Revista a Primeira EVOLUÇÃO

Ano IV n. 38 Mar. 2023
ISSN 2675-2573

ESCOLA CÂNDIDA OLIVEIRA LUZ

Porto Barreiro – PR

(em um acampamento de famílias Sem Terra)

Filiada à: ABEC BRASIL

Platform & workflow by OJS / PKP

www.primeiraevolucao.com.br

Revista a1 EVOLUÇÃO

Ano IV - nº 38 - Março de 2023

ISSN 2675-2573

Uma publicação mensal da Edições Livro Alternativo

AUTORES(AS) DESTA EDIÇÃO

Anildo Joaquim da Silva
Isabel Delfina Casimiro e Luís Venâncio
Jucélia Maria do Nascimento
Jucira Moura Vieira da Silva
Juliana Godoi Marques
Leidimar Martins da Rocha Almeida
Leila da Silva Siqueira
Luciana Mendes do Rego
Marlene da Silva
Patrícia Mendes Cavalcante de Souza
Rita de Cássia Martins Serafim
Vera Lucia Meneses de Lima Marques
Viviane de Cássia Araujo

Dados Internacionais de Catalogação na Publicação (CIP)

Revista Primeira Evolução [recurso eletrônico] / [Editor] Antonio Raimundo Pereira Medrado. – ano 4, n. 38 (mar. 2023). – São Paulo : Edições Livro Alternativo, 2023.
132 p. : il. color

Bibliografia
Mensal
Vol. 1, n. 1 (fev. 2020)
ISSN 2675-2573 (on-line)
Modo de acesso: https://primeiraevolucao.com.br
DOI 10.52078/issn2673-2573.rpe.38

1. Educação – Periódicos. 2. Pedagogia – Periódicos. I. Medrado, Antonio Raimundo Pereira, editor. II. Título.

CDD 22. ed. 370.5

Patrícia Martins da Silva Rede – Bibliotecária – CRB-8/5877

ACESSOS: https://primeiraevolucao.com.br https://doi.org/10.52078/issn2673-2573.rpe.38

São Paulo | 2023

Revista PRIMEIRA EVOLUÇÃO

ISSN: 2675-2573
Publicação Mensal

Editor Responsável:
Antônio Raimundo Pereira Medrado

Editor correspondente (ANGOLA):
Manuel Francisco Neto

Coordenação editorial:
Ana Paula de Lima
Andreia Fernandes de Souza
Antônio Raimndo Pereira Medrado
Isac dos Santos Pereira
José Wilton dos Santos
Manuel Francisco Neto
Vilma Maria da Silva

Com. de Avaliação e Leitura:
Prof. Me. Adeílson Batista Lins
Prof. Me. Alexandre Passos Bitencourt
Profa. Esp. Ana Paula de Lima
Profa. Dra. Andreia Fernandes de Souza
Profa. Dra. Denise Mak
Prof. Dr. Isac dos Santos Pereira
Prof. Dr. Manuel Francisco Neto
Profa. Ma. Maria Mbuanda Caneca Gunza Francisco
Profa. Mirella Clerici Loayza
Profa. Dra. Patrícia Tanganelli Lara
Profa. Dra. Thaís Thomaz Bovo

Bibliotecária:
Patrícia Martins da Silva Rede

Colunistas:
Profa. Esp. Ana Paula de Lima
Profa. Ma. Cleia Teixeira da Silva
Prof. Dr. Isac dos Santos Pereira
Prof. Me. José Wilton dos Santos

Edição, Web-edição e projetos:
Antonio Raimundo Pereira Medrado
Vilma Maria da Silva
Lee Anthony Medrado

Contatos
Tel. 55(11) 99543-5703
Whatsapp: 55(11) 99543-5703
primeiraevolucao@gmail.com (S. Paulo)
netomanuelfrancisco@gmail.com (Luanda)
https://primeiraevolucao.com.br

Imagens, fotos, vetores etc:
https://publicdomainvectors.org/
https://pixabay.com
https://www.pngwing.com
https://br.freepik.com

Publicada no Brasil por:
Edições Livro Alternativo
CNPJ: 28.657. 494/0001-09
Colaboradores voluntários em:

A revista PRIMEIRA EVOLUÇÃO é um projeto editorial criado pela **Edições Livro Alternativo** para ajudar e incentivar professores(as) a publicarem suas pesquisas, estudos, vivências ou relatos de experiências.

Seu corpo editorial é formado por professores/as especialistas, mestres/as e doutores/as que atuam na rede pública de ensino, e por profissionais do livro e da tecnologia da informação.

Uma de suas principais características é o fato de ser **independente e totalmente financiada por professoras e professores**, e de distribuição gratuita.

PROPÓSITOS:

Rediscutir, repensar e refletir sobre os mais diversos aspectos educacionais com base nas experiências, pesquisas, estudos e vivências dos profissionais da educação;

Proporcionar a publicação de livros, artigos e ensaios que contribuam para a evolução da educação e dos educadores(as);

Possibilitar a publicação de livros de autores(as) independentes;

Promover o acesso, informação, uso, estudo e compartilhamento de sofwares livres;

Incentivar a produção de livros escritos por professores/as e autores independentes;

Financiar (total ou parcialmente,) livros de professoras/es e estudantes da rede pública.

PRINCÍPIOS:

Os trabalhos voltados para a **educação, cultura** e produções independentes;

O uso exclusivo de **softwares livres** na produção dos livros, revistas, divulgação etc;

A ênfase na produção de **obras coletivas** de profissionais da educação;

Publicar e divulgar **livros de professores(as)** e autores(as) independentes;

O respeito à **liberdade e autonomia** dos autores(as);

O combate ao despotismo, ao preconceito e à superstição;

O respeito à **diversidade**.

Esta revista é mantida e financiada por professoras e professores.
Sua distribuição é, e sempre será, livre e gratuita.

