FACULDADE DE TECNOLOGIA DE SÃO PAULO

Kaique Volpi Rosseto

CLOUD COMPUTING SECURITY

Desvendando e entendendo a proteção de nossos dados

São Paulo

2022

FACULDADE DE TECNOLOGIA DE SÃO PAULO

KAIQUE VOLPI ROSSETO

CLOUD SECURITY

Desvendando e entendendo a proteção de nossos dados

Trabalho submetido como exigência parcial para a obtenção do Grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Orientador: Professora Edmea Pujol Canton

São Paulo

2022

FACULDADE DE TECNOLOGIA DE SÃO PAULO

KAIQUE VOLPI ROSSETO

CLOUD COMPUTING SECURITY

Desvendando e entendendo a proteção de nossos dados

Trabalho submetido como exigência parcial para a obtenção do Grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Parecer do Professor Orientador:

O Trabalho de Conclusão de Curso do aluno Kaique Volpi Rosseto atendeu a todas as exigências do Departamento de Tecnologia da Informação.

Conceito/Nota Final: 10 (Dez inteiros)

Orientador: Professora Edmea Pujol Canton

São Paulo, 25 de Junho de 2022.

Assinatura do Orientador

Edmea Pujol Cantón

Assinatura do aluno

Kaique Volpi

Dedico esta monografia a minha mãe, Mônica Luzia Volpi Rodrigues, por sempre lutar por mim e me incentivar em tudo que tentei fazer.

Sem você, não chegaria aonde cheguei.

Muito obrigado.

Agradecimentos

Gostaria de agradecer e dedicar esta dissertação às seguintes pessoas:

Minha Família minha mãe Mônica Volpi, meu pai Anderson Rosseto, meu padrinho e tio Douglas Rossetto, e ao meu amigo Gabriel Nascimento Rocha, por sempre estarem comigo e me ajudarem a chegar até aqui.

Minha orientadora Prof. Edmea Pujol Canton.

“Só se pode alcançar um grande êxito quando nos mantemos fiéis a nós mesmos.”

(Friedrich Nietzsche)

RESUMO

O conceito de cloud vem se difundindo no mercado e na cabeça das pessoas. Todo dispositivo adquirido hoje em dia, vem com ofertas de serviços de cloud de várias empresas, cada conta criada temos a opção de contratar um armazenamento.

As últimas evoluções apontam para deixarmos de ter grandes armazenamentos locais no dispositivo e acessar tudo via cloud, e isso tem sido visto com bons olhos, então as pessoas estão usando massivamente estes serviços. Quando aceitamos e contratamos um serviço de cloud, estamos concordando que todos os nossos dados pessoais, imagens, arquivos e até senhas, saiam do nosso dispositivo, que em teoria temos o controle e está literalmente em nossas mãos, e vão para um servidor externo, muitas vezes até fora do nosso país, para ficar sob responsabilidade da empresa à qual estamos contratando, e consequentemente, confiando nossas informações.

Muito se fala hoje sobre armazenamento em nuvem, e se enxerga como o futuro da computação, mas será que sabemos de fato como isso funciona, o que é, e principalmente o quão seguros estamos ao usar esta tecnologia?

Neste trabalho de conclusão de curso, abordaremos o conceito de cloud computing e quão seguros estaremos ao inserir nossos dados em um serviço deste tipo.

Palavras-chave: Cloud, Computação, Serviço, Segurança, Informação.

ABSTRACT

The concept of cloud has been spreading in the market and in people's minds. Every device purchased today comes with cloud service offerings from various companies, each account created has the option of hiring a storage.

The latest developments point to us no longer having large local storage on the device and accessing everything via the cloud, and this has been seen with good eyes, so people are massively using these services. When we accept and contract a cloud service, we are agreeing that all our personal data, images, files and even passwords, leave our device, which in theory we have control and is literally in our hands, and go to an external server, many times even outside our country, to be under the responsibility of the company to which we are hiring, and consequently, entrusting our information.

Much is said today about cloud storage, and it is seen as the future of computing, but do we really know how it works, what it is, and especially how safe we are when using this technology?

In this final paper, we will approach the concept of cloud computing and how safe we will be when inserting our data in a service of this type.

Keywords: Cloud, Computing, Service, Security, Information.

Lista de siglas

ABNT	-	Associação Brasileira de Normas Técnicas
ISO	-	International Organization for Standardization
SaaS	-	Software as a service
IaaS	-	Cloud System Infrastructure Services
PaaS	-	Cloud Application Infrastructure Services
BPaaS	-	Cloud Business Process Services
DaaS	-	Desktop as a Service
MIT	-	Massachusetts Institute of Technology
ERP	-	Enterprise Resource Planning (Sistema de gestão empresarial)
LGPD	-	Lei Geral de Proteção de Dados
MFA	-	Multiple Factor Authentication
FEBRABAN	-	Federação Brasileira de Bancos
VPN	-	Virtual Private Network

Lista de Figuras

Lista de quadros

Sumário

INTRODUÇÃO

Contextualização Histórica

Apesar de começar a ser fortemente difundido recentemente, o conceito de nuvem é algo que já está presente, ao menos, no imaginário de especialistas desde os aos 50 e 60. Nesta época, algumas empresas já se utilizavam de um conceito que é considerado como o primórdio da nuvem, as máquinas de alto desempenho para o processamento de uma grande quantidade de dados serem muito caras, portanto, algumas empresas utilizavam um sistema onde existia uma máquina principal como o Mainframe processando a grande quantidade de dados, e os funcionários acessavam os dados através de estações conectadas a este mainframe.

Nos anos 60, este conceito foi ganhando forma, quando John McCarthy, que é conhecido como o pai da Inteligência Artificial, devido ao seu projeto mais notável, a linguagem LISP (List Processor), linguagem baseada em listas vinculadas, fortemente difundida e utilizada em projetos de Inteligências Artificiais, e nesta época, McCarthy começou a discutir e elaborar um conceito que ele mesmo batizou de “Utility Computing”. Onde a ideia principal eram dois ou mais usuários acessarem um computador de forma simultânea, com uma proposta também chamada por ele de “time-sharing”, esta ideia foi apresentada por McCarthy no MIT em 1961. (IPM sistemas blog, 2020).

