risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 17/10/2021
Aceitação/Acceptance: 25/01/2022

Cloud Computing – Quem garante a segurança dos dados?

Nuno Miguel Carvalho Galego[1], Nelson Duarte[2], Domingos Martinho[3]

Nuno.galego@islasantarem.pt; Nelson.Duarte@islasantarem.pt

[1] ISLA – Instituto Superior de Gestão e Administração, Santarém, Portugal

[2] ISLA – Instituto Superior de Gestão e Administração, Santarém, Portugal

[3] ISLA – Instituto Superior de Gestão e Administração, Santarém, Portugal

Pages: 105-115

Resumo: Cloud computing elevou a realidade dos sistemas de informação para novos limites, oferecendo novos paradigmas tais como armazenamento e processamento de dados de forma flexível. Existe uma tendência crescente do uso de ambientes de Cloud para necessidades de armazenamento e processamento de dados, no entanto, a adoção de um paradigma de Cloud computing pode ter efeitos positivos e negativos sobre a segurança de dados dos utilizadores. Nos últimos anos, tem havido um progresso rápido no que toca a Cloud computing. Com o número crescente de empresas a recorrer aos recursos da nuvem, havendo a necessidade de proteger os dados dos vários utilizadores. Alguns dos grandes desafios que estão a ser enfrentados pela Cloud computing são para garantir, proteger e processar os dados. Este trabalho tem por finalidade destacar as questões de segurança importantes existentes nos ambientes de Cloud computing tal como as vantagens e desvantagens de um ambiente Cloud, tal como as estratégias de proteção de dados de forma a garantir a segurança dos dados.

Palavras-chave: Cloud computing; Informação; Segurança; Dados.

Cloud Computing – Who ensures data security?

Abstract: Cloud computing has elevated the reality of information systems to new boundaries, offering new paradigms such as storage and data processing flexibly. There is a growing tendency to use cloud environments for storage and data processing needs, however, the adoption of a cloud computing paradigm may have positive and negative effects on user data security. In recent years, there has been rapid progress in cloud computing, with the growing number of companies using cloud resources and the need to protect the data from various users. Some of the significant challenges cloud computing faces are ensuring, protecting, and processing the data. This work highlights the critical security issues in cloud computing environments, such as the advantages and disadvantages of a cloud environment, such as data protection strategies to ensure data security.

Keywords: Cloud Computing; Information; Security; Data.

1. Introdução

Cloud computing é a próxima geração da Internet que fornece serviços personalizáveis e fáceis para os utilizadores acederem ou trabalharem com várias aplicações na nuvem. *Cloud computing* fornece uma maneira de armazenar e aceder aos dados na nuvem de qualquer lugar a qualquer hora com recurso a uma ligação à Internet. Escolhendo os serviços da nuvem, os utilizadores são capazes de armazenar dados em servidores remotos. Os dados armazenados no *datacenter* remoto podem ser acedidos ou geridos através dos serviços de nuvem (*Cloud Services*) fornecidos pelos operadores de serviços de nuvem. Os dados armazenados num *datacenter* remoto onde ocorrem os processamentos de dados devem ser feitos com o máximo cuidado.

O ambiente de *cloud computing*, torna-se preocupante porque os dados estão localizados em lugares diferentes, podendo estar noutro pais ou outro continente, proteção, privacidade e segurança da informação são os principais fatores de preocupação dos utilizadores sobre esta nova tecnologia. Embora existam algumas investigações sobre o tema, proteção, privacidade e segurança estão a tornar-se importantes para o desenvolvimento desta tecnologia em todas as organizações.

Segurança da informação na nuvem refere-se a confidencialidade dos dados, integridade, disponibilidade e estes requisitos podem ser os grandes problemas para a *cloud computing*. Confidencialidade de dados requer que a informação esteja disponível e divulgada apenas a pessoas autorizadas.