Produzida com utilização de softwares livres

Filiada à:

www.primeiraevolucao.com.br

A educação evolui quanto mais evoluem seus profissionais

SUMÁRIO

ARTIGOS

APRESENTAÇÃO

Os professores desempenham um papel crucial no desenvolvimento educacional e intelectual de seus alunos, mas também têm um papel importante a desempenhar na pesquisa e publicação de seus estudos. A pesquisa acadêmica é fundamental para avançar o conhecimento em uma determinada área e para aprimorar a qualidade do ensino em geral.

Quando os professores pesquisam e publicam seus estudos, eles contribuem para o avanço do conhecimento em sua área de atuação e ajudam a criar uma cultura de aprendizado contínuo. Ao conduzir pesquisas, os professores têm a oportunidade de aprofundar sua compreensão de tópicos específicos e descobrir novas informações que podem ser aplicadas em suas aulas.

Além disso, a publicação de estudos ajuda a disseminar essas descobertas e contribuições para uma audiência mais ampla, incluindo outros professores, pesquisadores e estudantes. Isso pode levar a novas colaborações e oportunidades de pesquisa, bem como a uma melhor compreensão dos desafios e oportunidades enfrentados pelos educadores.

Por fim, a pesquisa e publicação de estudos também pode ser uma fonte de inspiração para os alunos, mostrando-lhes que seus professores estão engajados em aprender continuamente e que valorizam o conhecimento e a descoberta. Isso pode motivar os alunos a se tornarem mais envolvidos em suas próprias pesquisas e estudos, criando assim uma cultura de aprendizado e descoberta contínua.

Nós, da Revista Primeira Evolução, temos orgulho de proporcionar um espaço inclusivo e colaborativo para que os profissionais da educação publiquem seus estudos, pesquisas e experiências. Fazemos isso porque amamos a educação, conhecemos e vivemos a realidade das salas de aulas e nos dedicamos diariamente ao bem-estar e à emancipação do ser humano.

Junte-se a nós. #Junt@sSomosMaisFortes

Profª. Vilma Maria da Silva
Pedagoga, especialista em Educação Especial e Alfabetização.
Coordenadora Editorial da Edições Livro Alternativo
vilmamedrado@gmail.com

SEGURANÇA DE INFORMAÇÃO NO AMBIENTE DA COMPUTAÇÃO NA NUVEM

ANILDO JOAQUIM DA SILVA

RESUMO

Esta pesquisa demonstra de forma sucinta sobre a Cloud Computing e a sua Segurança. É um novo paradigma da Tecnologia de Informação, de facto, que tem sido imparável pela facilidade dos seus serviços que têm características essenciais tais como Autoatendimento sob demanda, Amplo acesso à rede, Elasticidade rápida, Mensuração do serviço e Localização-recurso transparente de pool para múltiplos cliente. Para além das características supracitadas, a Cloud Computing (CC) possui os principais modelos deinfraestrutura como serviço (IaaS), Plataforma como serviço (PaaS) e Software como serviço (SaaS), visto que isto, consiste no armazenamento, compartilhamento e acessibilidade dos dados em qualquer parte do mundo com acesso remoto e Internet. Este feito é graças a Virtualização, que é abstração de hardware, ou seja, quase inexistência de memória física, mas, com maior capacidade de armazenamento em memória virtual. Não obstante, ao que já frisamos, o objectivo principal deste artigo é analisar e exteriorizar as principais ameaças nos modelos da computação na Nuvem, portanto, é uma preocupação proeminente das pessoas singulares e empresas, ora bem, a Segurança em Cloud consiste em proteger os dados e serviços através dos seus quatro pilares fundamentais, nomeadamente: Confidencialidade, Autenticidade, Integridade e Disponibilidade, no sentido de evitar qualquer risco em todo processo de migração e armazenamento dos dados. Com esta Dissertação, pretendemos reforçar a garantia do uso dos serviços da Cloud Computing, em função as vantagens que tem oferecido aos utentes, como eficiência, automação, elasticidade, escalabilidade e o aumento da produtividade. Por isso é que, a adesão e a migração das empresas é cada vez eminente para a Computação das Nuvens, mas pensando em como será garantida a segurança por terceiros, visto que, é um elemento crucial para qualquer pessoa singular ou empresa.

Palavras Chave: Cloud Computing. Segurança. Virtualização. Empresa

ANÁLISE DAS CONDIÇÕES DE SEGURANÇA NA COMPUTAÇÃO DAS NUVENS

Nestes últimos anos, a Tecnologia de Informação (TI), tem evoluído cada segundo que passa, trazendo consigo novos modelos de tecnologias que têm ajudado na redução significativa dos recursos ou meios físicos nas empresas. Um destes modelos de tecnologia é o Cloud Computing, ou seja, Computação em Nuvem, que consiste na organização, armazenamento e entrega dos recursos de através da Internet, utilizando um provedor de serviços da nuvem, como por exemplo o AWS – Amazon Web Services, Microsoft e Google.

Diferente dos modos anteriores, a computação da nuvem introduz novas modalidades de negócio como é o caso de pagamento conforme o uso, Serviços mensuráveis e sob demanda, entrega fácil por via web. Dado o facto de utilizar a virtualização, a computação na nuvem para além de tornar os recursos elásticos, vem libertar as empresas do factor hardware, o que vem diminuir o consumo de energia, propiciando um ambiente computacional amigável ao ambiente.

O termo Cloud Computing, representa não uma nova tecnologia, mas sim um novo modelo operacional que reúne um conjunto de tecnologias já existentes para conduzir negócios de uma maneira diferente. E por este facto que existem diferentes percepções do que seja cloud computing, o que torna a padronização da sua definição uma tarefa difícil(Andrei Braga, s/d). Segundo o NIST – National Instutite of Standards and Technology (Instituto Nacional de Padrões e Tecnologia) do Ministério do Comércio americano, (2019) a computação em nuvem é um modelo para habilitar o acesso por rede ubíquo, conveniente e sob demanda a um conjunto compartilhado de recursos de computação (como redes, servidores, armazenamento, aplicações e serviços) que possam ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços(NIST, 2019).