Esta ideia de Utility computing, foi endossada por um importante órgão americano, o ARPANET (Advanced Research Projects Agency Network), em projeto que teve ajuda fundamental de Joseph Carl Robnett Licklider, que em 1962, por coincidência ou não também no MIT, falava sobre a criação de uma rede intergaláctica de computadores, no sentido de interligar computadores através de uma rede, independentemente de onde estão fisicamente, e foi seguindo esta linha de ideias que anos mais tarde, em 1969, o ARPANET criaria a Internet, se tornando a primeira rede que permitiu o compartilhamento de informações entre computadores sem estarem no mesmo, local físico. (IPM sistemas blog, 2020).

Portanto, podemos afirmar que as ideias de McCarthy influenciaram diretamente no conceito de internet e cloud que vemos hoje, que em síntese, buscam oferecer duas funcionalidades: disponibilidade e acessibilidade.

Apesar de toda ideia já estar no imaginário dos profissionais desde os anos 60, foi apenas a partir dos anos 90 que cloud começou a tomar a forma na qual vemos hoje, onde algumas empresas começaram a investir na criação de redes virtualizadas, com o objetivo de fornecer aos seus funcionários acesso compartilhado a mesma infraestrutura de servidor físico. A ideia era simples, existia um grande datacenter físico, e as outras estações acessavam este ambiente de forma virtualizada, como pode ser observado na FIGURA 1.

Figura 1 - Representação da virtualização de redes
Fonte: Redes & Servidores, Rui Natário, 2013.

Os datacenters foram úteis durante um certo tempo, porém, se provaram ineficientes a longo prazo, entrando em desuso durante os anos 90, mas na virada do século, por falta de alternativas, voltou com tudo. Isso trouxe consequências, em 2002 os datacenters consumiam cerca 1,5% da energia gerada em todo o território dos Estados Unidos, e com uma ordem de crescimento anual de 10%, se fez necessário buscar solucionar este problema. (Rui Natário, 2013)

O principal problema era o fato de a indústria ter se moldado a produção barata até aquele momento, produzindo quase toda a estrutura baseada na arquitetura x86, que se provou ineficiente e subutilizados para virtualização, fazendo com que fosse necessária uma quantidade muito alta de máquinas e consequentemente energia e arrefecimento.

Até que, em 1998 a VMWare consegue mudar esse panorama, resolvendo o problema da virtualização de sistemas x86, abrindo o caminho para a consolidação deste sistema de servidores e possibilitando que as empresas que investissem neste método, criassem uma infraestrutura de TI sustentável.

A partir daí, cloud começou a ganhar mais força, e começam a estourar os serviços SaaS, em 1999 a Salesforce lança a primeira aplicação empresarial web, abrindo o caminho para que as aplicações cloud ganhassem força comercialmente, poucos anos depois a Amazon começa a oferecer serviços de aluguel de computadores em nuvem, posteriormente, em 2008, a Google e um ano depois a Microsoft. Porém, pouco antes destes investimentos, nem mesmo o termo era conhecido e se dividiam as nomenclaturas de como chamar este serviço, até que, segundo Taurion (2009), o termo computação em nuvem foi apresentado em 2006, por Eric Schmidt, presidente da Google até hoje, em uma palestra onde explicava a forma como a Google gerenciava seus datacenters.

Contexto atual

Desde então, o mercado cresceu muito, segundo pesquisas da empresa norte-americana Gartner, Inc. (2022), o gasto anual de usuários com nuvem em 2021 foi de 410,9 bilhões de dólares e se estima um crescimento de 20.4%, atingindo a incrível marca de 494,7 bilhões no ano de 2022, dados que podem ser observados no QUADRO 1.

Quadro 1 – Previsão de gastos do usuário final de serviços de Nuvem Pública mundial (em bilhões de dólares)

	2021	2022	2023
Processos de Negócios como Serviços (BPaaS)	51,4	55,5	60,6
Aplicações de Plataforma como serviço (PaaS)	86,9	109,6	136,4
Software como Serviço (SaaS)	152,1	176,6	208
Serviços de gerenciamento e segurança de Nuvem	26,6	30,4	35,2
Infraestrutura como serviço (IaaS)	91,6	119,7	156,2
Desktop como Serviço (Daas)	2	2,6	3,2
Total	**410,915**	**494,654**	**599,840**

Fonte: Gartner, 2022.

Segundo este estudo o maior crescimento porcentual está nos serviços de IaaS, o que vai de encontro com a ideia de que as empresas estão se modernizando e se estruturando para colocar todos os seus dados em nuvens, principalmente com a nova realidade do trabalho híbrido ou 100% remoto do mundo pós-pandemia, faz-se necessário uma infraestrutura nas empresas em que os funcionários sejam capazes de acessar de qualquer lugar. Este mesmo motivo deve impulsionar os serviços DaaS, pois atualmente muitas empresas, em sua maioria consultorias, estão deixando de ter estações físicas e fornecendo acessos à serviços DaaS aos seus funcionários, e a tendência é que grandes organizações façam o mesmo.

Na divulgação deste estudo, Sig Nag, Vice-Presidente de Pesquisa da Gartner, vê Cloud como a "Potência que impulsiona as organizações digitais hoje" (traduzido pelo autor), e complementa com a visão de que o mercado além de inchado, está cada vez mais competitivo, uma vez que com tantas opções, a tomada de decisão sobre qual empresa contratar para estes serviços se tornou peça crucial para o negócio da empresa.

Em nosso contexto local, a partir de 2018 com a aprovação da LGPD[1], o contexto entrou na pauta em todas as empresas, todos passaram a se planejar para se adequar ao novo cenário, e com a lei entrando em vigor em 2021, a pauta está mais quente do que nunca, e já inserida no dia a dia das empresas, que em sua maioria tiveram grandes projetos para se adequar a ela, e ainda segundo pesquisa realizada pela ABNT(2021) em parceria com consultorias e a Privacy tools, apenas 1 em cada 10 empresas acredita ter se adequado 100% à lei até 2021.