Integridade de dados garante que os dados são mantidos no seu estado original e não foram intencionalmente ou acidentalmente alterados ou eliminados.

Disponibilidade dos dados garante o acesso contínuo aos dados no caso de um desastre natural ou sintético ou eventos, tais como incêndios ou perdas de energia.

Este estudo procura fazer uma revisão de segurança da proteção de dados na nuvem e visa reforçar a proteção da segurança e privacidade de dados num ambiente de nuvem.

2. Segurança da Informação em Cloud Computing

Cada vez mais o meio empresarial e os governos estão a migrar os seus dados para a nuvem, mas ainda há quem resista a essa mudança, devido a desconfiança e receios com a segurança das suas informações. Embora as preocupações sejam compreensíveis, a realidade hoje é que, se essa migração for executada correctamente, a segurança da informação na *Cloud* pode ser tão segura ou mais do que ter os dados em plataformas tradicionais locais (Akamai, 2017).

Na verdade, a segurança da informação na nuvem é potencialmente superior ao *datacenter* típico, isto porque os fornecedores de serviços na *Cloud* protegem a informação através da utilização de dados de vários centros com replicação entre as várias instalações.

Nos *datacenters*, onde estão alojados os dados da nuvem, os custos associados com a segurança dos dados são distribuídos entre um grande número de clientes, para que os operadores possam aplicar mais recursos para as medidas de segurança físicas, técnicas e operacionais, que a maioria das empresas ou governos não possuem, uma vez

que, ao contrario da maioria das empresas e órgãos públicos, a principal atividade dos operadores é a exploração e distribuição destes serviços.

No entanto, apesar das tecnologias e da experiência em segurança de informação na *Cloud* que os operadores possam ter, permanecem válidas as preocupações sobre a segurança.

Os operadores fornecem proteção contra as principais ameaças à segurança, como ataques de DDoS, injeções SQL e scripts entre *sites*, bem como formas mais opacas de ataques que existam na *Internet*

As soluções de segurança deste tipo de operadores que fornecem serviços na *Cloud* são altamente escaláveis e fornecem uma defesa distribuída, que deteta e bloqueia os ataques antes que eles atinjam o seu *datacenter*.

2.1. Prós e Contras da Cloud Computing

Tal como acontece com qualquer tecnologia nova, para ter uma ideia de todas as suas vantagens e desvantagens é necessária uma análise.

2.1.1. Vantagens da Cloud

Se for usada correctamente e na medida necessária, trabalhar os dados na *Cloud* pode beneficiar imensamente todos os tipos de empresas. Estas são, algumas das suas vantagens mais importantes (Linthicum, 2016):

Economia de custos

A *Cloud* é provavelmente o método mais eficiente ao nível do custo para usar, manter e atualizar. Com a *Cloud* é possível reduzir os custos de forma substancial, isto sem servidores físicos na infraestrutura local, o que também remove a energia, ar condicionado e os custos de administração. Já o *software* tradicional que tem um custo significativo para as empresas, somando-se as taxas de licenciamento para vários utilizadores que se pode revelar muito caro, também é eliminado. Além disso, existem soluções *pay-per-use* (pago por utilização) disponíveis.

Manutenções e atualizações na infraestrutura de IT são eliminados, passando essa tarefa ao operador.

A *Cloud*, por outro lado, está disponível a preços mais acessíveis e pode reduzir significativamente a despesa para a empresa. Desta forma, não são necessários investimentos iniciais caros com a incerteza de os conseguir pagar.

Armazenamento quase ilimitado

O armazenamento de informações na *Cloud* oferece a capacidade de armazenamento quase ilimitado, não existindo preocupação com falta de espaço, relativamente ao armazenamento atual.

Este é o principal fator que define a nuvem, é possivel aumentar a capacidade e reduzir, num curto espaço de tempo, conforme as necessidades.