A Segurança da informação nada mais é do que garantir a integridade e protecção das informações de uma organização (Jean Dias, 2012). Enquanto que, a NIST, afirma que as organizações que utilizam uma abordagem de computação em nuvens privadas possuem um maior nível de controle sobre os dados (NIST, 2019).

O ritmo de evolução da computação na Nuvem e sobretudo as valências que fornece propõem, de forma inevitável, a sua adesão. Nesta Dissertação, a abordagem fundamental recaí sobre a segurança dos serviços de Cloud Computing que é uma grande preocupação dos clientes e é o desafio mais visível a ser enfrentado. O trabalho analisa e exterioriza as principais ameaças nos modelos principais da computação na Nuvem como é o caso do SaaS, PaaS e IaaS e os mecanismos actualmente existentes para a sua mitigação. Uma infraestrutura em OpenStack é criada para facilitar a aproximação dos aspectos de segurança.

COMPUTAÇÃO EM NUVEM

O NIST definiu computação em nuvem como um modelo, para permitir o acesso ubíquo e conveniente à rede a pedido de um conjunto partilhado de recursos de computação configuráveis (redes, servidores, armazenamento, serviços e aplicações) quepode ser rapidamente aprovisionado e libertado, com o mínimo esforço de gestão ou interação do prestador de serviços (NIST, 2019).

Computação em nuvem, significa desenvolvimento e aplicação de tecnologia de computação baseada na Internet. Este termo é um método de cálculos informáticos, num espaço em que as capacidades baseadas em TI são apresentadas como um serviço para o utilizador, podendo ter acesso a serviços

baseados em tecnologia na Internet, sem informação especializada sobre estas tecnologias ou ter ocontrole de infraestruturas tecnológicas que as suportam. Trata-se assim de um conceito geral, que está a ser usado para a integração de novas tecnologias, incluindo

software como serviço, web e outras novas soluções apresentadas recentemente, podendo atender a todos os requisitos do utilizador no espaço Internet (Barros, 2021). A computação na nuvem é um novo modelo de computação que permite ao usuário final acessar uma grande quantidade de aplicações e serviços em qualquer lugar e independente da plataforma, bastando para isso ter um terminal conectado à "nuvem". A palavra nuvem sugere uma ideia de ambiente desconhecido, o qual podemos ver somente seu início e fim. Por este motivo esta foi muito bem empregada na nomenclatura deste novo modelo, onde toda a infraestrutura e recursos computacionais ficam "escondidos", tendo o usuário o acesso apenas a uma interface padrão através da qual é disponibilizado todo o conjunto de variadas aplicações e serviços(Andrei Braga e Nogueira, s/d).

É bom lembrar que, por detrás deste mistério todo (computação em nuvem), existem data centers que suportam os serviços de armazenamento, compartilhamento e acessibilidade, o que tem suportado o funcionamento pleno das plataformas dos provedores para os clientes.

CARACTERÍSTICAS ESSENCIAIS PARA UMA NUVEM DE ALTO DESEMPENHO

O (NIST) Instituto Nacional de Normas e Tecnologia Americano, identifica várias características essenciais de uma nuvem de alto desempenho (NIST, 2019).

Serviços sob demanda: o usuário pode definir automaticamente e sob demanda o fornecimento de recursos da nuvem, tais como poder de processamento e capacidade de armazenamento, conforme sua necessidade e sem que haja interação humana com o prestador de serviço.

Acesso por banda larga: recursos estão disponíveis na rede e são acessados pelos clientes através de variadas plataformas (e.g., smartphones, laptops, desktops, etc.).

Conjunto de recursos: os recursos de computação (armazenamento,processamento,memória, largura de banda e máquinas virtuais) do provedor são agrupados para atender múltiplos usuários. Esses recursos, sejam eles físicos ou virtuais, são atribuídos dinamicamente e de acordo com a demanda dos clientes.

Elasticidade rápida: recursos podem ser rapidamente fornecidos para garantir a escalabilidade dos serviços. Assim, o usuário tem a impressão de que os recursos disponíveis são ilimitados e podem ser adquiridos em qualquer quantidade e a qualquer momento.

Serviço mensurável: a nuvem controla e otimiza o uso de recursos, fornecendo métricas de acordo com o tipo de serviço sendo fornecido. Tanto o provedor quanto o cliente podem monitorar e controlar a utilização dos recursos.

PRINCIPAIS MODELOS DOS SERVIÇOS DA COMPUTAÇÃO EM NUVEM

Além desses características supracitadas, o NIST também define camadas de oferta de serviço e modelos de implantação. Os modelos de implantação incluem nuvens privadas, públicas, comunidade e híbridas. As camadas de serviço para cada um desses modelos de entrega incluem:

Infraestrutura como Serviço - *IaaS (Infrastructure as a Service*): Se refere à disponibilização dos componentes básicos da TI em nuvem como: processamento, armazenamento, rede entre outros recursos. Entre outras palavras, fornece todos os

recursos de um Data Center local de forma virtualizada, disponível via Internet através de hospedagem do provedor do serviço. Este modelo de computação em nuvem, permite ao usuário controlar ou gerenciar os serviços por meio de aplicações acessadas pela Internet. Além disso, implantar sistemas operacionais, controlar o armazenamento de dados e arquivos e prover infraestrutura para as aplicações desenvolvidas por meio de servidores de aplicação são também papéis desse tipo de infraestrutura. Seus principais benefícios são: Maior segurança e qualidade dos hardwares ofertados por um preço menor do que seria se fosse montado um Data Center local com as mesmas configurações que foram contratadas para esse serviço e maior agilidade na inovação e implementação de aplicativos e serviços oferecidos aos clientes por estar num ambiente altamente escalável, de alta adaptabilidade e pronto para uso e alterações de acordo com o desejo do cliente (Silva, 2022). A imagem abaixo, ilustra uma infraestrutura Iaas:

Fonte: https://blog.introduce.com.br/iaas-paas-saas-conheca-os-modelos-de-cloud-computing/

