínua da segurança, através das reclassificações das informações, serviços, sistemas e aplicativos ao longo de seus respectivos ciclos de vida, principalmente no contexto da computação em nuvem, onde serão realizadas continuamente análises de riscos para balanceamento de risco/benefício e decisão da gestão em migração/permanência de ativos na nuvem, ambiente na qual as ameaças não podem ser controladas, apenas vulnerabilidades tratadas e riscos mitigados.

5.2 Risco x ameaça x vulnerabilidade

A análise do relacionamento entre riscos, ameaças e vulnerabilidades é de extrema importância para a implementação da segurança da informação, pois possibilita a gestão realizar a análise do risco/benefício de disponibilizar determinadas informações, serviços, sistemas e aplicativos em quaisquer ambientes, incluindo o ambiente da computação em nuvem.

No geral, a gestão analisa o valor de uma determinada informação, serviço e sistema e o grau de segurança ao qual estariam submetidos no ambiente da nuvem e através deste balanceamento, decide por adotar/manter ou não a nuvem ou serviço agregado a ela.

5.2.1 Conceito de risco

O risco, na segurança da informação, representa a probabilidade de um agente ou evento explorar intencionalmente ou não premeditadamente a vulnerabilidade de uma entidade, seja pessoa, serviço ou empresa, e provocar um dano ao mesmo, ou seja, corresponde ao grau de possibilidade de ocorrência de uma ameaça se concretizar e provocar danos a uma entidade por meio de algum ponto vulnerável que esta possua.

5.2.2 Conceito de vulnerabilidade

A vulnerabilidade corresponde a um ponto de deficiência, fraqueza, brecha de segurança ou suscetibilidade, por meio do qual uma entidade é colocada em um status de risco podendo ser acometida alguma ameaça. Esta entidade pode ser pessoas, processos, sistemas, empresas e outros.

A vulnerabilidade significa para Oliveira (2016), “Falha ou fraqueza de procedimento, *design*, implementação, ou controles internos de um sistema que possa ser acidentalmente ou propositalmente explorada, resultando em uma brecha de segurança ou violação da política de segurança do sistema”.

Ainda segundo Oliveira (2016), na segurança da informação, uma vulnerabilidade corresponde a uma fraqueza que permite que o atacante reduza a garantia da informação do sistema. Vulnerabilidade é a interseção da suscetibilidade do sistema, acesso à falha e a capacidade do atacante em explorar a falha.

5.2.3 Conceito de ameaça

A ameaça corresponde a um ato que potencialmente causa danos a um recurso, seja desabilitando-o, removendo-o ou até mesmo destruindo-o. As ameaças são oportunistas e buscam aproveitar as vulnerabilidades de segurança de um sistema para ataca-lo e provocar danos a ele ou a rede da empresa e aos ativos nela presentes, no qual o sistema vulnerável se encontra. Oliveira (2016) ainda define a ameaça como: “Possibilidade de um agente (ou fonte de ameaça) explorar acidentalmente ou propositalmente uma vulnerabilidade especifica”.

5.2.4 Tratando riscos

A existência de ameaças, vulnerabilidades e exposição de ativos valorosos aumentam os riscos, sendo que as vulnerabilidades expõem os ativos, entretanto, uma vez que os riscos são identificados, os mesmos indicam os requisitos de proteção que devem ser tratados almejando alcançar a salvaguarda das informações, serviços, sistemas e aplicativos, uma vez que a salvaguarda é realizada, aumenta-se a proteção contras as ameaças e consequentemente se reduz os riscos. Segue a ilustração do relacionamento entre riscos, ameaças e vulnerabilidades:

Ilustração 11 – Relação entre risco, ameaça e vulnerabilidade

Fonte: GRUPOFATEC2013, 2013 [13]

5.3 Gerenciamento de riscos e a segurança da informação na nuvem

Os benefícios da computação em nuvem são diversos e já foram mencionados no item 3 da pesquisa, assim como o quantitativo de ameaças existentes no ambiente

[13]- Disponível em: <https://cgerumblog.wordpress.com/> Acesso em 28 de fevereiro de 2018.

virtual também o são, entretanto quando este ambiente se encontra na nuvem, principalmente na pública, várias questões de segurança não são tratadas pela corporação em si, mas pelos fornecedores de nuvem e é neste caso que atua de forma mais consistente o gerenciamento dos riscos, ou seja, a gestão da empresa contratante do serviço de nuvem, por meio da sua política de segurança da informação, se valem da gerência de riscos para decidir quais aplicações, serviços e informações podem ser submetidos ao grau de risco oferecido por determinados fornecedores.

Há um conjunto de questionamentos que devem ser feitos aos fornecedores com o intuito de se chegar à aferição dos riscos:

- Quais são as ações em caso de falha?
- Quanto tempo levará para o reestabelecer o serviço?
- O *backup* é realizado com redundância?
- Qual o *Service Level Agreement* (SLA) dos serviços?
- Quem terá acesso aos dados e informações da organização?
- Qual a política de controle e privacidade dos dados?
- Como é feito o isolamento dos dados em um DC compartilhado?
- Os dados serão transferidos para fora do país?
- Em caso positivo, para qual país?
- Quanto tempo os dados estarão nessa localidade?

Conforme Castro e Sousa V. L. P (2010, p. 1):

> A problemática é como adotar modelos de segurança em um paradigma totalmente novo para as práticas do mercado. 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. A solução mais adequada está vinculada à definição de padrões de governança de TI, que permitam as organizações identificar e catalogar as informações que serão armazenadas na nuvem. A adequação das políticas de segurança da informação auxiliará a definição de diretrizes para que o consumo dos serviços da nuvem possua um nível de segurança aceitável.

A segurança na nuvem é implementada através do mapeamento e gerenciamento dos riscos identificados, os quais são mensurados através da identificação das ameaças e da detecção de pontos de vulnerabilidades em todos os ativos da empresa, sejam pessoas, processos ou ferramentas.

Uma vez que as ameaças presentes no ambiente de nuvem não podem ser controladas, o gerenciamento dos riscos é realizado através do tratamento dos pontos de vulnerabilidades, onde busca-se reduzir ou eliminar a vulnerabilidade com o intuito de reduzir o risco de forma a torna-lo aceitável dentro dos padrões especificados na política de segurança.

5.3.1 Tratando pontos vulneráveis: pessoas

A implementação de segurança em qualquer tipo de nuvem ou arquitetura de serviço de nuvem, objetivando a proteção de informações corporativas, começa através da definição da política de segurança a ser aplicada aos *insiders* em geral. De nada vale a inserção de ferramentas de software para a proteção do ambiente virtual, a adoção de metodologias de desenvolvimento de aplicativos para nuvem e de um conjunto de outras boas práticas de segurança, se o maior ponto de vulnerabilidade da segurança da informação não for tratado: as pessoas. Embora a segurança da informação não seja uma ciência exata e com uma definição única, há um aspecto em que todas as literaturas apresentam concordância: o maior foco de vulnerabilidades presente na questão da segurança da informação corresponde aos *insiders*.

Segundo Silva, D. R. P e Stein (2007, p. 47): “O problema da segurança da informação tem sempre duas faces, que são representadas pelas características inerentes de dois mundos diferentes e por vezes conflitantes: o mundo da tecnologia e o mundo dos seres humanos”.

A forma de se tentar tratar as vulnerabilidades de segurança presentes no fator humano é através do investimento em campanhas de conscientização e treinamentos dos colaboradores.

5.3.1.1 Campanhas de conscientização

As campanhas de conscientização devem ser frequentes e precisam apresentar e esclarecer dúvidas sobre as técnicas de engenharia social, utilizadas por cibercriminosos, desde contatos telefônicos até o envio de *e-mails* maliciosos, além de apresentar algumas práticas que não podem ser adotadas dentro do ambiente corporativo, tais como: compartilhamento de credencias de acesso aos sistemas da

corporação e utilização dos recursos corporativos para fins particulares. É importante frisar que a utilização dos recursos e serviços de TI deve estar em conformidade com a política de segurança adotada na empresa.