Além do âmbito de negócio, cloud no contexto atual é algo muito difundido para o uso pessoal, porém, de uma forma diferente. Nas organizações a palavra é Cloud Computing, virtualizar o processamento e tornar os processos mais eficientes, já para uso pessoal, usamos muito também o Cloud Storage[2], estamos armazenando nossos dados em nuvem. Assim que criamos um e-mail em uma organização como por exemplo o Google, além de todas as mensagens que trocamos neste e-mail já estarem na nuvem do google, recebemos uma quantidade de armazenamento no Drive para nossos arquivos pessoais, isso ocasiona que, quando possuímos um celular com o sistema operacional android, por exemplo, automaticamente vinculamos o e-mail no aparelho e as fotos, vídeos, músicas, conversas em aplicativos de mensagens, ficam nesta nuvem também. E o mesmo acontece com a Apple e Microsoft com seus serviços de nuvem.

Segundo estudo da Cloud Awards, quando falamos de cloud como um todo, pelos dados de Market Share em 2021, a maior companhia em serviços de cloud é a

---

[1] A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A Lei fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado. (Governo federal, 2018)

[2] É o armazenamento na nuvem, um modelo de computação em nuvem que armazena dados na Internet por meio de um provedor de computação na nuvem, que gerencia e opera o armazenamento físico de dados como serviço. (Amazon AWS, 2019)

Amazon, os serviços AWS tomam cerca de 31% do mercado, seguido pela Microsoft, com 20% do mercado para os serviços Azure, o Google cloud somente em terceiro com 7%. Porém, quando falamos de uso pessoal de cloud storage a situação é bem diferente, o Google Drive é disparado o mais utilizado, com 94% das pessoas utilizando ou tendo uma conta no Drive, seguido de longe pelo Dropbox e o OneDrive Microsoft somente em terceiro.

O uso pessoal não fica somente em storage, estamos constantemente usando cloud como usuários finais e muitas vezes não sabemos, mas um mercado que se tornou muito lucrativo nos últimos anos foi o mercado de *video streaming,* que em 2021 já movimentava 59,14 bilhões de dólares, e tem uma projeção de crescimento anual de 21%. Portanto, estamos fazendo uso de serviços de cloud ao usar serviços como Netflix, Disney+, HBO Max etc.

Outro mercado que vem ganhando espaço no segmento de Cloud, é o Cloud Gaming, funcionando de uma maneira semelhando aos streamings de vídeos, porém para jogar video game, ao invés de comprar um console físico, podemos contratar um serviço para acessar e jogar de qualquer dispositivo. O mercado já é milionário e, segundo pesquisa de 2021 da Cloud Awards, deve entrar na casa dos bilhões até 2025, este mercado que, sendo difundido, pode mais uma vez através de serviços de cloud, mudar a forma pela qual consumimos um tipo de entretenimento e até com a venda de aparelhos físicos de consoles de video games. Provando que serviços clouds estão profundamente presentes no dia a dia das pessoas e empresas.

Apresentação do Problema

Tendo em mente que 94% das pessoas hoje usam ao menos algum tipo de serviço de cloud para seus dados e arquivos pessoais e o investimento bilionário das empresas para virtualizar suas máquinas e capacidade computacional, nos tornamos cada vez mais dependentes destes serviços que estão hospedados em algum lugar, que na maioria das vezes, não sabemos onde.

Se temos tantos dados e empresas inteiras nas mãos destas empresas, o quanto esta empresa pode me garantir que meus dados estão seguros? O que impede que um hacker invada os servidores e derrube meu serviço ou tenha acesso aos meus dados? A empresa tem acesso aos dados que estou armazenando na nuvem dela? Quais os protocolos de segurança, a que tipos de ataques estamos sujeitos e que

cuidados devemos tomar ao subir arquivos pessoais e íntimos para estas plataformas?

Recentemente, no início de 2021, tivemos o maior vazamento de dados da história, um arquivo com cerca de 40 milhões de CNPJs, 223 milhões de CPFs e 104 milhões de dados de veículos esteve circulando na darkweb[3]. com as informações de score e classificação, facilitando para atividades ilícitas como fraudes e estelionatos. (Tecnoblog, 2021).

Este cenário gerou muita insegurança das empresas, visto que o Brasil é um dos países que mais sofre ataques aos dados, segundo pesquisa divulgada pela F5 labs, em 2021, fazendo com que a nuvem se tornasse, ainda mais, a grande solução em segurança para os ERPs das empresas, mas, esta é mesmo a solução? Estamos seguros só pelo fato de colocar nossos dados em nuvem, e como escolher a melhor nuvem? Todas são seguras?

E principalmente, que riscos estamos correndo quando não migramos para o armazenamento em nuvem e nos mantemos com armazenamento em servidores e dispositivos locais.

Objetivo Geral

Entender como é feito o armazenamento dos dados em nuvem, o que a empresa que hospeda os seus dados faz e como ela protege seus dados de ataques, a fim de entender o porquê do uso de cloud deixar de ser uma opção tanto para uso pessoal quanto para uso empresarial, ajudando a saber escolher o melhor fornecedor para estes serviços.

Objetivos específicos

Sabendo do crescente uso de cloud tanto nas empresas quanto no âmbito pessoal, precisamos entender o porquê isso aconteceu e se isso é seguro, portanto, foram definidos 3 objetivos específicos:

1) Entender como funciona a segurança dos dados na nuvem, com as práticas usadas pelos principais fornecedores.

[3] A Dark Web é o coletivo oculto de sites da Internet que só podem ser acessados com um navegador de Internet especializado. Ela é usada para manter atividades anônimas e privadas na Internet, algo que pode ser útil em contextos legais e ilegais. (Kaspersky, 2022)

2) Mostrar as diferenças de segurança em comparação com o armazenamento local.
3) Ajudar a tomar a melhor decisão no momento de migrar seus dados para nuvem, conscientizando as pessoas sobre os cuidados necessários.