Plataforma como Serviço - PaaS (Platform as a Service): é um dos modelos de computação em nuvem. Possui o foco em criar e hospedar aplicativos Web, como também prover soluções para suportar o desenvolvimento de aplicações, passando por todas as fases do ciclo de vida de um aplicativo Web: compilação, teste, implantação, gerenciamento e atualização. PaaS nada mais é do que um ambiente de desenvolvimento e implantação completo na nuvem marcado principalmente por uma agilidade no desenvolvimento e na implantação de softwares. O PaaS fornece aos usuários e desenvolvedores as ferramentas necessárias para tal, sem se preocupar com a configuração ou gerenciamento da infraestrutura dos servidores, armazenamento, redes e bancos de dados (Silva, 2022). Utiliza a mesma estrutura do IaaS com o adicional da utilização de sistemas operacionais, ferramentas de desenvolvimento, serviços de BI (Business Intelligence) e sistemas gerenciadores de banco de dados por exemplo. Alguns dos softwares ou provedores PaaS mais conhecidos são: IBM Bluemix, Microsoft Windows Azure, Jelastic, Google App Engine e Red Hat OpenShift. A imagem abaixo, ilustra uma plataforma Paas:

Fonte: https://blog.introduce.com.br/iaas-paas-saas-conheca-os-modelos-de-cloud-computing/

Software como Serviço - SaaS *(Software as a Service)*: software como serviço de computação em nuvem é uma definição que se dá para quando um cliente, empresa ou corporação utiliza uma aplicação sem ter que instalá-lo em suas máquinas e servidores. O acesso é realizado de forma totalmente remota e normalmente através de qualquer dispositivo, seja computadores, notebooks, tablets ou smartphones (Silva, 2022). Esse é um serviço completo e o principal tipo de utilização da nuvem como serviço. Alguns dos sistemas SaaS mais conhecidos são os de armazenamento de arquivo, como por exemplo Dropbox, Google Docs, Google Drive. Tem também o Salesforce, Amazon AWS, LinkedIn, Workday entre outros. A imagem abaixo, ilustra interação com o software Saas:

Fonte: https://blog.introduce.com.br/iaas-paas-saas-conheca-os-modelos-de-cloud-computing/

Uma **infraestrutura na nuvem** é o conjunto de hardware e software que habilita as cinco características essenciais da computação em nuvem. A infraestrutura na nuvem é composta por uma camada física e uma camada de abstração. A camada física consiste dos recursos de hardware que suportam os serviços na nuvem sendo oferecidos, e geralmente inclui servidores, armazenamento e rede. A camada de abstração consiste do software instalado sobre a camada física, através do qual as cinco características essenciais da nuvem se manifestam. Conceitualmente, a camada de abstração assenta-se sobre a camada física (NIST, 2019).

TIPOS DE CLOUDS OU MODALIDADES DE INSTALAÇÃO

Segundo O NIST – *National Instutite of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia) do Ministério do Comércio americano (Center, 2014), os tipos de clouds são os seguintes:

Nuvem privada: A infraestrutura na nuvem é provisionada para uso exclusivo por uma única organização composta de diversos consumidores (como unidades de negócio). A sua propriedade, gerenciamento e operação podem ser da organização, de terceiros ou de uma combinação mista, e pode estar dentro ou fora das instalações da organização.

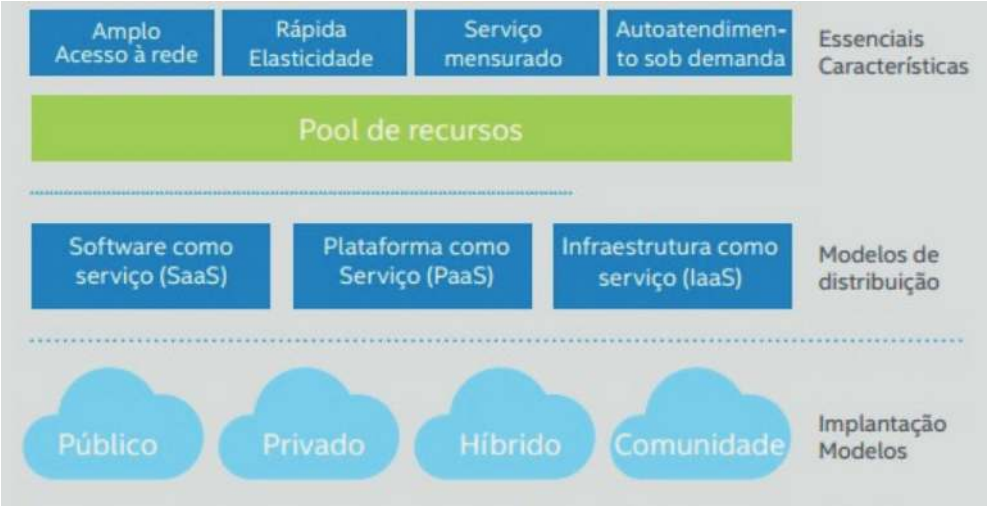
Nuvem comunitária: A infraestrutura na nuvem é provisionada para uso exclusivo por uma determinada comunidade de consumidores de organizações que têm interesses em comum (de missão, requisitos de segurança, políticas, observância de regulamentações). A sua propriedade, gerenciamento e operação podem ser de uma ou mais organizações da comunidade, de terceiros ou de uma combinação mista, e pode estar dentro ou fora das instalações das organizações participantes.

Nuvem pública: A infraestrutura na nuvem é provisionada para uso aberto ao público em geral. A sua propriedade, gerenciamento e operação podem ser de uma empresa,

uma instituição acadêmica, uma organização do governo, ou de uma combinação mista. Ela fica nas instalações do fornecedor.

Nuvem híbrida: A infraestrutura na nuvem é uma composição de duas ou mais infraestruturas na nuvem (privadas, comunitárias ou públicas) que permanecem entidades distintas, mas são interligadas por tecnologia padronizada ou proprietária que permite a comunicação de dados e portabilidade de aplicações (como transferência de processamento para a nuvem para balanceamento de carga entre nuvens).