5.3.1.2 Treinamento de capacitação

Treinamento de capacitação para utilização dos recursos e serviços de TI da empresa de forma segura, com o intuito de prevenir a utilização dos recursos de forma equivocada, as quais poderiam comprometer a segurança da rede interna da empresa. Por exemplo: configuração de *spam* no cliente de *e-mail*. Algum usuário poderia alterar o filtro de forma equivocada e acabar recebendo *e-mails* contendo códigos maliciosos que podem contaminar a rede e comprometer a segurança da mesma, caso o usuário abra o *e-mail* fraudulento ou tente executar algum anexo que contenha o código.

5.3.2 Tratando pontos vulneráveis: processos e ferramentas de software

Os processos correspondem ao grupo de diversos documentos e atividades que estão definidos na política de segurança da informação, tais como: política de *backup*, descarte de mídias de dados, configurações de sistemas internos, análise do ciclo de vida das informações armazenadas, política de atualização de vacinas de antivírus, atualizações das definições de *spam*, permissões de grupos de usuários/permissão de acesso, testes de vulnerabilidades, atualização da gestão de riscos, contratos de fornecimento dos diversos serviços de nuvem, SLAs dos serviços dentre muitas outras.

As ferramentas de *software* correspondem aos programas, aplicativos e sistemas presentes no ambiente virtual, tais como: *software* antivírus, *software* de *backup*, *firewall*, *proxy* e outros.

A forma de se tentar tratar as vulnerabilidades de segurança presentes nos processos e ferramentas de *software* é através da utilização de ferramentas de inspeção e monitoramento dos parques virtuais e da realização de auditorias.

5.3.2.1 Ferramentas de inspeção e monitoramento

As ferramentas de inspeção e monitoramento executam a análise dos *logs* de registro de praticamente todas as atividades executadas no ambiente virtual, desde o horário de acesso de um determinado usuário a um determinado *site*, até o horário de execução de um *job* de *backup*, possibilitando checar também o comportamento das atividades de um sistema ou aplicação. Cabe destacar que as ferramentas de inspeção e monitoramento, assim como a abrangência de sua utilização devem estar especificadas na política de segurança da informação da corporação.

5.3.2.2 Auditorias para tratamento de processos e ferramentas de software

As auditorias são realizas por meio do auxílio das ferramentas de inspeção e monitoramento, permitindo analisar se todas as diretrizes de segurança da informação, definidas e documentadas na política segurança da corporação e geridas pelo SGSI, estão sendo seguidas por colaboradores, sistemas e ferramentas diversas que compõem o ambiente de TI da organização. Quando há a identificação de atividades que estejam ferindo as diretrizes de segurança, os infratores são notificados, assim como os responsáveis pela segurança da informação também o são, os quais tomam providencias para que as atividades inconformes sejam tratadas de forma a se evitar as suas reincidências e com esta medida, consequentemente corrigem vulnerabilidades de segurança da informação no ambiente.

5.4 Implementando a segurança nos diferentes tipos de nuvens

A implementação da segurança da informação em nuvem possui muitos aspectos comuns com a implementação da segurança da informação de qualquer ambiente.

> Os controles de segurança na nuvem não diferem dos controles de segurança de qualquer ambiente de TI. No entanto, a computação em nuvem envolve uma lenta perda de controle uma vez que os quesitos de segurança podem ficar a cargo do provedor. À medida que a organização vai amadurecendo, o sistema de segurança também é ajustado (CSA, 2010 apud FREITAS, R. R.; GOMES N. A.; PENHA, 2016, p. 19).

As abordagens para implementação de segurança da informação irão variar conforme o tipo de nuvem e a arquitetura de serviço almejada, pelo fato de que as segregações das responsabilidades pelo controle da infraestrutura, plataformas de desenvolvimento e dos serviços de *software* são diferentes, conforme apresentados no capítulo 4 desta pesquisa.

Conforme Castro e Sousa V. L. P (2016), as ameaças podem afetar diretamente os pilares da segurança da informação: disponibilidade, confidencialidade e integridade, e desta forma comprometer toda a nuvem. A garantia de cumprimento dos princípios da segurança da informação relaciona-se com o tipo e a arquitetura da nuvem aderida pela empresa.

Segue quadro apresentando o risco de implantação de cada tipo de nuvem:

Quadro 02 – Tipo de nuvem x descrição x risco

Tipo de Implantação	Descrição	Provável Risco
 Nuvem Pública	Com a nuvem pública, os serviços são entregues aos clientes por meio de uma rede aberta para uso público.	Dificuldade para avaliar, implementar e gerenciar os controles de acesso.
 Nuvem Privada	A nuvem privada oferece mais segurança e controle porque os serviços são mantidos em uma rede privada protegida por firewall.	Os controles de acesso são mais fáceis de serem gerenciados e controlados.
 Nuvem Híbrida	Na nuvem híbrida temos uma composição dos modelos de nuvens públicas e privadas, oferecendo maior diversidade.	Os riscos relacionados a gestão do controle de acesso varia de acordo com o escopo de tecnologia aplicado.

Fonte: FARIAS, 2017 [14]

Conforme mencionado anteriormente, a implementação da segurança da nuvem começa pela definição de quais informações, e recursos serão disponibilizados na nuvem.

A equipe de TI mapeia as informações, serviços, sistemas e aplicativos e identifica as ameaças existentes, através de uma simulação hipotética ou mesmo real, por meio de provas de conceito, assim como analisa e estuda formas de minimizar as vulnerabilidades, com o intuito de se reduzir os riscos. Após gerar a tabela de riscos por meio da classificação aferição dos riscos associados a cada tipo de informação, recursos e serviços, a mesma é apresentada a alta gestão da empresa, a qual decide sobre o conteúdo que irá subir para a nuvem, decisão e ação que devem ser documentadas e registradas na política de segurança da empresa.

14- Disponível em: <http://www.farmaceuticas.com.br/cloud-computing-computacao-em-nuvem-o-novo-desafio-para-a-validacao-de-sistemas-computadorizados/> Acesso em 27 de fevereiro de 2018

5.4.1 Segurança na nuvem privada

A nuvem privada de uma empresa pode ser implementada tanto por uma equipe de terceiros quanto por uma equipe de TI própria. No geral, a nuvem privada corresponde ao formato de nuvem que apresenta o maior nível de segurança entre todos os outros tipos, pois possibilita um nível de controle personalizado, uma vez que sua estrutura e manutenção como um todo geralmente fica dentro da própria empresa ou em um ambiente totalmente controlado por ela.
O principal mecanismo de segurança adotado para este tipo de nuvem é a política de acesso, a qual pode ser realizada por meio dos provedores de serviços, recursos de gerenciamento de redes e ferramentas diversas de controle de acesso e autenticação.