Backup e recuperação

Desde que os dados estejam armazenados na *Cloud*, *backup* e restauros são relativamente mais simples do que noutros métodos tradicionais de armazenamento de dados.

Recuperação de desastres (disaster recovery) e continuidade do negócio (Business continuity)

Os utilizadores exigem que as suas operações e serviços continuem ativos no caso de calamidade ou no caso de acontecer algum incidente com o operador de serviços onde os dados estão alojados.

Acesso à informação

Uma vez na *Cloud,* é possível aceder às informações de qualquer lugar, desde que exista ligação à *Internet*. Este recurso permite avançar para além das questões de localização geográfica e fuso horário.

Disponibilidade

A *Cloud* só tem valor quando a rede e a largura de banda contratada estiver disponível, caso contrário não é possível aceder à informação, parecido com um ataque de negação de serviço (DoS) (Winkler , 2011)**.** A maioria dos operadores oferecem um nível de serviço que garante 24 horas por dia, 7 dias por semana, 365 por ano e 99,99% de disponibilidade. A organização pode beneficiar de uma redundância de recursos, bem como mecanismos de failover, i.e., se um servidor falhar, as aplicações e serviços podem ser facilmente transferidos para outro dos servidores disponíveis, sem impacto para o negócio.

O mecanismo da *Cloud* é distribuído de acordo com a necessidade de cada cliente, oferecendo uma incrível escalabilidade de recursos.

Em comparação com um servidor dedicado

A comparação é dificil, mas a melhor maneira de apreciar as vantagens da nuvem é compará-lo com o que sabemos de muitos anos atrás: um clássico com servidor dedicado. A **Figura 1** mostra-nos uma comparação das principais vantagensce desvantagens de um servidor Cloud e um servidor On-Premise.

Em primeiro lugar, com um servidor dedicado (uma máquina física), os recursos disponíveis são limitados, e não é possível expandir facilmente estes recursos, e muito menos sem interrupção do serviço, não esquecendo que esta máquina terá manutenções e períodos em que não estará disponível.

Em segundo lugar, é necessário ter uma equipa interna com o conhecimento necessário de administração deste tipo de servidores e o *software* associado a ele. Aqui existe um custo associado ao nível da equipa interna, ou contratada em regime de *outsourcing*.

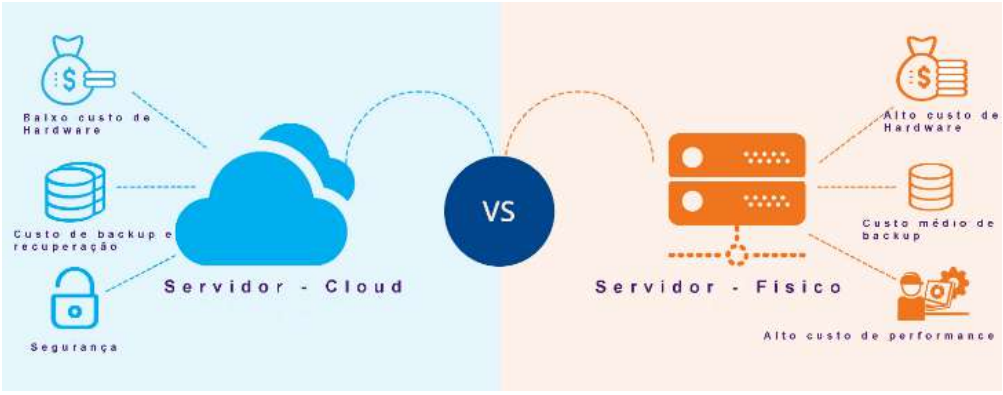

Figura 1 – Infraestrutura Cloud vs física (Adaptado de (Tahir, 2017)

Se forem avaliadas apenas as vantagens da *Cloud* acima mencionadas, está claro que a opção de um servidor dedicado é pior. Esta análise não está completa e para isso também foi feita uma análise das desvantagens de um sistema *Cloud*.