Justificativa

No cenário atual, o uso de cloud deixou de ser uma opção, todo mundo usa de alguma forma, seja na empresa que trabalha, quando cria um conta de e-mail para o seu novo smartphone, no seu próprio negócio, para salvas suas fotos, suas conversas do aplicativo de mensagens, assinando um serviço de streaming etc. Dito isso, existem pessoas que nem mesmo sabem que estão usando cloud a maior parte do tempo.

Segundo report realizado pela ESET em 2021, os ataques mais realizados atualmente, são os de engenharia social, através de phising[4]. e outros métodos, portanto, uma noção de educação ao usuário sobre a segurança, se tornou parte fundamental de qualquer infraestrutura de segurança.

Portanto, se torna essencial que todos entendam onde estamos colocando os dados de nossas empresas e nossos arquivos pessoais, e que tipo de segurança estes fornecedores têm a oferecer.

O uso de armazenamento e computação em nuvem só tende a aumentar nos próximos anos, e vai se tornar, cada vez mais, essencial que todos saibam, como funciona, e avaliar os serviços oferecidos para tomar a melhor decisão para proteger seus dados pessoais e da sua empresa.

[4] O phishing é um dos golpes mais antigos e conhecidos da internet. Podemos definir phishing como qualquer tipo de fraude por meios de telecomunicação, que usa truques de engenharia social para obter dados privados das vítimas. (Avast, 2022)

1. SEGURANÇA EM NUVEM

Quando falamos de segurança em nuvem, temos um grande mistério sobre como funciona e uma ideia da maioria das pessoas que a segurança já vem pronta e que simplesmente é mais seguro, porém, para montar e cuidar de uma infraestrutura em nuvem, temos 5 pilares para seguir.

1.1. Métodos

Estes pilares podem ser entendidos como os métodos para uma boa segurança em cloud, em resumo, as boas práticas para garantir que nossos dados estão seguros.

1.1.1 Educação do usuário

Como podemos observar na FIGURA 2, a base da pirâmide dos pilares de cyber segurança em nuvem é a Educação do usuário.

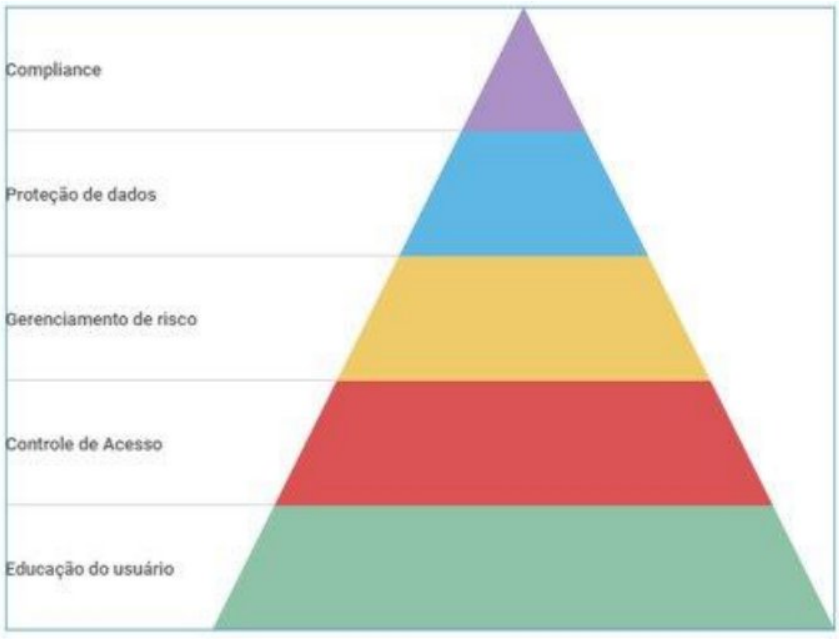

Figura 2 - 5 pilares da segurança em cloud
Fonte: HSBS, 2021.

Nos últimos anos, os ataques mais comuns foram os de engenharia social, segundo o diretor da Comissão executiva de prevenção a Fraudes da Febraban (Federação Brasileira de Bancos) (2020), Adriano Volpini, “70% dos golpes do mundo cibernético hoje estão relacionados a engenharia social”, portanto, a base da nossa pirâmide é a educação ao usuário, ataques de phishing estão cada vez mais comuns

nas organizações, assim como os treinamentos de como se prevenir e identificar um e-mail ou mensagem de phishing, não usar senhas simples ou compartilhar senhas entre diferentes colaboradores, a educação do usuário é peça fundamental, tanto dentro da empresa quanto para a vida pessoal deste funcionário.

1.1.2 Autenticação em múltiplos fatores (MFA)

O segundo pilar é o controle de acesso, o que nos leva diretamente para o primeiro método que vamos conhecer, a autenticação em múltiplos fatores.

Hoje em qualquer uma das grandes fornecedoras de serviços em cloud, como a Microsoft, AWS etc., já possui o controle do acesso via MFA, o que faz com que nós já estejamos mais ambientados sobre o que é. As autenticações ou formas de login convencionais partem que para você provar que você é você, é necessário fornecer algo que você sabe: suas credenciais. No caso de um login via MFA, é necessário que você comprove isso com algo a mais: Algo que você é, como por exemplo reconhecimento facial ou biometria, ou então algo que você tem, como um smartphone para receber um Token ou um acesso a um e-mail seguro, onde este token será enviado. Isso cria ao menos uma camada a mais de segurança, dificultando as invasões, uma vez que apenas descobrir a senha não é suficiente, e com este método, programas de quebrar senhas, por exemplo, não funcionam.

Ao contratar os serviços da Microsoft Azure, por exemplo, existem vários métodos de MFA para serem escolhidos, com entre 2 e 4 camadas de autenticação, explicados no QUADRO 2:

Quadro 2 - Métodos de Autenticação Microsoft Azure

	Segurança	Usabilidade	Disponibilidade
Windows Hello for Business	Alto	Alto	Alto
Aplicativo Microsoft Authenticator	Alto	Alto	Alto
Chave de segurança FIDO2	Alto	Alto	Alto
Tokens de hardware OATH (versão prévia)	Médio	Alto	Alto
Tokens de software OATH	Médio	Médio	Alto
SMS	Médio	Alto	Médio
Voz	Médio	Médio	Médio
Senha	Baixo	Alto	Alto

Fonte: Microsoft, 2022.