5.4.1.1 Segurança na nuvem privada com arquitetura IaaS

Na arquitetura IaaS, a empresa responde pela manutenção e expansão da sua nuvem e desta forma, torna-se responsável por toda a implementação da segurança da informação na mesma. A implementação de segurança nos serviços IaaS na nuvem privada é realizada através da definição de aspectos, tais como:

- campanhas de conscientização e treinamento dos colaboradores na utilização consciente dos recursos de tecnologia da informação da corporação e na preservação de dados e informações de caráter corporativo e confidenciais contra vazamentos voluntários ou criminosos, motivados por práticas de engenharia social ou por algum tipo de fraude ao qual o usuário tenha sido acometido por cibercriminosos;
- monitoramento constante do tráfego de rede, do comportamento dos sistemas e das requisições de usuários;
- testes de vulnerabilidades, para garantir que as aplicações e servidores existentes na rede/nuvem não apresentem portas ativas desprotegidas, as quais podem ser usadas como alvo de ataques. Os testes de vulnerabilidades contribuem com todos os três aspectos dos pilares da segurança da informação;
- utilização de *firewall* e *proxy*, para garantir um controle rigoroso sobre as solicitações que entram na rede/nuvem e sobre as solicitações que saem da

rede/nuvem da empresa, contribuindo para a manutenção da confidencialidade, integridade e disponibilidade das informações, uma vez que reduzem os riscos do usuário acessar uma página indevida e comprometer toda a nuvem da organização;

- política de *backup* de dados e informações de negócios, de fiscalização e de configurações de sistemas contendo redundância para endereço físico diferente do DC, visando garantir a disponibilidade das informações;
- planos de contingência em caso de indisponibilidade do DC;
- descarte de mídias de dados com o uso de ferramentas específicas e em ambiente isolado e efetuado somente por pessoas devidamente capacitadas e designadas para tal fim, visando garantir a confidencialidade das informações;
- configurações de sistemas internos com as proteções de portas e com política de atualização bem definida, visando garantir a confidencialidade, disponibilidade e integridade dos dados e informações;
- análise periódica do ciclo de vida das informações armazenadas, possibilitando a reclassificação dos dados e informações, assim como as definições de criticidade e seu destino de armazenamento e *backup*, visando a confidencialidade das informações;
- política de atualização de vacinas de antivírus, para proteção contra códigos maliciosos de tipos diversos, visando a integridade, confidencialidade e disponibilidade das informações, uma vez que os códigos maliciosos não serão executados diretamente no *host*;
- atualizações das definições de *spam*, para proteção das caixas de *e-mail* dos usuários de um determinado ambiente, reduzindo desta forma o risco dos usuários caírem em alguma fraude ou sofrerem algum ataque e consequentemente auxiliando a disponibilidade, integridade e confidencialidade das informações;
- definições de grupos de usuários/permissão e controle de acesso com uso de autenticação, para tentar garantir a confidencialidade. Na criação de grupos de usuários delegam-se permissões sobre o acesso/alteração de dados e informações, o que coopera para a manutenção da confidencialidade, integridade e disponibilidade dos mesmos;

- redundância do *link* de dados do(s) DC(s), para garantir a disponibilidade dos sistemas e informações presentes no(s) mesmo(s). Caso um dos *links* tenha queda, o outro *link* assume com o intuito de manter a disponibilidade dos serviços;
- sistemas críticos implementados em *cluster* de alto desempenho, alta disponibilidade e balanceamento de carga, para garantir o bom funcionamento dos sistemas em caso de sobrecarga de processamento ou falhas de *hardware*, mantendo a disponibilidade das informações e serviços;
- manutenções e atualizações dos *hardwares*, *softwares* e sistemas físicos diversos de segurança dos DCs, com o intuito de evitar falhas provenientes das defasagens dos mesmos, buscando manter a disponibilidade de informações e serviços.
- realização de auditorias para identificar se as diretrizes de segurança da informação estão sendo seguidas por colaboradores, serviços e sistemas;
- atualização e revisão constante da política de segurança da empresa, preferencialmente através de um SGSI, apoiado pela gestão de riscos.

5.4.1.2 Segurança na nuvem privada com arquitetura PaaS

Na arquitetura PaaS, a empresa responde pela manutenção e continuidade de todo o ambiente de desenvolvimento disponibilizado, assim como a disponibilidade das ferramentas e *frameworks* de desenvolvimento. A implementação de segurança nos serviços PaaS na nuvem privada é realizada através de:

- implementação de toda a segurança da arquitetura IaaS, uma vez que, na nuvem privada, a PaaS será suportada pela IaaS da empresa;
- montagem de máquinas robustas com grandes capacidades de memórias, processadores, discos e SOs atualizados e protegidos por *software* antivírus, para suporte das ferramentas e *frameworks* de desenvolvimento, para garantir a disponibilidade, integridade e confidencialidade das informações que podem ser comprometidas em caso de invasões por ataques em pontos de vulnerabilidades presentes no ambiente de desenvolvimento;
- se possível for, recomenda-se implementar o ambiente de desenvolvimento em *clusters* de alto desempenho e alta disponibilidade;

- atualizações frequentes de todas as ferramentas e *frameworks* de desenvolvimento, os quais geralmente são padrões de mercado, cujas atualizações são disponibilizadas pelos fabricantes. Cabe destacar que, geralmente esta medida aumenta também a segurança das aplicações desenvolvidas;
- controle de acesso ao ambiente de desenvolvimento com uso de autenticação, objetivando que somente os desenvolvedores tenham acesso às ferramentas de desenvolvimento e consequentemente reforçando a confidencialidade e a integridade do ambiente e das informações nele presentes.

5.4.1.3 Segurança na nuvem privada com arquitetura SaaS

Na arquitetura SaaS, a empresa responde pela manutenção e continuidade das aplicações disponibilizadas. A implementação de segurança na SaaS na nuvem privada é realizada através de:

- implementação de toda a segurança da arquitetura IaaS, uma vez que, na nuvem privada, a SaaS será suportada pela IaaS da empresa, assim como a PaaS também é suportada;
- implementação de toda a segurança da arquitetura PaaS da empresa, caso a mesma seja responsável pelo desenvolvimento das aplicações disponibilizadas na SaaS da corporação (geralmente quando uma empresa possui ferramentas de desenvolvimento, ela desenvolve a maioria das aplicações que utiliza);
- montagem de servidores robustos com grande capacidade computacional, memória e SOs atualizados e protegidos por *software* antivírus, para suporte das aplicações, visando garantir a disponibilidade, integridade e confidencialidade das informações;
- disponibilização das aplicações por meio de *clusters* (dependendo da criticidade das aplicações), visando garantir a disponibilidade e integridade das aplicações e informações;
- testes de vulnerabilidades frequentes, efetuados sobre as aplicações disponibilizadas;

- implementação de controle de acesso e uso das aplicações por meio da autenticação de usuários, com possibilidade de restrição de acesso a determinados recursos da aplicação com o intuito de manter a disponibilidade dos serviços e informações somente para entidades autorizadas;
- implementação de controle de acesso por *hosts* via IP ou endereço *Media Access Control* (MAC) aos serviços SaaS, protegendo os *hosts* com *software* antivírus e/ou módulos de segurança, na tentativa de guardar os dados que são inseridos nas interfaces locais para acesso ao ambiente e aplicações da nuvem;
- proteger a comunicação da origem ao destino, via criptografia, na utilização do SaaS, quando o dispositivo estiver tentando acessar os serviços de fora da rede da empresa, caso esta prática seja autorizada pela política de segurança.

5.4.2 Segurança na nuvem pública

Na nuvem pública a empresa não detém a infraestrutura, ou seja, a infraestrutura é mantida fora dela, através de DCs de terceiros, os quais disponibilizam os serviços de TI através da internet. Neste tipo de nuvem, toda a estrutura de *hardware* é mantida pelo fornecedor do serviço e dependendo da arquitetura da nuvem, os próprios ambientes de desenvolvimento e aplicações também são disponibilizados e mantidos pelo fornecedor. Em ambos os casos a segurança oferecida pelos fornecedores de nuvem é um padrão de mercado.