Modelo de computação em nuvem do Instituto Nacional de Normas e Tecnologia Americano (NIST).



Fonte: http:// csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

Tabela: Comparação entre abordagens de implantação (NIST).

Nuvem	Gerência	Propriedade	Localização	Segurança
Pública	Terceira	Terceira	Externa e Interna	Baixa
Privada	Própria	Própria ou Terceira	Externa e Interna	Alta
Híbrida	Própria ou Terceira	Própria ou Terceira	Externa e Interna	Média
Comunitária	Própria ou Terceira	Própria ou Terceira	Externa e Interna	Média

Adaptada: de (CSA, 2011)

A gerência diz respeito a quem controla a nuvem, ou seja, quem organiza e administra os serviços. Assim, em nuvens privadas a gerência é feita pela própria instituição que se utiliza de seus serviços, enquanto em nuvens públicas a gerência é realizada por terceiros; já no caso de nuvens híbridas/comunitárias, a gerência pode ser própria ou de terceiros. A propriedade indica quem fornece o serviço de nuvem: em uma nuvem pública, o serviço é fornecido por terceiros, enquanto nuvens públicas, híbridas e comunitárias podem ser fornecidas tanto por terceiros ou usando recursos próprios. A localização refere-se ao posicionamento da parte física da nuvem, como, por exemplo, a sala-cofre na qual está localizado o hardware sob o qual as camadas da nuvem são construídas. Como tecnologias de nuvem em geral fornecem um elevado grau de transparência na localização dos recursos subjacentes, nuvens computacionais podem ser colocadas tanto em ambientes

externos como internos à organização (ou mesmo uma combinação dos dois), independentemente do seu tipo (Koslovski, 2014).

Finalmente, no tocante à segurança, com uma nuvem privada a organização mantém seus dados limitados ao acesso interno, garantindo um elevado nível de segurança pois a gerência e utilização da nuvem são realizadas pela própria organização. Ao utilizar uma nuvem híbrida a organização permite que sua nuvem privada comunique-se com uma nuvem (pública ou privada) sob gerência de outrem, tornando o nível de segurança um pouco mais baixo devido à troca de dados com uma entidade cujas políticas de segurança são possivelmente desconhecidas (ENISA, 2011). Já a nuvem pública é o tipo de nuvem que possui nível de segurança mais baixo, pois está aberta a qualquer perfil de usuário que conheça a localização do serviço.

SEGURANÇA NA COMPUTAÇÃO EM NUVEM

A segurança da informação na nuvem são segredos comerciais, *know-how* técnico ou informações sobre clientes e preços são a base de muitas empresas. A protecção dessas informações é uma tarefa importante, sendo a principal preocupação a protecção contra perda e uso indevido de dados. Por essas razões, a protecção de informações confidenciais é de grande importância para proteger as corporações de danos económicos, sendo o objecto da segurança da informação (Barbieri, 2019).

Segurança da Informação

Segurança é firmeza, certeza, convicção, protecção contra possíveis atentados ou ataques a uma instituição ou personalidade. A Informação é um conjunto de dados, em princípio imprevisíveis, recebido do exterior ou por um ser vivo (especialmente o homem) por intermédio dos seus sentidos ou por uma máquina electrónica (Dicionário de Língua Portuguesa, 2003).

A segurança da informação, consiste na protecção dos activos (dados), desde a sua concessão, manuseamento ou processamento e armazenamento, sem interferência de terceiros com intenção maleciosa. Varella define a segurança da informação que, visa proteger o acesso ou modificação não autorizados de dados, ao mesmo tempo em que torna possível garantir que apenas usuários autorizados tenham acesso a esses. Esse conjunto de práticas de proteção são aplicadas tanto durante o armazenamento quanto durante a transmissão de um local físico para um virtual, ou vice-versa (Varella, 2019). Enquanto Laudon, define que, Segurança é um termo que compreende todas as ações desempenhadas junto às políticas, aos processos e às medidas técnicas para causar a restrição quanto ao acesso não autorizado, alterações, roubos ou danos físicos aos sistemas de informação (Laudon & Jane, 2011).

Segurança de TI, segurança cibernética ou segurança na Internet, todos esses termos vão na mesmadirecção, mas existem diferenças sutis. A segurança de TI é comumente definida como a proteção de sistemas de TI contra danos e ameaças, se estendendo desde o arquivo individual até computadores, redes, serviços em nuvem e data centers inteiros (Ferreira, 2015).

A segurança cibernética estende a segurança de TI a todo o espaço cibernético. Como a maioria dos sistemas está conectada à Internet, a segurança de TI e a segurança cibernética são frequentemente equiparadas, já que incluem todas as medidas técnicas e organizacionais para proteger os sistemas contra ataques cibernéticos e outras ameaças. Incluem, por exemplo, controles de acesso, criptografia, gerenciamento de direitos, *firewalls, proxies*, antivírus, gerenciamento de vulnerabilidades e muito mais. O termo segurança na Internet refere-se especificamente à proteção contra ameaças da Internet (Varella, 2019).

PRINCIPAIS TÓPICOS DE SEGURANÇA NA CLOUD COMPUTING

Nesta seção serão explicados com maiores detalhes os tópicos que mais impactam na segurança na cloud computing. Originalmente, a CSA (Cloud Security Alliance) dividiu a segurança na cloud em 15 itens. Para melhor entendimento, eles foram categorizados em três tópicos. São eles:

- Segurança tradicional
- Disponibilidade
- Controle de dados por terceiros

Segurança Tradicional

São as invasões ou ataques que se tornam possíveis, ou pelo menos mais fáceis de acontecer, quando um sistema é migrado para a nuvem. Os provedores de serviços na nuvem respondem dizendo que seus sistemas de segurança estão mais maduros do que de outras companhias. Outro argumento usado é que é mais eficiente garantir a segurança se controlada por um terceiro do que internamente, se o que preocupa as companhias são as ameaças internas. Além disso, é melhor garantir a segurança com contratos com provedores do serviço do que com formas tradicionais de segurança (Zanutto, s/d).