1.1.3 Gestão Partilhada de Risco

Como mencionamos anteriormente, a base da segurança na nuvem é a educação do usuário, partindo deste pressuposto, outro pilar importante é a gestão dos riscos, que no caso de Cloud Security, o modelo adotado pelas empresas é o da gestão partilhada. Na FIGURA 3, podemos observar uma rápida comparação do modelo de responsabilidade compartilhada entre serviços locais ou On-Prem, e os diferentes serviços de cloud.

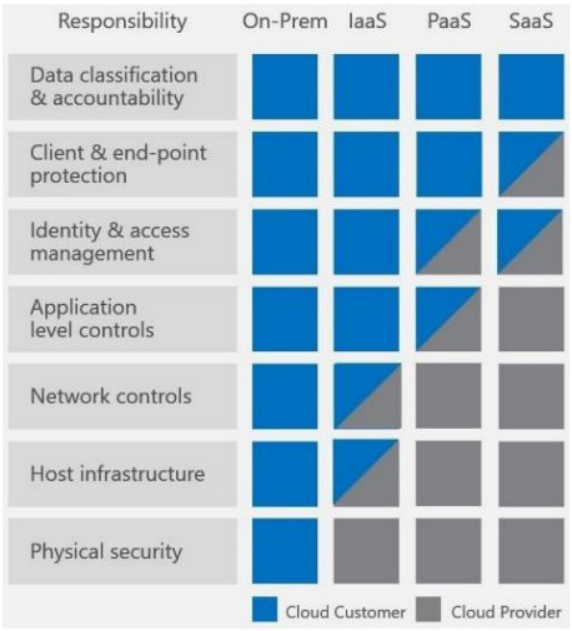

Figura 3 – Responsabilidade Partilhada para Cloud Computing
Fonte: Microsoft, 2019.

Podemos notar que, independentemente do modelo adotado, a classificação dos dados é de responsabilidade do cliente, porém, quando adotamos um modelo de cloud, o fornecedor passa a ter mais responsabilidades, ou seja, temos menos preocupações. Importante notar que, a gestão dos acessos é sempre minimamente compartilhada, nunca de total responsabilidade do fornecedor, ressaltando mais uma vez a questão do controle do acesso aliada à educação do usuário.

1.1.4 Proteção de dados

Outra grande dúvida da maior parte dos usuários finais, é como funciona a proteção de nossos dados na nuvem, e a resposta pode ser simples ou mais complexa, dependendo de qual pergunta estamos fazendo. Para a mais simples que já cheguei a ouvir algumas vezes: A empresa que está fornecendo os serviços de nuvem pode ter acesso aos dados que estou armazenando nos servidores deles? A resposta pode seguramente ser: Não.

Ao menos as empresas maiores, oferecem criptografia de ponta a ponta para os seus dados, e inclusive podemos consultar qual o tipo de criptografia utilizada no site destas empresas.

Para garantir que uma empresa é idônea e confiável aos seus dados, existem algumas certificações oferecidas pela ISO (Organização Internacional de

Normalização) que garantem que podemos confiar nossos dados a este fornecedor: ISO 27001 que trata da gestão de Segurança da Informação, ISO 27017 que trata da própria segurança em Nuvem, ISO 27018 que trata da Privacidade na nuvem e proteção de dados e ISO 27701 que trata da Gestão de informações de privacidade. Todas as empresas que citaremos aqui, possuem todas estas certificações, e isso pode ser consultado nos sites das fornecedoras.

Reunimos alguns dos mais famosos: Na Microsoft Azure possuímos dois protocolos de criptografia para os seus dados: Quando os dados estão em repouso, ou seja, sem estarem sendo acessados através da nuvem, caímos novamente no conceito de responsabilidade compartilhada visto anteriormente, o cliente pode escolher o protocolo que será utilizado para criptografar seus dados e suas VMs, e utilizar o Azure Key Vault (Cofre de senhas da Azure) para guardar as suas chaves de criptografia, e esse gerenciamento fica por responsabilidade do cliente.

No caso dos dados em trânsito, seja pela rede interna da Azure ou pela internet para chegar ao usuário final, seus dados estão sendo protegidos pelo protocolo de criptografia TLS 1.2 ou superior, e autenticação via IPsec ou SBM, que são os protocolos de ponta utilizados hoje em dia no mercado. Já no caso do Google Drive, garante utilizar chaves AES de 256 bits para criptografia de dados em trânsito e em repouso, que é uma criptografia de ponta, em nível militar. Enquanto a Dropbox, afirma em seu site realizar a criptografia de ponta-a-ponta em conformidade com as normas ISO, e dividir cada arquivo em blocos, com diferentes chaves, para aumentar a segurança.

Outro método de proteção, é como os dados estão protegidos de ataques externos. Além das criptografias de ponta, os serviços de nuvem podem ser protegidos por firewalls, permitindo autenticação apenas aos IPs autorizados ou via VPN.

O indicado é o uso de um firewall do tipo FwaaS, representado na imagem da FIGURA 3, o Firewall como serviço, executado dentro da nuvem, associado a uma VPN do tipo SSTP[5] ou superior.

[5] Secure Socket Tunneling Protocolos, VPN baseada em SSl para obter acessos à maioria dos firewalls, através da porta TCP 443. (Microsoft, 2022).