2.1.2. Desvantagens da Cloud

Apesar de seus muitos benefícios, como mencionado acima, *Cloud computing* tem muitas vantagens que vão fazer com que a sua introdução no mercado aumente nos próximos anos, mas também tem as suas desvantagens, as empresas, especialmente as pequenas, precisam estar cientes destes contras antes de adotar esta tecnologia. Quando acontece uma migração dos serviços para a *Cloud*, existem alguns problemas e perigos do seu uso, alguns deles estão listados abaixo (Seshachala, 2015).

Controlo limitado

Desde que a infraestrutura esteja totalmente na *Cloud*, a gestão e monitorização é feita em grande parte pelo operador, transferindo um controlo mínimo para o cliente. O cliente apenas controla e gere as aplicações, dados e serviços que funcionem em cima disso, não a infraestrutura de *back-end*.

É sempre difícil confiar num terceiro para guardar a nossa informação, especialmente quando não sabemos onde estão os nossos dados, nem onde é que as nossas aplicações estão a ser executadas.

As principais tarefas administrativas tais como, atualizações e *firmware* não são tarefas do cliente.

Existe algum medo, é preciso prudência para ultrapassar este primeiro problema, e ganhar confiança.

Confidencialidade e segurança dos dados

Apesar de existir um contracto assinado de confidencialidade muito detalhado, que obriga o operador a, sempre que existam problemas de segurança, manutenção inadequada, que possa causar danos à empresa, este tem de tomar medidas, mas nada garante que essas medidas não venham a ser ocultadas ou omitidas, uma vez que geralmente o cliente não tem essa perceção, além de possivelmente não ser do conhecimento do cliente onde os dados se encontram.

Um serviço de *Cloud computing* implementa os melhores padrões de segurança e certificações da indústria, armazenamento de dados e arquivos importantes, mas mesmo com todos estes cuidados existe sempre um risco.

Numa arquitetura com múltiplos clientes, onde vários estão hospedados no mesmo servidor, um *hacker* pode invadir os dados de outros clientes que armazenam informações no mesmo servidor e aceder às suas informações.

Antes de adotar esta tecnologia, é preciso saber que vão ser cedidas informações confidenciais da empresa a um operador de serviços de *Cloud*.

Disponibilidade do serviço

No caso de pequenas e médias empresas, que não têm um orçamento alto para investir em infraestrutura e técnicos qualificados, é estatisticamente mais seguro ter a informação e as suas aplicações na *Cloud*, que nos próprios servidores, mas ainda assim deve ser uma decisão ponderada. Podem vir a acontecer paragens técnicas, podendo ter um impacto brutal no negócio de qualquer organização, ficando em suspenso temporariamente. Além disso, se a ligação à *Internet* estiver *offline*, não é possível aceder a qualquer uma das suas aplicações, servidor ou dados que estejam na *Cloud*.

Questões técnicas

Embora seja verdade que as informações e dados na *Cloud* podem ser acedidas a qualquer hora e em qualquer lugar, de vez em quando este sistema pode ter alguma disfunção grave. É preciso estar consciente de que esta tecnologia está sempre propensa a falhas e outros problemas técnicos. Mesmo os melhores prestadores de serviços *Cloud* podem ter este tipo de problemas, apesar de manterem os elevados padrões de manutenção. É essencial ter uma boa ligação à *Internet* para obter um bom acesso aos servidores, em qualquer momento, e com qualquer nível de carga. Inevitavelmente, existirão sérios problemas caso haja um problema de rede ou ligação.

O armazenamento de informações na *Cloud* pode colocar qualquer empresa vulnerável a ameaças e ataques externos de *hacking*.