Ainda (Zanutto, s/d) afirma que as preocupações que concernem a este tópico são:

1. Ataque no nível de Máquina Virtual (VM-Level attacks. Potenciais vulnerabilidades no hypervisor ou tecnologia de virtualização de máquinas (VM) empregada pelos provedores de cloud com arquiteturas para múltiplos usuários. Vulnerabilidades aparecem no VMWare, XEN e Microsoft Virtual PC e Virtual Server. Os provedores usualmente garantem a segurança através do uso de firewalls e do monitoramento constante.

2. Vulnerabilidades do provedor da Cloud. São problemas a nível de plataforma, como SQL Injections ou scripts cross-site no salesforce.com. Mesmo o Google Docs, da Google, foi vítima desse tipo de ataque. Segundo a Google, não existe nada de novo no que diz respeito a esses ataques, apenas o contexto. Este tipo de ataque tem se tornado extremamente comuns ultimamente, alguns exemplos serão citados numa seção posterior. A IBM oferece sua ferramenta Rational AppScan, que procura por vulnerabilidades em web services como um serviço de segurança na nuvem.

3. Phishing de provedores de Cloud. Phising nada mais é do que se passar por alguém confiável (um site, por exemplo) para obter informações confidenciais como login e senha. Phishers e engenheiros sociais têm atacado através de phishing de provedores de Cloud, como os acontecidos com o Salesforce.com.

4. Superfície de Ataque a Rede Expandida. Diz respeito em como o usuário deve proteger a infraestrutura de comunicação com a nuvem, uma vez que esta geralmente estará do outro lado de um firewall.

5. Autenticação e Autorização. O framework de autenticação e autorização empresarial não se estende à cloud naturalmente. Como as companhias mesclam seus frameworks existentes para incluir os recursos da cloud? Além disso, como as empresas mesclam seus sistemas e métricas de segurança com os sistemas e métricas dos provedores de segurança da cloud (se houverem)?

6. Forense na Cloud. Em uma investigação forense tradicional, os investigadores levam em consideração o equipamento usado para recuperar os dados desejados. Em um sistema tradicional, a proporção de dados escritos, apagados e reescrito tem baixo impacto. Todavia, quando se pensa na cloud, tem-se uma escala muito maior, com os provedores de cloud rodando suas próprias infraestruturas multi-server.

Disponibilidade

Diz respeito a disponibilidade de serviços e dados críticos. Exemplos de incidentes neste quesito são a queda do Gmail em 2008 e do Amazon S3 também em 2008. Algumas falhas são indicadas segundo (Zanutto, s/d):

1. Uptime. Assim como com os tópicos de segurança tradicional, os provedores de Cloud afirmam estar seguros neste quesito, mais até do que um sistema de datacenters controlado pela própria empresa cliente. Além do risco de ter o serviço fora do ar, ainda existe o risco da nuvem não conseguir ser escalável para aplicações. O CEO da SAP, Leo Apotheker diz que certas coisas não devem ser colocadas na nuvem, pois esta pode entrar em colapso, como empresas que oferecem um serviço para 50 milhões de clientes.

2. Único Ponto de Falha. Os provedores de nuvem são geralmente vistos como tendo uma disponibilidade muito maior do que a de um sistema interno, mas isso pode não ser verdade, uma vez que existem mais de um ponto isolado de falha para ataques. Imaginemos a nuvem da Amazon. Um atacante que tente derrubar um dos serviços nela hospedado pode derrubar todo o servidor, logo derrubando também serviços "inocentes", que não eram originalmente alvos para o ataque.

3. Garantia de Integridade Computacional. Basicamente se trata de ter certeza que uma aplicação está em execução na nuvem e gerando resultados válidos. Como exemplo, o Folding@Home de Stanford realiza a mesma tarefa em múltiplos clientes e analisa o resultado que, espera-se, esteja em um consenso.

Controle de Dados por Terceiros

As implicações legais de dados e aplicações sendo mantidos por terceiros não são bem compreendidas e por vezes se torna algo complexo. Um risco quando dados são manipulados por terceiros é a falta de controle e a transparência. Uma das tendências da nuvem é permitir implementações de forma independente, mas isso vai contra conformidades regulamentares da cloud, que requerem transparência. Basicamente isso quer dizer que a mesma

transparência que facilita algumas coisas para os desenvolvedores, também os impede de ter um maior controle sobre seus dados. Com esses alertas, alguns provedores de Cloud estão começando a criar mais nuvens privadas a fim de evitar esses problemas e continuar usufruindo alguns dos benefícios da cloud. Como exemplo, Benjamin Linder, CEO da Scalent Systems, diz que na sua posição de CEO o que ele mais vê no mercado são empresas tendo dificuldades em confiar em nuvens externas com sistemas proprietários e de alta disponibilidade. Dessa forma, elas estão criando nuvens internas que atendam suas necessidades de forma maiscontrolada. Alguns problemas também são apontados quanto ao controle, segundo (Zanutto, s/d):

> 1. Por Diligência. Uma empresa contratante de serviço de nuvem é autuada judicialmente ou sofre outra acção legal. Ela pode contar com uma resposta do provedor da nuvem em tempo hábil? Uma questão relacionada é no que diz respeito à exclusão de arquivos da Cloud segundo políticas da empresa contratante. Ela tem garantias que o seu dado foi realmente excluído?
>
> 2. Auditabilidade. Problemas de auditabilidade são outro problema causado pela falta de controle da nuvem. Imaginemos uma empresa com seus dados e serviços na cloud. Existe transparência suficiente nas operações do provedor de cloud para que estes dados e serviços sejam usados a fim de auditoria? A revista Information Security Magazine coloca em questão como é possível fazer a auditoria de um sistema de uma organização quando este se encontra na nuvem, um ambiente distribuído e dinâmico com vários usuários, além da empresa auditada, e que pode estar distribuído por todo o globo? Isso torna difícil para os auditores comprovarem que os dados estão seguros e não podem ser a cessados indevidamente.