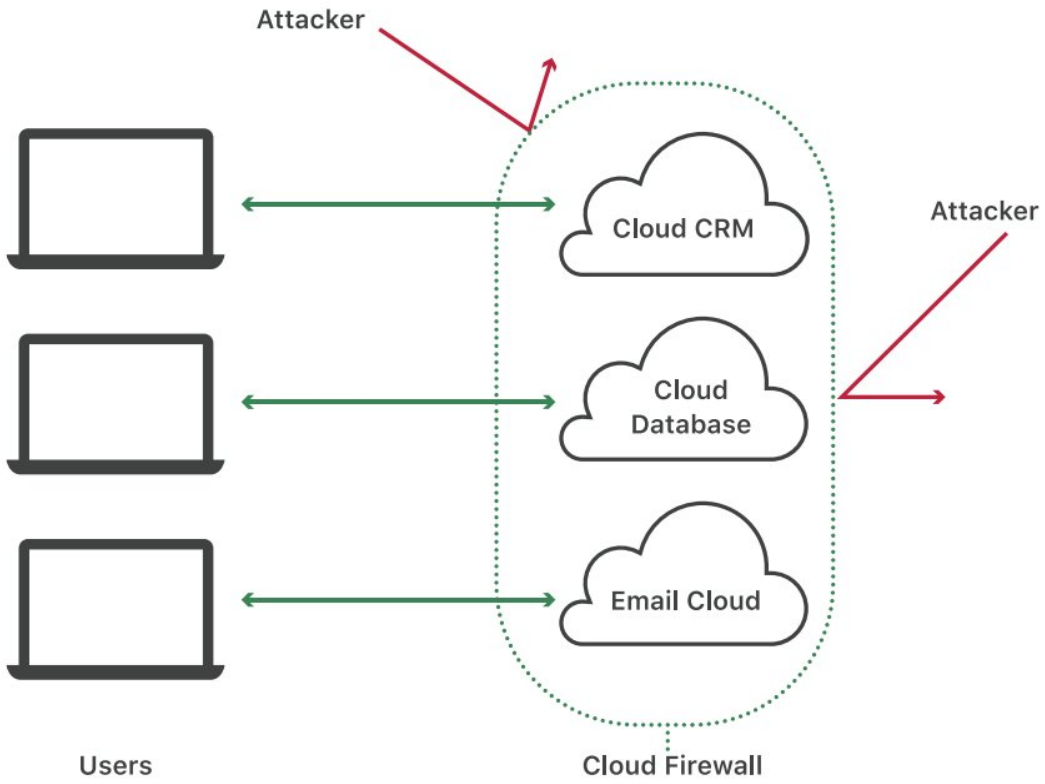

Figura 3 - Modelo de Cloud Firewall
Fonte: Cloudflare, 2021

1.1.5 Compliance

O quinto e último pilar é o Compliance, basicamente estar dentro de todas as normas e padrões estabelecidos, olhando para o Brasil em uma visão do lado da empresa, precisamos estar em conformidade com a LGPD, e no cenário global, temos as normas ISO mencionadas no tópico anterior, e para além disso, temos os relatórios SOC (Service Organization Control), a certificação PCI DSS (Payment Card Industry – Data Security Standard), sobre o padrão internacional de segurança de dados para a indústria de cartões, o relatório SOC 1 é voltado a controles financeiros e ainda temos o SOC 2 e SOC 3, voltados para a segurança, integridade e eficácia dos sistemas.

Ainda existem outras conformidades aos protocolos de segurança de agências nacionais como a americana FedRAMP e a do Reino Unido UK OFFICIAL, e de empresas privadas relevantes como a HITRUST.

Mas, por que estas certificações são importantes? Além da confiabilidade que a empresa passa a quem está se hospedando nesta nuvem, implementar sua infraestrutura em um fornecedor com estas certificações, significa que a sua infraestrutura também as possuirá, o que significa mais confiabilidade e credibilidade para os seus clientes, isso é possível através de ferramentas como o Azure Blueprint, que possibilita habilitar uma função de desenvolvimento dentro das conformidades das certificações desejadas, adequando o seu ambiente em tempo real de desenvolvimento.

2. SEGURANÇA LOCAL

A nuvem veio para trazer mais agilidade e escalabilidade aos servidores e para a computação, mas em termos de segurança, vamos observar se também estamos em evolução, elencando prós e contras de um cenário hipotético de uma migração do seu servidor local para a nuvem.

2.1 Contras

Em termos de segurança física do servidor, o servidor local é imbatível, a única forma de você garantir a integridade do seu servidor fisicamente, é ele estando sobre a sua posse e responsabilidade, portanto, este pode ser colocado como um pró, apesar da questão da responsabilidade.

É fato que o armazenamento em cloud já ganhou do local para pequenas quantidades de dados, principalmente com muitas empresas oferecendo pacotes com os primeiros Gigabytes gratuitos, cloud se tornou a melhor alternativa para pequenas empresas, até pela facilidade do gerenciamento e criação de infraestrutura, porém, quando falamos de quantidades massivas de dados, na casa de Terabytes ou Pentabytes, como por exemplo para Big Data e Data Science, o armazenamento local ainda vence na questão do custo, pois ainda hoje, quando escalamos para grandes quantidades de dados, o custo de cloud se torna exponencial e inviável para muitas empresas.

Indo na mesma linha, um dos prós do armazenamento local é o controle, possibilitando a livre escolha de protocolos de criptografia, firewalls, controle de acesso etc., apesar de aumentar o trabalho e ter a necessidade do gerenciamento e monitoramento do ambiente, impede que fique sujeito aos protocolos, controles e processos do fornecedor, portanto, na teoria, os servidores locais podem ser mais seguros que os em nuvem.

2.2 Prós

Se na teoria o servidor local é mais seguro, com essa liberdade de aplicar quais protocolos a empresa preferir para a segurança, na prática o cenário é bem diferente. Em pesquisa recente divulgada pela Gartner, Inc. (2021), 95% das falhas causadas

em ambientes de nuvem, são causadas no primeiro pilar, a educação do usuário, ou seja, a causa é uma má prática do usuário e não a estrutura em si, portanto, o servidor local não vai impedir as más práticas, e não garantindo mais segurança.