Existem conteúdos na Internet que não são seguros, existindo sempre a possibilidade de roubo de dados sensíveis. Em forma de conclusão, o *Cloud computing* também tem os seus prós e contras. Embora ainda existam algumas preocupações sobre a perspetiva da segurança da informação na nuvem, esta é essencialmente uma conclusão imprecisa. É fácil ver como as vantagens da *Cloud* facilmente superam as desvantagens, diminuição de custos, tempo de inatividade reduzida e menos esforço de gestão são benefícios que falam por si.

Com as suas qualidades inerentes, a *Cloud* tem um enorme potencial para as organizações melhorarem a segurança dos sistemas de informação.

3. Estratégias de protecção de dados

Até há alguns anos, a proteção de dados era uma tarefa secundária, onde não se dava a devida importância. Nos dias de hoje, é considerada uma atividade estratégica, que contribui para o sucesso do negócio, isto porque uma boa estratégia de proteção de dados pode evitar a interrupção dos serviços. Ainda assim a implementação de uma boa estratégia de proteção de dados requer alguns cuidados que devem ser tomados em atenção. Segundo Priya Viswanathan (Viswanathan, 2016) existem questões essenciais que devem ser tomadas para que a proteção de dados traga mais benefícios do que malefícios para a empresa.

Que estratégias uma empresa deve adotar para assegurar a proteção de dados?

Os ataques recentes no sector empresarial trazem questões muito importantes a este trabalho. Quão segura é a empresa? Quais são as políticas de segurança que uma empresa deve seguir para proteger as suas informações corporativas? Mais importante, que estratégias de proteção de dados o sector de empresas deve adotar? É essencial para qualquer empresa aplicar uma estratégia de proteção de dados eficaz, para assegurar a confidencialidade dos dados relativos a essa empresa. Considerando a importância deste aspeto da segurança na empresa, é mostrado abaixo uma secção de perguntas frequentes sobre as estratégias de proteção de dados que o sector empresarial deve seguir.

Porque é que uma estratégia de proteção de dados é importante?

Uma estratégia de proteção de dados eficaz tem de estar em conformidade com os requisitos de privacidade da empresa, tal como estipulado pela lei. A outra razão é que para manter uma política de proteção de dados eficaz, a empresa deve elaborar um inventário completo de todos os seus processos de dados e propriedade intelectual, ajudando também a criar uma estratégia abrangente de segurança. Todos os dados da empresa devem ser contabilizados neste processo, incluindo a propriedade intelectual tais como patentes, marcas comerciais e outro material protegido por direitos de autor, como funcionam os processos, códigos fonte de *software*, manuais, planos, relatórios e afins.

Como iniciar esta estratégia?

Existem vários departamentos numa empresa que gerem as informações confidenciais da empresa.

- O departamento de IT, por exemplo, lida com todas as informações que passam pelos servidores da empresa. Este processo pode ajudar a manter o inventário de dados e a implementar estratégias de segurança para o mesmo.
- O departamento jurídico, oficialmente, pode formular regras na empresa em relação ao uso desses arquivos e outros dados oficiais, confidenciais ou não. Esta secção é normalmente focada na criação e gestão das políticas de segurança da empresa.

- O departamento de recursos humanos pode trabalhar em conjunto com o departamento jurídico no rastreio dos funcionários para manter as informações pessoais identificáveis.

Que outras precauções que devem as empresas tomar?

Além de criar e manter uma política de segurança clara, a empresa deve gerir eficazmente toda a informação disponível. Isso inclui os seguintes aspetos:

- Uma política de segurança adequada e detalhada é uma necessidade absoluta para qualquer empresa. Os funcionários devem ser informados de todos os princípios e disposições incluídas na política de segurança, para que entendam que tipos de dados podem ou não podem aceder, e as informações que podem ou não divulgar a outras pessoas fora da empresa.
- Todos os dados e informações devem ser classificadas de acordo com o seu nível de sensibilidade. Podem dar alta prioridade somente para o que for considerado dados confidenciais. Muitas vezes, os dados que são vistos como menos importantes são completamente ignorados, criando assim uma possível fuga de informação.
- É muito importante atualizar constantemente todos os sistemas de segurança de dados, para que a empresa esteja preparada para lidar com as ameaças de segurança mais recentes. Embora seja quase impossível garantir uma segurança empresarial completa em todos os momentos, a empresa deve garantir a máxima segurança, mantendo os sistemas de segurança de dados o mais atualizados possível.