Segue relação da arquitetura/modelo de serviço de nuvem com as características dos riscos:

Quadro 03 – Arquitetura de nuvem x descrição x risco [15]

Modelo de Serviço	Características do Risco	Risco Relativo
Infrastructure as a Service (IaaS)	Neste modelo de serviço o consumidor não administra ou controla a infraestrutura da nuvem subjacente, mas tem controle sobre os sistemas operacionais, armazenamento de aplicativos implantados, e os componentes de rede selecionados.	Médio
Platform as a Service (PaaS)	Neste modelo de serviço o consumidor não administra ou controla os recursos de infraestrutura da nuvem subjacente, tais como componente de rede, servidores, sistemas operacionais, ou armazenamento. Porém o consumidor tem controle sobre os aplicativos utilizados na hospedagem de aplicativos e nas configurações de ambientes.	Alto
Software as a Service (SaaS)	Neste modelo de serviço o consumidor não administra ou controla a infraestrutura subjacente da nuvem. O que inclui componentes de rede, servidores, sistemas operacionais, armazenamento ou capacidade de aplicação individual. A possível exceção relaciona-se a algumas configurações específicas do usuário e de algumas configuração de aplicativos.	Muito Alto

Fonte: CASTRO, SOUSA V. L. P., 2010, p. 5 [15]

5.4.2.1 Segurança na nuvem pública com arquitetura IaaS

Na arquitetura IaaS da nuvem pública, o fornecedor dos serviços de computação em nuvem é responsável por implementar todos os aspectos de segurança da informação que tangem a infraestrutura a ser disponibilizada para as corporações, cabendo às mesmas somente a escolha de seus fornecedores, assim como a implementação de segurança nos sistemas, aplicativos e em alguns casos, nos componentes de rede. No geral, para a implementação da segurança na IaaS da nuvem pública, é necessário:

[15-] Castro, Rita de C. C. de; SOUSA, Verônica L. Pimentel de. Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança. Artigo Científico, Brasil, 2010.

- realizar campanhas de conscientização e treinamento dos colaboradores na utilização consciente dos recursos de tecnologia da informação da corporação e na preservação de dados e informações de caráter corporativo e confidenciais contra vazamentos voluntários ou criminosos, motivados por práticas de engenharia social ou por algum tipo de fraude ao qual o usuário tenha sido acometido por cibercriminosos, assim como na nuvem privada;
- elaboração cuidadosa do termo de referência (especificação) da infraestrutura necessária para abrigar os serviços de TI que são almejados para atender as demandas de negócios da organização. Desta forma, busca-se evitar que a disponibilidade dos serviços seja comprometida devido à insuficiência de recursos computacionais.
- pesquisar por fornecedores que permitam a realização da prova de conceito, na qual o provedor disponibiliza o serviço de infraestrutura na nuvem de forma gratuita, por tempo predeterminado, para testes por parte dos usuários, possibilitando uma melhor percepção da qualidade dos serviços e suportes ofertados, evitando a contratação equivocada de serviços que não atendam a demanda de negócios da corporação ou mesmo que colocam em risco a integridade, disponibilidade e/ou confidencialidade das informações submetidas ao ambiente da nuvem;
- pesquisar por fornecedores de serviços de nuvem que possuam parcerias com grandes empresas desenvolvedoras de tecnologias de segurança da informação, tais como: *Kaspersky*, *Trend Micro*, *MCAfee* e outras, o que é um indicativo de que o fornecedor segue um padrão de segurança mais robusto, complexo e qualitativo, o que consequentemente torna a proteção difícil de ser violada por entidades que buscam acesso às informações mantidas na nuvem.
- analisar cuidadosamente o catálogo das ofertas de serviços de IaaS dos fornecedores de nuvem, comparando as configurações de processadores, memórias, tecnologias de *storage* e *backup* de dados, redundância de *backup*, planos de contingência em casos de falhas, ferramentas de gerenciamento de virtualização e a console de acesso aos serviços da nuvem, buscando a melhor qualidade de recursos possíveis, com o intuito de garantir a disponibilidade dos serviços e informações;

- pesquisar na internet se existem processos judiciais contra os fornecedores pretendidos, por questões de quebra de sigilo, comprometimento, roubo ou sequestro de informações corporativas armazenadas em suas nuvens, na tentativa de identificar quais fornecedores apresentam segurança questionável na proteção de dados de terceiros;
- resguarde da corporação no âmbito contratual, através de especificação dos serviços contratados, de SLAs referentes à disponibilidade e suporte dos mesmos e de termos de guarda e sigilo das informações armazenadas na nuvem, estando as especificações, SLAs e termos declarados na política de segurança da informação;
- implementar/configurar *softwares* de segurança da informação, tais como: antivírus, *firewall*, *proxy*, *antispam* e outros, quando for o caso, na rede, servidores e VDIs contratados, de acordo com o perfil do usuário;
- optar por fornecedores que utilizem recursos de criptografia na comunicação entre os *hosts* e os serviços, quando for tecnicamente viável, considerando os tipos de serviços disponibilizados nesta arquitetura;
- implementar a segurança dos *hosts* que iram acessar o ambiente de nuvem, através de software antivírus, módulos de segurança ou outros, dependendo do tipo de serviço;
- implementar controles diversos de acesso ao ambiente da nuvem, até mesmo por cadastro de *hosts*, por meio de recursos de rede ou outros, se viável com autenticação, de forma a tentar assegurar a confidencialidade e integridade dos dados e informações presentes no ambiente da nuvem;
- utilizar *links* de dados redundantes na corporação para tentar manter a disponibilidade de acesso aos serviços IaaS da nuvem pública, por parte da contratante.

5.4.2.2 Segurança na nuvem pública com arquitetura PaaS

Na arquitetura PaaS da nuvem pública, diferentemente da nuvem privada, não há como garantir questões de segurança na arquitetura IaaS do fornecedor, com o intuito de se ter garantias de que ela irá suportar o PaaS que o mesmo oferece.

Entretanto, há outras maneiras da empresa tentar garantir a segurança das informações nesta arquitetura, as quais seguem:

- deve-se realizar campanhas de conscientização e treinamento dos colaboradores na utilização consciente dos recursos de TI da corporação e na preservação de dados e informações de caráter corporativo e confidenciais contra vazamentos voluntários ou criminosos. Cabe destacar que as arquiteturas PaaS e SaaS pode ser contratadas isoladamente do IaaS na nuvem pública, desta forma, as campanhas de conscientização e treinamentos dos colaboradores necessitam ser considerados como medidas de implementação de segurança em cada arquitetura de nuvem;
- deve-se pesquisar se há processos judiciais contra os fornecedores vislumbrados na prestação de qualquer tipo de serviço de nuvem, com o intuito de se identificar se os mesmo possuem algum indicativo ruim quanto à garantia da segurança da informação;
- deve-se comparar os produtos ofertados por diferentes fornecedores;
- deve-se optar por fornecedores que permitam realizar a prova de conceito das ferramentas de desenvolvimento, assim como de todo o ambiente disponibilizado;
- deve-se procurar por fornecedores que possuam parcerias com os grandes fabricantes de ferramentas de desenvolvimento, o que representa um bom indicativo de segurança, uma vez que as ferramentas estarão sempre atualizadas e com correção constante de erros/falhas de segurança, os quais podem comprometer todo o ambiente de desenvolvimento, assim como as informações que passam por ele;
- deve-se assegurar os SLAs de disponibilidade das ferramentas de desenvolvimento contratualmente, assim como a especificação técnica do ambiente e seus recursos e a guarda e confidencialidade dos códigos e outras informações que tramitam por esta arquitetura de nuvem;
- deve-se optar por ambientes de desenvolvimento que possuam controle de acesso por usuário e com autenticação, e possibilidade de restrição a determinados recursos da plataforma, conforme o perfil do usuário, visando garantir a disponibilidade, confidencialidade e integridade das informações,

uma vez que serão acessadas e/ou modificadas somente por entidades autorizadas;

- deve-se optar por ambientes que permitam a restrição de acesso por *host* via IP/MAC e com autenticação, de forma a tentar assegurar que o ambiente somente seja acessado por *hosts* cadastrados, os quais podem ser monitorados, controlados e protegidos por *software* antivírus, com o intuito de se proteger as informações que são inseridas nas interfaces locais para acesso ao ambiente de nuvem, assim como evitar a contaminação da nuvem por ameaças que podem se instalar nos *hosts*;
- deve-se utilizar criptografia ponta a ponta e em alguns casos, módulo de segurança, com o intuito de se proteger toda a comunicação entre o *host* e o serviço da nuvem, principalmente se o *host* estiver sendo utilizado de fora da rede corporativa, a qual geralmente possui mecanismos próprios para a proteção dos mesmos;
- utilizar *links* de dados redundantes na corporação para tentar manter a disponibilidade de acesso aos serviços PaaS da nuvem pública, por parte da contratante.