Boa parte dos ganhos de uma estrutura em cloud estão na escalabilidade, disponibilidade e manutenção. Em teoria, a possibilidade de aumentar e deixar mais robusta uma estrutura na nuvem, é infinita mediante a contratação de pacotes maiores, fazendo com que ao mesmo tempo seja mais flexível, você ajustar a sua estrutura à necessidade do seu negócio. Outro ponto é a manutenção, apesar de no ambiente de cloud o investimento em manutenção ser contínuo, é possível notar uma econômica na força de trabalho, uma vez que o monitoramento e manutenção ficarão sob responsabilidade do provedor, livrando a sua equipe para desenvolvimento de outros projetos.

E por último, acreditamos que, o maior dos benefícios de uma estrutura em cloud, o backup. Tendo um backup em nuvem dos seus arquivos, você leva basicamente para zero a chance de perder seus arquivos, mesmo que seu aparelho seja destruído ou roubado, mesmo que o servidor pegue fogo, os principais fornecedores oferecem serviços de recuperação até mesmo com problemas nos servidores do fornecedor, utilizando servidores de contingência, você tem a garantia de ter o seu arquivo, quando você precisar dele.

2.3 Conclusão sobre migrações

Não podemos sintetizar um maior número de prós do que contras, afirmando puramente que Cloud é a melhor escolha, porém, levando em consideração a indicação do crescimento anual de uso de cloud batendo os 20%, segundo pesquisas Gartner Inc. (2021), o cenário acolhedor para pequenas empresas, e o retorno positivo das grandes empresas, aumentando os cases de migração no mercado, a tendência é que cloud ganhe cada vez mais as disputas com os servidores on-premise, atingindo o maior custo-benefício.

3. COMO ESCOLHER UM FORNECEDOR

Escolher um fornecedor não é das tarefas mais simples, mas temos alguns pontos para levar em consideração quando estamos decidindo quem vai guardar os nossos dados, infraestrutura ou serviços.

Mas claro, diferentes cenários requerem diferentes cuidados, dependendo do seu objetivo e tipo de dados, podemos valorizar diferentes atributos.

3.1 Especificações

É de suma importância verificar se o fornecedor atende as especificações necessárias para o seu objetivo final.

A primeira coisa que podemos avaliar são as certificações, algumas são básicas e devem ser essenciais ao provedor que está sendo avaliado, são estas a ISO 27001, que é a norma ISO para segurança da informação, que consiste em um conjunto de regras e definições do padrão internacional de segurança da informação, envolvendo tratamento de riscos, organização, melhoria, suporte, avaliação de desempenho etc.

Outra noma básica é a ISO 27018, considerada um adendo da ISO 27001, voltada para o armazenamento de dados pessoais em nuvem, que garante que os clientes saberão onde os dados estão sendo armazenados, os dados do cliente não serão usados para marketing ou publicidade sem o consentimento explícito, e que o provedor irá cumprir as solicitações de divulgações de dados, somente se obrigadas por lei, como por exemplo em caso de investigação criminal.

No caso do Brasil, é necessário que a empresa esteja de acordo com a LGPD, aprovada desde 2018, é essencial que o provedor esteja de acordo, para que também estejamos.

Agora para objetivos específicos em outros países, temos diferentes casos, como pode ser a CCPA (Lei de Privacidade do Consumidor da Califórnia), VCDPA (Lei de Proteção de Dados do Consumidor da Virgínia), FedRAMP (Programa Federal de Gerenciamento de Autorização e Risco dos Estados Unidos) ou a GDPR, que é a Regulação Geral sobre a Proteção de dados da União Europeia. Sobre estas leis regionais, é importante ter em mente que as leis de onde o servidor do seu provedor

de Cloud está hospedado, podem ser aplicadas aos seus dados, portanto, a recomendação geral, é sempre optar por servidores na Europa com a certificação GDPR, pois a LGPD foi diretamente inspirada nesta lei.

No momento da escolha do fornecedor, devemos levar em consideração a sensibilidade dos dados que estamos tratando, claro, sempre mais proteção é melhor, porém isso pode acarretar maiores custos, e de acordo com o tipo dos dados contidos, podemos optar por diferentes tipos de criptografia, e diferentes níveis de segurança. Por exemplo, se estamos lidando com dados sigilosos, é indicado além de olhar os tipos de criptografia, contratar um serviço de Cloud Firewall e uma VPN com alto nível de segurança.

3.2 Riscos

Agora entendemos o que buscar e exigir dos provedores de nuvem, mas, garantir estes requisitos não nos deixa isentos de riscos. Além de garantir as certificações, é necessário analisar a reputação e histórico das empresas lidando com a proteção dos dados e ataques.

Uma das maiores e mais conceituadas empresas quando falamos de computação em nuvem é a Microsoft, atendendo a todos os requisitos e principais certificações de segurança, a Microsoft segue todas as recomendações e utiliza as mais avançadas técnicas de criptografia existentes e conta com os melhores protocolos de firewalls, porém, em 2021, uma reportagem da americana Reuters, foi exposta uma falha de segurança na Azure. Um upload em uma ferramenta chamada Jupyter Notebook, utilizada no CosmosDB, banco de dados NoSQL[6] da Azure, fez com que a Microsoft precisasse alertar seus usuários sobre possibilidade de vazamento de dados, e aplicar correções, deixando os bancos fora do ar por momentos e causando um grande alvoroço nos clientes e empresas.

Portanto, não temos garantias de 100%, por mais que seja mais seguro, mais moderno e melhor, se não estamos no controle, haverá situações que fogem do nosso controle.

[6] NoSQL é um termo genérico que representa os bancos de dados não relacionais

CONCLUSÃO

Cloud Computing não pode mais ser considerado como o futuro da computação, além disso, já é uma realidade. Está totalmente inserido em nosso dia a dia, tanto no trabalho quanto na vida pessoal, negar isso é negar a realidade.

Uma vez que não podemos combater a evolução, devemos nos adequar e ambientar para fazer as melhores escolhas. Cloud se tornou essencial para o backup dos seus arquivos, para o trabalho remoto, para as transações financeiras, para a comunicação através dos aplicativos mensageiros e até para o entretenimento com os serviços streaming.