Os problemas mais importantes são os seguintes:

Abusos na Cloud computing

A infraestrutura de nuvem tem sido utilizada para fins menos claros como *botnet's* e redes de envio de *spam*. Isto acontece porque o acesso a esses recursos não é restrito. Qualquer pessoa que pague, pode ter recursos consideráveis para cometer um crime. E é preciso não esquecer que ao lado dessas aplicações "criminosas", na mesma *Cloud*, estão os dados das empresas.

Interfaces inseguras e APIs

Os serviços de *Cloud* fornecem uma interface, ou uma API para acesso a recursos, configuração, *status*, adicionar e remover recursos. Isso pode representar uma falha de segurança, já que não se controla quem está a aceder à *Cloud,* e assim, intencionalmente ou acidentalmente acontecer uma negação de serviço ou provocar algum mal ao serviço e, em caso extremo, a outros clientes do mesmo operador na *Cloud***.**

Perda de informação

Os problemas de informação são muitos e variados, perda de dados por exclusão acidental, acesso a dados fora da empresa, onde os recursos são partilhados com outros clientes, numa partilha, numa pasta alojada no operador de *Cloud*, onde pode existir

alguém mal-intencionado, que pode negligenciar os dados da empresa ou cometer um ato criminosos, ou até mesmo vender essas informações.

Roubo de sessão

Todos os controlos de acessos dos recursos da *Cloud* são efetuados usando credenciais (geralmente *username* e *password*), da mesma forma que acedemos ao *webmail*. Obviamente, se essas credenciais caírem nas mãos erradas, quem tiver esse acesso pode espiar e manipular dados, o que terá um impacto negativo no negócio.

Riscos devido à ignorância

Uma das vantagens da *Cloud* é precisamente de que não precisamos de saber os detalhes da infraestrutura. No entanto, é necessário ter um conhecimento mínimo das decisões a respeito da segurança e dimensionamento dos recursos. **Algumas recomendações importantes são:**

Conformidade normativa

Os clientes são responsáveis pela segurança e a integridade dos dados, mas os operadores devem permitir que sejam efetuadas auditorias, para mostrar que é possível confiar os dados confidenciais da empresa nessa infraestrutura.

Localização de dados

É importante conhecer a lei aplicável em matéria de proteção de dados, de preferência tem que existir um acordo, para aplicar as regras do país do cliente.

O isolamento de dados

O isolamento dos dados entre um cliente e outro deve existir, uma vez que vários clientes partilham os mesmos recursos. Se isso não for feito, existe o risco de fugas de informação confidencial.

Política de backup e recuperação

É muito importante exigir uma política de *backup* e recuperação de desastres. Vivemos num mundo digital, onde as regras da informação estão acima de tudo, portanto, desenvolver uma estratégia de proteção de dados eficaz torna-se imperativo para qualquer empresa. Esta estratégia de proteção de dados, tem de levar em consideração todos os dados da empresa, processos administrativos e políticas de segurança.