Uma preocupação relacionada diz respeito à administração de atividades na nuvem. É extremamente simples se tornar usuário da nuvem, às vezes mais do que deveria. Uma das principais diretrizes de auditoria é a SAS 70, que define diretrizes para auditores avaliarem controles internos, para controle de instâncias de processos de informações sensíveis. Algumas dessas diretrizes de auditorias exigem que os dados sejam processados em uma determinada localidade geográfica. As empresas provedoras de cloud estão respondendo a isto com ofertas de produtos “geolocalizados”, que garantem este requisito.

> 3. Obrigações Contratuais. Quando se usa a infraestrutura de uma outra empresa, é fato que estas não têm interesses comuns. Mas algumas exigências contratuais no uso da cloud são até mesmo impressionantes. Como exemplo, este trecho retirado das condições de uso da Amazon EC2, usado também por outros provedores como o OpSource Cloud: ” Não-afirmação. Durante e após o termo do acordo, com respeito a qualquer um dos serviços que você optar por usar, você não vai se valer de, autorizar, assistir, nem encorajará qualquer terceiro a afirmar contra nós ou contra qualquer um de nossos clientes, usuários finais, fornecedores, parceiros de negócios (incluindo vendedores de terceiros em websites operados por, ou em nosso nome) licenciados, sub-licenciados ou cessionários, qualquer violação de patentes ou outros alegando violação de propriedade intelectual com respeito a tais serviços”. Isso quer dizer que ao usar a EC2 da Amazon ou o OpSource, você não tem o direito de reivindicar a

patente de algo lá hospedado, se este vazar, acusando a Amazon ou qualquer um dos outros clientes da mesma. Até o momento, não se sabe da validade legal desse termo, mas o simples fato do mesmo existir não é um bom sinal para qualquer contratante que correria então o risco de ter uma patente violada.

4. Espionagem do Provedor da Cloud. Diz respeito à preocupação com roubo de dados proprietários da companhia por parte da empresa que provedora da nuvem. Exemplos disso são o Google Docs e o Google Apps. Ambos são serviços prestados por uma infraestrutura de nuvem fechada. Os usuários têm medo de confiar seus dados privados em nuvens assim, ainda que se trate de uma empresa gigante como a Google, como disse Shoukry Tiab, vice-presidente de TI da Jenny Craig, usuário do Postini e do Google Maps. Pelo menos neste caso, os usuários da nuvem chegaram ao consenso que o risco era bem menor do que os benefícios de se confiar dados privados na nuvem. Logo esta não é a maior preocupação hoje no que diz respeito à Cloud Computing.

5. Bloqueio de Dados (Data Lock-in). Como um usuário da nuvem evite que seus dados fiquem bloqueados em um provedor da nuvem? Um provedor pode armazenar seus dados em formatos proprietários diferentes dos outros, e quando o usuário pretende uma migração de provedor, encontra muita dificuldade. Imagine então o cenário de um provedor deixando de prestar seu serviço. Foi o que aconteceu na Coghead. A empresa anunciou que deixaria de prestar seus serviços e deu um intervalo de tempo realmente curto (em torno de dois meses) para desenvolvedores migrarem de seus sistemas. Uma saída simples para o bloqueio de dados, é a padronização, com uso de GoGrid API, por exemplo.

6. Natureza Transitiva. Uma outra preocupação de usuários da nuvem é a transitividade da mesma. É possível que um provedor do serviço terceirize algumas funções para outras empresas, deixando ainda menos controle para usuários. Como exemplo, imaginemos uma empresa que ofereça o serviço de cloud computing, mas esta empresa cuida apenas do processamento e da rede para os usuários, deixando o armazenamento pesado de dados para uma outra empresa. Um exemplo claro de problemas nessa área é um provedor chamado The Linkup. O The Linkup armazenada dados no Nirvanix. O The Linkup então fechou as portas após a perda de alguns dados, dados estes que estavam confiados ao Nirvanix. Outro exemplo de problema que se pode fazer disso é o uso de equipamento de outras empresas. Um provedor de cloud pode alugar equipamento de outra empresa. Foi o caso da Carbonite, que processou seu fornecedor de hardware após a perda de dados de usuários.

MAIORES AMEAÇAS DE SEGURANÇA EM COMPUTAÇÃO EM NUVEM

As maiores ameaças de segurança em computação em nuvem – (CSA, 2011) são as seguintes:

1. Violação de dados: Informações sigilosas podem ser violadas por meio dos recursos computacionais compartilhados da nuvem, viabilizando actividades de espionagem industrial e outras;

2. Perda de dados: Dados podem ser perdidos na nuvem por diversas razões como ataques de usuários maliciosos, equívoco do provedor de serviços de computação em nuvem, desastres naturais e outros;

3. Captura de Serviços: Serviços de computação em nuvem estão sujeitos a acesso não autorizado por meio da captura de credenciais, através de métodos de ataques que utilizam phishing, fraudes ou exploração de vulnerabilidades de software;

4. APIs e interfaces não seguras: APIs e Interfaces utilizadas para comunicação entre usuário e os serviços de computação em nuvem, assim como para comunicação entre diferentes serviços, estão sujeitas a problemas como interceptação, alteração e replicação de dados;

5. Negação de Serviços: O serviço de computação em nuvem é forçado a consumir grandes quantidades de recursos (e.g., processador, memória, banda de rede,etc.), diminuindo sua capacidade de resposta do provedor e impedindo usuários acessarem seus dados e aplicações;

6. Usuário autorizado malicioso: Usuários com acesso aos recursos de computação em nuvem (e.g., funcionário ou parceiro do provedor de serviços) podem reduzir a qualidade do serviço prestado por meio de acções mal intencionadas;

7. Abuso dos serviços de nuvem: Utilização dos serviços oferecidos pelo provedor de computação em nuvem para fins maliciosos, como ataques distribuídos de negação de serviços, quebra de senhas e distribuição de malwares e softwares piratas;

8. Insuficiência por falta de diligência: Organizações fazem uso de serviços de computação em nuvem sem possuir o conhecimento necessário dos riscos envolvidos, aumentando, assim, a vulnerabilidade de seus dados e aplicações;

9. Tecnologias de compartilhamento: Nem todas as tecnologias empregadas no compartilhamento de recursos, como infraestrutura computacional, plataformas e aplicações, foram projetadas para prover o isolamento necessário entre os múltiplos usuários dos serviços prestados;

A CSA estabelece ainda treze áreas críticas de segurança a serem consideradas na implementação e implantação de serviços de computação em nuvem agrupando essas áreas em três grandes domínios de segurança que abrangem o projecto, a gestão e a operação de serviços (CSA, 2011).