O cloud computing deve ser o grande marco tecnológico dos últimos anos, pois possibilitou uma grande mudança de paradigma na forma com que trabalhamos e consumimos entretenimento.

Podemos concluir que sim, a tendência é só aumentar o uso deste modelo de serviço, e que sim, com toda certeza, devemos ter cuidados com qual serviços estamos usando, ficar atentos às certificações, localidade da hospedagem, protocolos de segurança e quais dados estamos mandando para à nuvem.

REFERÊNCIA BIBLIOGRÁFICA

ABNT. Levantamento mostra que empresas na área financeira se adequaram mais a LGPD do que as de serviços. 2021 Disponível em: <https://www.abnt.com.br/release/279/Levantamento-mostra-que-empresas-na-area-financeira-se-adequaram-mais-a-LGPD-do-que-as-de-servicos/> Acesso em: 14 jun 2022.

AMAZON. Armazenamento na nuvem. 2022. Disponível em: < https://aws.amazon.com/pt/what-is-cloud-storage/ > Acesso em: 24 jun 2022.

AVAST. O guia essencial sobre phishing: Como funciona e como se proteger. 2022. Disponível em: < https://www.avast.com/pt-br/c-phishing > Acesso em: 24 jun 2022.

Cloud Awards. Cloud computing statistics. 2022. Disponível em: <https://www.cloudwards.net/cloud-computing-statistics/#:~:text=With%20an%20overwhelming%2094.44%20percent,and%20iCloud%20(38.89%20percent)/>
Acesso em: 14 jun 2022.

Dropbox. Conformidade com padrões e regulamentações. 2022. Disponível em:<https://www.dropbox.com/pt_BR/business/trust/compliance/certifications-compliance/> Acesso em: 21 jun 2022.

ESET. ESET Security Report 2021 América Latina. 2022. Disponível em: < https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET_security_report_2021_PT.pdf/> Acesso em: 20 jun 2022.

EXAME. Microsoft alerta clientes sobre falha de segurança em banco de dados. 2021. Disponível em: <https://exame.com/tecnologia/microsoft-alerta-clientes-sobre-risco-de-vazamento-de-dados/> Acesso em: 22 jun 2022.

F5 Labs. Cyberattacks Targeting Latin America, January through March 2021. 2021. Disponível em: <https://www.f5.com/labs/articles/threat-intelligence/cyberattacks-targeting-latin-america-january-through-march-2021/> Acesso em: 17 jun 2022.
JATHANNA, Rohan, JAGLI, Dhanamma. **Cloud Computing and Security Issues** International Journal of Engineering Research and Applications. 2017.

FEBRABAN. Brasil tem alta de 200% nos ataques de engenharia social em 2020. 2020. Disponível em: <https://noomis.febraban.org.br/temas/seguranca/brasil-tem-alta-de-200-nos-ataques-de-engenharia-social-em-2020/> Acesso em: 21 jun 2022.

Gartner. Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $500 Billion in 2022. 2019. Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022/>
Acesso em: 09 jun 2022.

GOVERNO FEDERAL. Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd> Acesso em: 24 jun 2022.

IPM. História da computação em nuvem: como surgiu a cloud computing? Maio, 2020. Disponível em:< https://www.ipm.com.br/blog/administracao-geral/historia-da-computacao-em-nuvem-como-surgiu-a-cloud-computing/>
Acesso em: 07 jun. 2022.

ISO. O que é a norma ISO 27001? 2022. Disponível em: <https://www.27001.pt/index.html> Acesso em: 21 jun 2022.

MARINOS, A., Briscoe, G. **Community Cloud Computing**. Lecture Notes in Computer Science. Springer. 2009.

Medium. On-Premise x Cloud Servers. 2019. Disponível em: <https://medium.com/realizeit/on-premise-x-cloud-servers-3c6e6818933d/> Acesso em: 21 jun 2022.

Microsoft. Quais métodos de autenticação e verificação estão disponíveis no Azure Active Directory? 2022. Disponível em: <https://docs.microsoft.com/pt-BR/azure/active-directory/authentication/concept-authentication-methods/> Acesso em: 21 jun 2022.

Microsoft. Proteção de dados do cliente do Azure. 2022. Disponível em: <https://docs.microsoft.com/pt-br/azure/security/fundamentals/protection-customer-data/> Acesso em: 21 jun 2022.

Microsoft. Código de Conduta ISO/IEC 27018 para Proteção de Dados Pessoais na Nuvem. 2022. Disponível em: <https://docs.microsoft.com/pt-br/compliance/regulatory/offering-iso-27018/> Acesso em: 21 jun 2022.

Microsoft. Fazer a transição do SSTP para o protocolo OpenVPN ou IKEv2. 2022. Disponível em: <https://docs.microsoft.com/pt-br/azure/vpn-gateway/ikev2-openvpn-from-sstp/> Acesso em: 25 jun 2022.

Nasajon. O maior vazamento de dados da história mostra que usar sistema em Nuvem é essencial. 2021. Disponível em: <https://nasajon.com.br/o-maior-vazamento-de-dados-de-historia-mostra-que-usar-sistema-em-nuvem-e-essencial/> Acesso em: 17 jun 2022.

Natário. Rui. **A Evolução da Computação: A Virtualização**. Redes & Servidores. Março, 2013. Disponível em: < https://redes-e-servidores.blogspot.com/2013/03/a-evolucao-da-computacao-virtualizacao.html> Acesso em: 07 jun. 2022.

TAURION, C. **Computação em Nuvem: Transformando o mundo da tecnologia da informação**. Rio de Janeiro: Brasport, 2009.

Tecnoblog. Exclusivo: o que há no vazamento que afetou 40 milhões de CNPJs. 2021. Disponível em: <https://tecnoblog.net/noticias/2021/01/22/exclusivo-o-que-ha-no-vazamento-que-afetou-40-milhoes-de-cnpjs//> Acesso em: 17 jun 2022

VMWARE. Virtualização. 2022. Disponível em:<https://www.vmware.com/br/solutions/virtualization.html/> Acesso em: 09 jun. 2022.