5.4.2.3 Segurança na nuvem pública com arquitetura SaaS

Na arquitetura SaaS da nuvem pública é onde se encontra o maior grau de incerteza quanto a segurança dos dados, essa consideração se faz em comparação com todas as arquiteturas de nuvem. Na SaaS os dados serão submetidos aos aplicativos disponibilizados nos serviços e um dos únicos controles disponíveis para os usuários, estão restritos a alguns ajustes básicos de personalização da aplicação para o seu próprio perfil, entretanto há outras considerações que quando acatadas complementam a implementação de segurança, das quais quase todas já foram mencionadas anteriormente:

- realizar campanhas de conscientização e treinamentos dos colaboradores, com o intuito de que protejam suas credenciais de acesso aos serviços da nuvem e seus dispositivos de acesso contra ameaças virtuais de todos os tipos, principalmente as oriundas de técnicas de engenharia social, as quais geralmente culminam em fraudes via *e-mail* e outras. Desta forma, tenta-se assegurar a confidencialidade e integridade das informações;

- é importante pesquisar se os fornecedores almejados possuem processos correlacionados à perda de dados e informações de terceiros, assim como os relatos dos usuários sobre a utilização das aplicações vislumbradas;
- deve-se optar por fornecedores que permitam realizar provas de conceitos das aplicações que disponibilizam em seus portfólios de serviços, para se ter uma noção do desempenho e qualidade dos serviços ofertados;
- pesquisar por fornecedores que ofereçam o controle de acesso às suas aplicações por usuário, com uso de autenticação e possibilidade de restrição de acesso à recursos específicos por perfil de usuário;
- optar por fornecedores que ofereçam o controle de acesso por *host*, através de filtro IP/MAC;
- credenciar *hosts*, via política de segurança, para acesso aos serviços de SaaS e protege-los com *software* antivírus, e com módulos de segurança, este último, caso seja disponibilizado pelo fornecedor, visando proteger as informações que são passadas às interfaces de acesso aos serviços de nuvem;
- optar por fornecedores que ofereçam suas aplicações munidas com recursos de criptografia, certificado de segurança ou *token*, de forma a tentar garantir a segurança da informação entre a origem e o destino na comunicação do *host* com os serviços de nuvem;
- assegurar os SLAs de disponibilidade das aplicações e suporte de forma contratual, assim como a guarda e confidencialidade das informações que sejam geradas e/ou tramitem pelo ambiente das aplicações;
- utilizar *links* de dados redundantes na corporação para tentar manter a disponibilidade de acesso aos serviços SaaS da nuvem pública, por parte da contratante.

5.4.3 Segurança na nuvem híbrida

A nuvem híbrida apresenta uma característica notável em relação à segurança dos dados corporativos e a economia financeira, pois possibilita às empresas fragmentarem suas informações, serviços, sistemas e aplicativos de acordo com o nível de criticidade e sigilo, pelas nuvens públicas e privadas que constituem seu

ambiente virtual, ou seja, ao passo que se beneficia das vantagens da segurança da nuvem privada, imputando nela suas informações e sistemas críticos, beneficiam-se também das vantagens econômicas da nuvem pública, implementando na mesma a disponibilização de uma vasta gama de informações e serviços com criticidade mais baixa, os quais estão submetidos a um risco aceitável, por parte da gestão corporativa, entretanto a proteção deste ambiente híbrido se faz necessária, uma vez que haverá comunicações entre a nuvem privada e a pública e qualquer falha de segurança em uma delas, poderá comprometer a segurança da outra.

Como já mencionado anteriormente e com base na concepção de Taurion (2009), a garantia do cumprimento dos princípios de segurança da informação está diretamente relacionada com o modelo de implantação adotado pela empresa.

A nuvem híbrida que constitui o ambiente virtual de uma organização pode apresentar uma estrutura bastante heterogênea, sendo composta por diversas nuvens de tipos diferentes e com arquiteturas diferentes em cada um dos tipos, desta forma, as abordagens de segurança específicas recomendadas para cada tipo de nuvem em cada arquitetura que constitui a nuvem híbrida, são as mesmas apresentas nos itens 5.4.1 e 5.4.2, entretanto as recomendações gerais que se destacam para a implementação da segurança da nuvem híbrida em si, seguem:

- realização de campanhas de conscientização e treinamento com os *insiders* para utilização adequada dos recursos de TI disponibilizados pela empresa, assim como, para evitarem fraudes digitais, as quais poderiam comprometer o ambiente virtual da organização;
- realização continua da atualização da política de segurança, por meio do SGSI, e da gestão de riscos, assim como a reclassificação das informações, serviços, sistemas e aplicativos com o propósito de identificação de quais itens permanecem ou migram para a nuvem privada ou pública que compõem o ambiente;
- implementação de controles de acesso com autenticação por usuário, *host e* sistema aos ambientes, principalmente para acesso às nuvens públicas;
- utilização de criptografia na comunicação entre as nuvens privadas e públicas;
- gerenciamento através de c*loud management platform* (CMP) voltada especificamente para nuvens híbridas e apoiada por solução de segurança

específica para nuvem, com o intuito de tornar possível a gestão unificada de ativos, automação e aplicação de políticas de segurança em todos os nós de nuvens, aumentando dessa forma o controle e consequentemente a segurança de todo o ambiente;

- utilização de *links* redundantes para a manutenção da disponibilidade de acesso às informações, serviços, sistemas e aplicativos presentes na nuvem privada da estrutura híbrida.

5.4.4 Segurança na nuvem comunitária

Conforme já apresentado no item 3.6.4, a nuvem comunitária corresponde a uma nuvem com recursos compartilhados restritos a um grupo fechado de corporações ou entidades que apresentam aspectos comuns ou similares. Ambas corporações participam do custeamento da nuvem, e por este fato a mesma se torna uma opção economicamente viável e tecnicamente atrativa, uma vez que as questões de desempenho, dinamismo, praticidade e outras também se mantém no ambiente compartilhado, desde que este seja bem gerenciado.

Como em todo ambiente comunitário, na nuvem comunitária também é necessária a definição de uma governança de segurança, com o intuito de se tentar preservar a integridade, confidencialidade e disponibilidade dos dados e informações de todas as corporações que fazem uso da nuvem.

Conforme Castro e Sousa V. L. P. (2010, p. 3):

> Ao analisar o cenário atual para o gerenciamento de segurança da informação em ambientes de Computação em Nuvem, muitas literaturas apontam a necessidade e a importância de se adotar um modelo de Governança da Segurança da Informação com a finalidade de mitigar os riscos inerentes dos modelos de prestação de serviços na Nuvem.

A nuvem comunitária corresponde a uma opção de nuvem que geralmente apresenta mais segurança que uma nuvem pública e um pouco menos de segurança que uma nuvem privada. Seguem recomendações de implementação de segurança da informação em nuvens comunitárias:

- através da formação de comitê de gestão de negócios da comunidade corporativa, o qual será responsável por definir quais as informações,

serviços, sistemas e aplicativos serão disponibilizados de forma compartilhada no ambiente;

- através da formação de comitê de segurança da informação da comunidade, o qual será responsável por implementar os níveis de segurança ao qual estarão submetidos cada informação, serviço, sistema e aplicativo dentro da comunidade, assim como o gerenciamento e monitoramento de todo o ambiente da nuvem e também será responsável por realizar a atualização da gestão de risco, assim como apresenta-la à gestão dos negócios, para análise e atualização da política de segurança da informação;
- através da cooperatividade entre as corporações que compõem a nuvem;
- através da realização de campanhas de conscientização e treinamento com todos os *insiders* das corporações, os quais possuam algum tipo de vínculo com a utilização da nuvem comunitária, tanto sobre a utilização adequada dos recursos internos de suas respectivas empresas, quanto sobre a utilização dos recursos disponibilizados na comunidade;
- através da implementação de controle de acesso às informações, serviços, sistemas e aplicativos, com autenticação, tanto para usuários quanto para hosts e sistemas;
- através de ferramenta de *software*, geralmente de virtualização, que permita segregar de forma protegida os repositórios de dados armazenados, com o intuito de possibilitar que determinadas empresas não possuam acesso aos dados de outras, ainda que utilizem o mesmo sistema e o mesmo hardware de forma compartilhada, exceto com as devidas credenciais de autorização;
- através da redundância de *links* para cada um do(s) DC(s) que mantém a infraestrutura física de TI da comunidade, visando manter a disponibilidade das informações, serviços, sistemas e aplicativos.