4. Conclusões

Apesar do *Cloud Computing* ter inúmeras vantagens, ainda existem muitos problemas que precisam de ser resolvidos. As vulnerabilidades existentes no modelo de *Cloud* vão aumentar as ameaças perpetuadas pelos *hackers*. De acordo com a investigação feita, as questões de proteção de segurança e privacidade dos dados são os problemas principais, que precisam ser resolvidos o mais rápido possível. Apesar do *Cloud Computing* ser uma

tecnologia emergente que apresenta um bom número de benefícios para as empresas, ainda enfrenta muitos desafios de segurança. Questões de segurança e privacidade de dados existem em todos os níveis e em todas as fases do ciclo de vida dos dados. Os desafios na proteção da privacidade estão na partilha dos dados e proteção de dados pessoais. Qualquer empresa que esteja a pensar em mudar para a nuvem, deve primeiro compreender o tipo de informação que vai armazenar, onde está e qual seria o impacto de uma falha no recebimento de dados. Um inventário das informações e a classificação das mesmas, são informaçãoes importantes para todos os ambientes de negócio, e é particularmente importante que as empresas compreendam a sensibilidade dos dados atualmente armazenados dentro da empresa, até que eles sejam migrados para um ambiente de *Cloud*.

Neste artigo foi abordado a segurança na *Cloud*, vantagens, desvantagens e vulnerabilidades que existem. Foi também abordada uma estratégia de proteção de dados proporcionando recomendações de como a informação deve ser tratada.

Para escolher a melhor forma de proteger a informação, é preciso ter noção da importância da informação a proteger. A primeira operação a concretizar, é definir o nível de privacidade necessária, e o nível de proteção pretendido. É preciso ter em atenção que nem todas as empresas estão dispostas a pagar para ter os dados na *Cloud*, contudo e após esta análise, conclui-se que é mais seguro ter os dados na *Cloud*.

Referências

Abbedi, I. M. (2014). *Cloud Management and Security*. Wiley.

Akamai. (09 de Outubro de 2017). *Data Security in Cloud Computing*. Obtido de https://www.akamai.com/uk/en/resources/data-security-in-cloud-computing.jsp

GFI. (Outubro de 2017). On-premise vs. cloud-based solutions.

Halpert, B. (2011). *Auditing Cloud Computing - A Security and Privacy Guide*. Wiley.

Huang, Z. (2015). *Cloud Computing and Security, First International Conference, ICCCS 2015*. Springer.

Kan Yang, X. J. (2014). *Security for Cloud Storage Systems*. Springer.

Linthicum, D. (18 de Maio de 2016). *The Benefits of Cloud Computing for the Enterprise*. Obtido de https://cloudacademy.com/blog/the-benefits-of-cloud-computing-for-the-enterprise/

Mather, T. (2009). *Cloud Security and Privacy*. O'Reilly.

Misra, S., Ajayi, O., & Odun-Ayo, I. (2018). Cloud Computing Security: Issues and Developments. *Proceedings of the World Congress on Engineering*. London: WCE .

Newcombe, L. (2012). *Securing Cloud Services: A pragmatic approach to security architecture in the Cloud*. IT Governance Publishing.

Osei-Opoku, E., Regaieg, R., & Koubaa, M. (2020). Review on Cloud Computing Security Challenges. *European Scientific Journal*.

Raghu Yeluri, E. C.-L. (2014). *Building the Infrastructure for Cloud Security - A Solutions View*. Apress Open.

Sen, A. (2018). *Security risk assessment in cloud computing domains*. Missouri: Missouri University of Science and Technology.

Seshachala, S. (Março de 2015). *Disadvantages of Cloud Computing*. Obtido de https://cloudacademy.com/blog/disadvantages-of-cloud-computing/

Tahir, R. (Abril de 2017). *Video Hosting Costs in Cloud vs. On-Premises Infrastructure*. Obtido de https://blog.vidizmo.com/cloud-vs.-on-premises-video-hosting-costs#gsc.tab=0

Viswanathan, P. (Outubro de 2016). *FAQ on Data Protection Strategies for Enterprise*. Obtido de https://www.lifewire.com/strategies-for-enterprises-to-ensure-data-protection-2373385

Winkler , V. (2011). Seguridad en la nube. Elsevier .

Zhu, S. Y. (2015). *Guide to Security Assurance for Cloud Computing*. Springer