CONSIDERAÇÕES FINAIS

Se considera que:

1. A Computação em Nuvem, precisa 100% de Internet, para que se tenha os serviços do provedor e do cliente em pleno funcionamento;

2. A segurança em nuvem, não é absoluta, mas, as empresas, devem estar preparadas para adesão aos serviços da nuvem a qualquer momento, porque é a exigência do século;

3. Com a adesão a nuvem, as empresas diminuem o custo com equipamentos e aumentam a disponibilidade dos serviços a qualquer hora e lugar, desde que, tenha internet, que é um dos elementos fundamentais. Uma certeza, as empresas devem ter capacidade de custear os serviços de internet, para evitar indisponibilidade dos serviços em nuvem;

4. Os provedores dos serviços de nuvem, estão preparados para qualquer risco de segurança, física ou virtual, que possa ocorrer nos seus serviços. Elas investem com equipamentos e softwares de última geração para evitarem danos incontroláveis;

5. As Empresas (Clientes) antes de aderirem a nuvem, devem de facto, certificar a idoneidade da empresa fornecedora dos serviços, e se é possível, contratar um especialista particular para analisar o processo de adesão.

REFERÊNCIAS BIBLIOGRÁFICAS

Andrei Braga, G. S. **Cloud Computing**. Obtido em 2022, de https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/fernando/bibliografia.html, s/d.

Barbieri, C. **Governança de Dados:** Práticas, conceitos e novos caminhos. São Paulo, 2019.

Barros, I. N. **Proteção de Dados na Computação em Nuvem**. Obtido de https://comum.rcaap.pt/bitstream/10400.26/39868/1/99991908_Inoc%C3%AAncio_Barros.pdf, 2021.

Center, I. I. **Infraestrutura de Nuvem Privada Como Serviço**. Obtido em 2023, de https://www.intel.com.br/content/dam/www/public/lar/br/pt/documents/articles/iaas-cloud-pg-v1b-web-por.pdf, 2014.

CSA. **Security guidance for critical areas of focus in cloud computing**. Obtido de https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf, 2011.

Dicionário da Língua Portuguesa. Porto: Porto Editora, 2003.

ENISA. **Cloud Computing:** Benefits, Risks and Recommendations for Information, 2011.

Ferreira, A. M. **Introdução ao Cloud Computing**. IaaS, PaaS, SaaS, Tecnologia, Conceitos e Modelos de Negócio. São Paulo, 2015.

Jean Dias, R. R. **Segurança de Dados na Computação em Nuvem das Pequenas e Médias Empresas**. Obtido em 2023, de file:///C:/Users/Angola%20Livre/Downloads/287-862-1-PB.pdf, 2012.

Koslovski, C. C. **Análise de Segurança para Soluções de Computação em Nuvem**. Obtido de https://www.researchgate.net/publication/283274571, 2014.

Laudon, K. & Jane, L. **Sistemas de informação gerenciais**. São Paulo, 2011.

NIST. **Estrutura de Segurança Cibernética**. Obtido de https://d1.awsstatic.com/whitepapers/pt_BR/compliance/NIST_Cybersecurity_Framework_CSF.pdf, 2019.

Nogueira, P. P. **Computação em Nuvem**. Obtido em 2023, de https://ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G04-095352-120531-t2.pdf, s/d.

Silva, S. G. **Formulação de indicadores de SLA para monitoramento de Serviços de Computação em Nuvem**. Obtido de http://seer.uniacademia.edu.br/index.php/cesi/article/viewFile/1936/2257, 2022.

Varella, W. A. **Arquitetura de solução de computação em nuvem**. São Paulo: Editora Senac, 2019.

Zanutto, B. G. **Segurança em Cloud Computing**. Obtido de https://www.dcomp.ufscar.br/verdi/topicosCloud/Artigo-Seguranca-Cloud.pdf, s/d.

Anildo Joaquim da Silva

Professor da Faculdade de Engenharia e Tecnologias. Universidade Gregório Semedo. Luanda-Angola. Mestrando em Engenharia Informática, na Especialidade de Gestão de Redes de Computadores e Sistemas de Comunicação.

E-mail: anildosilva2014@gmail.com

ORGANIZAÇÃO:
Manuel Francisco Neto
Vilma Maria da Silva

AUTORES(AS):
Anildo Joaquim da Silva
Isabel Delfina Casimiro e Luís Venâncio
Jucélia Maria do Nascimento
Jucira Moura Vieira da Silva
Juliana Godoi Marques
Leidimar Martins da Rocha Almeida
Leila da Silva Siqueira
Luciana Mendes do Rego
Marlene da Silva
Patrícia Mendes Cavalcante de Souza
Rita de Cássia Martins Serafim
Vera Lucia Meneses de Lima Marques
Viviane de Cássia Araujo

ISSN 2675-2573
38
9 772675 257003

https://doi.org/10.52078/issn2673-2573.rpe.38

Produzida com utilização de softwares livres

FREE SOFTWARE FOUNDATION
debian
LibreOffice
Platform & workflow by OJS / PKP

www.primeiraevolucao.com.br

ABEC BRASIL Associação Brasileira de Editores Científicos
doi
Crossref
OJS OPEN JOURNAL SYSTEMS
CiteFactor Academic Scientific Journals
Google Acadêmico