6 CONSIDERAÇÕES FINAIS

O advento da computação em nuvem surgiu exatamente em um cenário no qual as corporações são pressionadas, pela instabilidade do mercado, a adotarem novas tecnologias e ferramentas que lhes possibilitem atender, com agilidade, praticidade, dinamismo, e bom desempenho, a uma enorme gama de demandas de negócios de portes variados, ao passo em que não se onerem de forma demasiada para tal, entretanto a computação em nuvem traz a problemática de quais as formas de se implementar segurança da informação em seus tipos e arquiteturas de forma a proteger as informações corporativas.

No decorrer do capítulo “Importância da informação e tecnologia para as corporações”, foram apresentados os conceitos de dados, informações e conhecimentos, a necessidade da informação para a continuidade dos negócios de uma corporação, o que são recursos de tecnologia da informação, as consequências do comprometimento de informações corporativas e a importância de se proteger as mesmas, e assim foi entendido como as informações e serviços, apoiados por recursos de tecnologia da informação, dão suporte aos gestores para a tomada de decisões e consequente manutenção da continuidade dos negócios corporativos e quanto as corporações podem ser prejudicadas em caso de comprometimento de suas informações.

Ao longo do capítulo “A computação em nuvem”, foram apresentados as definições de virtualização e data center, o conceito da computação em nuvem e seus benefícios, tipos e arquiteturas, e desta forma, tornou-se fácil entender os tipos de serviços ofertados em cada arquitetura, como os mesmos são disponibilizados e quais as implicações para sua manutenção nos diferentes tipos de nuvem.

No capítulo “Cibercrime e cibersegurança”, apresentou-se o conceito de cibercrime, os tipos de cibercriminosos, ataques e fraudes mais comuns praticados no ambiente virtual, o conceito e ferramentas de cibersegurança e os pilares, serviços, política e softwares de segurança da informação, tornando simples o entendimento das ameaças presentes no ambiente virtual e quais as ferramentas disponíveis para a proteção contra ataques.

No capítulo “Segurança na computação em nuvem”, além da problemática da pesquisa, também é apresentada a relação da política de segurança da informação com o uso de sistema de gerenciamento de segurança da informação, assim como o conceito de risco, ameaça e vulnerabilidade e a relação entre o gerenciamento de riscos e a segurança da informação na nuvem.

Após a apresentação dos assuntos mencionados anteriormente ao longo dos capítulos, os objetivos específicos foram alcançados e proporcionaram considerável embasamento teórico para responder a problemática apresentada na introdução desta pesquisa, a qual é tratada no item 5.4.

Considerando a necessidade de proteção dos dados corporativos e da adoção da nuvem por parte de diversas corporações e possuindo a ciência sobre os tipos e arquiteturas de nuvem, assim como dos aspectos de cibersegurança, cibercrime, riscos, ameaças e vulnerabilidades presentes no ambiente da computação em nuvem e seus ativos, tornou-se possível sugerir formas de implementação de segurança para cada arquitetura de nuvem privada e pública, assim como inferir considerações de implementação para a nuvem híbrida e comunitária.

Com base em uma visão sistêmica desta pesquisa, chega-se ao entendimento que os benefícios da computação em nuvem podem ser usufruídos ao passo que se mantem um alto grau de segurança das informações corporativas. Para isso, primeiramente torna-se necessário que a gestão da corporação seja assessorada por uma boa equipe de profissionais da área de tecnologia da informação e faça continuamente a gestão de riscos das informações, sistemas, serviços e aplicações a serem disponibilizados na nuvem (após a contratação dos serviços também), por meio da definição de uma política de segurança consistente e que preferencialmente esteja apoiada em um sistema de gestão de segurança da informação. Em seguida a corporação deve elaborar o termo de referência dos serviços que se deseja contratar para atender a sua demanda e posteriormente deverá realizar pesquisas de mercado com o intuito de se conhecer os fornecedores e os serviços disponibilizados por cada um, procurando identificar pontos positivos e negativos e após a escolha do fornecedor, deverá firmar contratualmente os SLAs para disponibilização de serviços/sistemas/suporte e termos de salvaguarda e sigilo das informações armazenadas e em trânsito pelo ambiente da nuvem.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Leandro Farias dos Santos. **A segurança da informação nas redes sociais**. Monografia apresentada como requisito parcial para a obtenção do título de Tecnólogo em Processamento de Dados, da Faculdade de Tecnologia de São Paulo, São Paulo-SP, Brasil, 2011.

ADÃES, Marcelo. **A maturidade da segurança da informação**, 2010. Portal Tecno Ativa. Disponível em: <https://tecnoativa.wordpress.com/tag/27001/> Acesso em 19 de fevereiro de 2018.

ALECRIM, Cecília Gomes Muraro; BRUGGER, Maria Teresa Caballero; CAIXETA, Juliana Eugênia; CAMPOS, Marcelo Moreira; ORNELAS, Maysa; QUERINO, Magda Maria de Freitas; RAPOSO, Denise Maria dos Santos Paulinelli; SANTOS, Elias Alexandre Oliveira dos; SILVA, Maurício. **Metodologia da Pesquisa e da Produção Científica**. Caderno de estudo da matéria Metodologia da Pesquisa e da Produção Científica, a qual compõe a grade do curso de especialista em Cybercrimes e Cybersecurity, da Faculdade Unyleya, Brasília-DF, Brasil, 2016.

ALECRIM, Emerson. **O que é Tecnologia da Informação (TI)?**, 2011. Portal Info Wester. Disponível em: <https://www.infowester.com/ti.php> Acesso em 16 de fevereiro de 2018.

ALMEIDA, Maxwell Gonçalves de. **Armazenamento big data no monitoramento em nuvem**. Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Ciências da Computação, do Departamento de Informática e Estatística da Universidade Federal de Santa Catarina, UFSC, Florianópolis-SC, Brasil, 2014.

ALVES, Deriks Marques; COSTA, Marcelo; FURTADO, Maria Renata Silva; MORAVIA, Rodrigo Vitorino. **Computação em nuvem: um estudo sobre seus conceitos, tecnologia e aplicação**. Artigo científico apresentado como atividade extracurricular do curso de Sistemas de Informação pela Faculdade Infórium de Tecnologia, Belo Horizonte-MG, Brasil, 2013.

ASCHOFF, Amanda. **Arquitetura de nuvem: conheça as 3 camadas e os 3 tipos**, 2016. Portal Blog Safetec. Disponível em: <http://blog.safetec.com.br/cloud-computing/arquitetura-de-nuvem/> Acesso em 14 de fevereiro de 2018.

Associação Brasileira de Normas Técnicas. **Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação**. NBR ISO/IEC 17799. Segunda edição 31.08.2015 (Válida a partir de 30.09.2005), 2005.

Associação Brasileira de Normas Técnicas. **Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação**. NBR ISO/IEC 27002. Primeira edição 31.08.2005 (Válida a partir de 30.09.2005), 2005.

AVAST. **O que é pharming?**, s/a. Portal Avast. Disponível em: <https://www.avast.com/pt-br/c-pharming/> Acesso em 18 de fevereiro de 2018.

Big data e cloud computing: desafios e oportunidades. Portal Data Science Academy. Disponível em: < http://datascienceacademy.com.br/blog/big-data-e-cloud-computing-desafios-e-oportunidades/> Acesso em 14 de fevereiro de 2018.

BORGES, Hélder Pereira; MURY, Antonio Roberto; SCHULZE, Bruno; SOUZA, José Neuman de Souza. **Computação em nuvem**. Artigo científico, Brasil, 2011.

BUZZATE, Patrícia Monego. **Análise de vulnerabilidades através de scanners detectores**. Monografia apresentada como requisito parcial para a obtenção do título de Tecnólogo em Redes de Computadores, da Universidade Federal de Santa Maria, Santa Maria-RS, Brasil, 2014.

CARVALHO, Erick. **Tudo como Serviço: SaaS, IaaS e PaaS**, 2017. Portal Bar8. Disponível em: < https://bar8.com.br/sap-paas-saas-iaas-f4b176565e04> Acesso em 15 de fevereiro de 2018.

CASTRO, Rita de C. C. de; SOUSA, Verônica L. Pimentel de Sousa. **Segurança em Cloud Computing: governança e gerenciamento de riscos de segurança.** Artigo científico, Ceará, Brasil, 2010.

CHIRIGATI, Fernando Seabra. **Computação em nuvem: vantagens e desafios**, 2009. Portal GTA UFRJ. Disponível em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2009_2/seabra/vantagens.html> Acesso em 14 de fevereiro de 2018.

CHOINACKI, Hugo. **Virtualização de Servidores**. Monografia apresentada como requisito parcial para obtenção do grau de especialista em Gerenciamento de Servidores, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná, Curitiba, Brasil, 2012.

Conceito de conhecimento, 2010. Portal Conceito.de. Disponível em: < https://conceito.de/conhecimento/> Acesso em 13 de fevereiro de 2018.

Conceito de dados, 2012. Portal Conceito.de. Disponível em: < https://conceito.de/dados/> Acesso em 13 de fevereiro de 2018.

CRUZ, Diego Lopes. **Uma abordagem para detecção e proteção de ataques man-in-the-middle (mitm)**. Monografia apresentada como requisito parcial para a obtenção do título de Especialista em Redes de Computadores e Segurança de Redes, da Universidade Tuiuti do Paraná, UTP, Curitiba-PR, Brasil, 2014.

DAVENPORT, Thomas H.; PRUSAK, Laurence. **Conhecimento empresarial: como as empresas gerenciam o seu capital intelectual**. 4ª Edição. Rio de Janeiro: Campus, 1998.

DENZIN, N. K, LINCOLN, Y. S. I**ntrodução: a disciplina e a prática da pesquisa qualitativa**. O planejamento da pesquisa qualitativa: teorias e abordagens. 2ª Edição. Porto Alegre: Artmed, 2006.

DORNBUSCH, Juliane Mara. **Crimes digitais na internet**. Monografia apresentada como requisito parcial para a obtenção do título de Bacharel em Direito pela Universidade Tuiuti do Paraná, UTP, Curitiba-PR, Brasil, 2002.

FARIAS, Joselene. **Cloud Computing: computação em nuvem o novo desafio para a validação de sistemas computadorizados**, 2017. Portal Farmacêuticas. Disponível em: < http://www.farmaceuticas.com.br/cloud-computing-computacao-em-nuvem-o-novo-desafio-para-a-validacao-de-sistemas-computadorizados/> Acesso em 27 de fevereiro de 2018.

FREITAS, Eduardo Antônio Mello. **Gestão de riscos aplicada a sistemas de informação: segurança estratégica da informação**. Monografia apresentada como requisito parcial para a obtenção do título de especialista em Gestão Estratégica e Qualidade, da Universidade Cândido Mendes, UCAM, Brasília-GO, Brasil, 2009.

FREITAS, Rodrigo Randow; GOMES, Nazur Amorim; PENHA, Elton Wager Machado. **Computação em nuvem: a segurança da informação em ambientes na nuvem e em redes físicas**. Artigo científico publicado no Brazilian Journal of Production Engineering, São Mateus, Vol. 2, N.º 1 (Julho). p. 12-27 (2016). Editora CEUNES/DETEC. São Mateus – ES, Brasil, 2016.

FURLAN, Marcos da Silva; ASSIS, Naziro Hamed de. **Backup: Proteção e segurança de dados e informações em ambientes corporativos**. Monografia apresentada como requisito parcial para obtenção do grau de especialista em Infraestrutura de Redes de Computadores, do Núcleo Tecnológico da Fundação de Assistência e Educação – FAESA, Vitória, Brasil, 2015.

GOMES, Bruno Henrique Gaignoux. **Privacidade digital: a proteção e segurança de dados**. Monografia apresentada na matéria metodologia do trabalho científico para obtenção da nota final do semestre em questão. Universidade Federal do Pará, UFPA, Pará, Brasil, 2014.

GONÇALVES, Bruno Ortale. **Gerência e monitoramento de uma nuvem privada**. Monografia apresentada como requisito parcial para a obtenção do título de Bacharel em Ciências da Computação do Centro Tecnológico da Universidade Federal de Santa Catarina, UFSC, Florianópolis-SC, Brasil, 2011.

GRUPOFATEC2013. **Plano de ação prática para implementação da ISO/IEC 27002**, Portal Cgerumblog.wordpress. Disponível em: < https://cgerumblog.wordpress.com/tag/plano-de-acao/> Acesso em 28 de fevereiro de 2018.

GSW. **A importância da gestão da segurança da informação**, 2011. Portal GSW. Disponível em: <https://www.gsw.com.br/noticias/21-centro-de-desenvolvimento-de-sistemas/97-a-importancia-da-gestao-da-seguranca-da-informacao/> Acesso em 19 de fevereiro de 2018.

HAMED, Ana Paula Lima Penha. **Segurança da informação em ambientes virtualizados**. Monografia apresentada como requisito parcial para obtenção do título de Especialista em Cibercrime e Cibersegurança, do Núcleo de Pós-Graduação EAD. Faculdade Unyleya, Vitória-ES, Brasil, 2017.

JESUS, Ygor Kiefer Follador de. **Análise e detecção de anomalias em políticas de segurança: um estudo prático com firewalls**. Dissertação submetida ao Programa de Pós-Graduação como requisito parcial para a obtenção do grau de Mestre em Informática, da Universidade Federal do Espírito Santo, UFES, Vitória-ES, Brasil, 2016.

JÚNIOR, João Francisco Gonçalves Sobrinho. **Storm IDS: um sistema de detecção de intrusão escalável e distribuído**. Monografia apresentada como requisito parcial para a obtenção do título de Engenheiro da Computação, da Universidade de Brasília, Brasília-GO, Brasil, 2016.

LOUREIRO, Geraldo. **Licitação de Serviços de Computação em Nuvem**, 2016. Portal Geraldo Loureiro – Wiki. Disponível em: < http://www.geraldoloureiro.com/wiki/index.php?title=1o_Fórum_IBGP_de_Debates> Acesso em 15 de fevereiro de 2018.

Informação, 2018. Portal Wikipedia. Disponível em: <https://pt.wikipedia.org/wiki/Informação/> Acesso em 13 de fevereiro de 2018.

MEDEIROS, Thyago dos Santos. **Proposta de uma metodologia para geração de dados para avaliação das ferramentas de detecção de intrusão**. Monografia apresentada como requisito parcial para a obtenção do título de Especialista em Redes de Computadores, da Universidade Federal do Rio Grande do Sul, UFRS, Porto Alegre-RS, Brasil, 2008.

Metodologia de Pesquisa. Portal Virtual UFC. Disponível em: http://www.virtual.ufc.br/solar/aula_link/gad/I_a_H/metodo_de_pesquisa/aula_02-2324/02.html> Acesso em 17 de fevereiro de 2018.

MORAES, Eliana Márcia. **Planejamento de Backup de Dados**. Dissertação (Mestrado em Gestão e Desenvolvimento Regional) – Departamento de Economia, Contabilidade e Administração, da Universidade de Taubaté, Taubaté, São Paulo, Brasil, 2007.

MORAES, Leonardo. **Gestão da informação e do conhecimento**, 2014. Portal Slideshare.net – Leomoraes. Disponível em: https://pt.slideshare.net/leomoraes/informao-e-conhecimento-nas-organizaes-gesto/> Acesso em 11 de fevereiro de 2018.

MOREIRA, Melo. **O que é cibercrime: o que é cibercrime e quais os principais cibercrimes praticados**, 2017. Portal Melo Moreira advogados. Disponível em: < https://melomoreiraadvogados.com.br/cibercrimes-saiba-mais-sobre-os-principais-crimes-praticados-na-internet/> Acesso em 19 de fevereiro de 2018.

NORMAS ABNT – Regras para TCC e Monografias (ATUALIZADAS), 2017. Portal Normas e Regras. Disponível em: http://www.normaseregras.com/normas-abnt/ Acesso em 15 de fevereiro de 2018.

NUBLING, Gabriela. **Cloud computing aplicada ao cenário corporativo**. Monografia apresentada como requisito parcial para a obtenção do título de Tecnólogo em Processamento de Dados da Faculdade de Tecnologia de São Paulo, FATEC, São Paulo-SP, Brasil, 2011.

O que é virtualização?, 2017. Portal One Linea Telecom. Disponível em: <http://www.onelinea.com.br/o-que-e-virtualizacao/> Acesso em 13 de fevereiro de 2018.

OLIVEIRA, Waldes. **Riscos, vulnerabilidade e ameaça em segurança da informação**, 2016. Portal Techtem. Disponível em: <http://www.techtem.com.br/seguranca-da-informacao-riscos-vulnerabilidade-e-ameaca/> Acesso em 28 de fevereiro de 2018.

ORLANDINI, Leandro. **A importância dos Sistemas de Informação**, 2005. Disponível em: <http://www.bonde.com.br/colunistas/administracao-e-tecnologia/a-importancia-dos-sistemas-de-informacao-54857.html/> Acesso em 14 de fevereiro de 2018.

PÁGINA da AWS Amazon. Disponível em: <https://aws.amazon.com/pt/> Acesso em 16 de fevereiro de 2018.

PÁGINA da Cloud Google. Disponível em: <https://cloud.google.com/> Acesso em 16 de fevereiro de 2018.

PÁGINA da Azure Microsoft. Disponível em: <https://azure.microsoft.com/pt-br/> Acesso em 16 de fevereiro de 2018.

PÁGINA da VMware. Disponível em: <https://www.vmware.com/br.html> Acesso em 16 de fevereiro de 2018.

PÁGINA da Salesforce. Disponível em: <https://www.salesforce.com/br/cloud-computing/> Acesso em 16 de fevereiro de 2018.

PÁGINA da Citrix. Disponível em: <https://www.citrix.com.br/> Acesso em 16 de fevereiro de 2018.

PÁGINA da AT&T. Disponível em: <https://www.synaptic.att.com/> Acesso em 16 de fevereiro de 2018.

PALMA, Fernando. **O que é um sistema de gestão de segurança da informação (SGSI)**, 2016. Portal GSTI. Disponível em: <https://www.portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html> Acesso em 19 de fevereiro de 2018.

PEREIRA, Francisco. **Cibercrime, cibersegurança e ciberguerra**, 2013. Portal Proteja Internet – Blogspot. Disponível em: <http://protejainternet.blogspot.com/2013/12/> Acesso em 15 de fevereiro de 2018.

Pesquisa nacional de segurança da informação 2014: resultados e desafios!, 2014. Portal Exin no Slideshare. Disponível em: < https://pt.slideshare.net/Exin/exin-daryus-apresentacao-pesquisa/> Acesso em 17 de fevereiro de 2018.

PINHEIRO, José Mauricio Santos. **O que é um data center**, 2014. Portal Projeto de Redes. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_datacenter.php> Acesso em 13 de fevereiro de 2018.

PINTO, Kleber de Souza. **Vantagens e benefícios da utilização da nuvem**, 2012. Portal TI Especialistas. Disponível em: <https://www.tiespecialistas.com.br/2012/10/vantagens-e-beneficios-da-utilizacao-da-nuvem/> Acesso em 14 de fevereiro de 2018.

PROOF. **Qual a importância da conscientização de usuários para a segurança da informação?**, 2017. Portal Proof. Disponível em: <http://www.proof.com.br/blog/conscientizacao-de-usuarios-seguranca-da-informacao/> Acesso em 19 de fevereiro de 2018.

REZENDE, Eliana. **Dados, Informação e Conhecimento. O que são?**, 2015. Portal Eliana Rezende. Disponível em: <http://eliana-rezende.com.br/dados-informacao-e-conhecimento-o-que-sao/> Acesso em 15 de fevereiro de 2018.

Significado de Informação, 2012. Portal Significados. Disponível em: <https://www.significados.com.br/informacao/> Acesso em 13 de fevereiro de 2018.

SILVA, Denise Ranghetti Pilar da; STEIN, Lilian Milnitsky. **Segurança da informação: uma reflexão sobre o componente humano**. Artigo científico, Brasil, 2007.

SILVA, Sidenilto Santos. **Backup não é apenas uma cópia,** 2014. Portal Sidus Maximus. Disponível em: <http://sidusmaximusti.blogspot.com.br/2014/02/backup-nao-e-apenas-uma-copia.html/> Acesso em 18 de fevereiro de 2018.

SOARES, Jackson. **6 soluções de computação em nuvem para cortar custos de TI**, 2016. Portal Linked In. Disponível em: <https://www.linkedin.com/pulse/6-soluções-de-computação-em-nuvem-para-cortar-custos-ti-soares> Acesso em 14 de fevereiro de 2018.

SOUZA, Saymon Castro de. **Uma abordagem baseada em regras e computação em nuvem para desenvolvimento de aplicações em redes de sensores sem fio**. Dissertação submetida ao Programa de Pós-Graduação como requisito parcial para a obtenção do grau de Mestre em Informática, da Universidade Federal do Espírito Santo, UFES, Vitória-ES, Brasil, 2013.

SYMANTEC. **Glossário - DoS (denial-of-service) attack (ataque de DoS (negação de serviço))**, s/a. Portal Symantec. Disponível em: < https://www.symantec.com/pt/br/security_response/glossary/define.jsp?letter=d&word=dos-denial-of-service-attack/> Acesso em 13 de fevereiro de 2018.

TAURION, Cezar. **Cloud Computing: computação em nuvem transformando o mundo da tecnologia da informação**. 1ª Edição. Rio de Janeiro: Brasport, 2009.

Tecnologia da Informação, 2017. Portal Wiki2 – Pastoral da Criança. Disponível em: <https://wiki2.pasoraldacrianca.org.br/wiki/Tecnologia_da_Informação > Acesso em 14 de fevereiro de 2018.

VANCE, Jeff. **Quais são as 10 empresas de nuvem mais poderosas?**, 2012. Portal Computer World. Disponível em: <http://computerworld.com.br/tecnologia/2012/09/10/as-10-empresas-de-nuvem-mais-poderosas> Acesso em 16 de fevereiro de 2018.

VERGARA, S. C. **Projeto e relatórios de pesquisa em administração**. Editora Atlas, São Paulo, Brasil, 2003.

VERONESE, Lucas de Paula. **Avaliação de um sistema escalável de classificação CNAE implementado em cloud computing**. Dissertação submetida ao Programa de Pós-Graduação como requisito parcial para a obtenção do grau de Mestre em Informática, da Universidade Federal do Espírito Santo, UFES, Vitória-ES, Brasil, 2011.

ÍNDICE ONOMÁSTICO