MACSON JOSÉ MENDES DE ALMEIDA

UTILIZAÇÃO DE SERVIÇOS EM NUVEM POR INSTITUIÇÕES MILITARES

Trabalho Acadêmico – Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do certificado do Curso Superior de Segurança e Defesa Cibernética.

Orientador: Prof Dr. Anderson Fernandes Pereira dos Santos - Cel

Rio de Janeiro

2023

C2023 ESG

_____

MACSON JOSÉ MENDES DE ALMEIDA

RESUMO

A computação em nuvem é uma das tecnologias que mais crescem e se espalham atualmente. Este crescimento ocorre de forma consistente e sistemática à medida que as corporações precisam renovar os seus parques tecnológicos. A razão para essa mudança na forma em que as instituições prestam ou consomem serviços de Tecnologia da Informação (TI) se dá principalmente pela drástica redução inicial nos custos de implementação. Nesta mesma esteira os governos dos países ao redor do mundo também desenvolveram suas estratégias de migração de serviços governamentais para a nuvem. Apesar de apresentar inúmeras vantagens, a migração de uma infraestrutura própria de TI para nuvens também traz alguns problemas que precisam ser endereçados. De forma a tirar proveito das vantagens que a computação em nuvem traz, muitas Forças Armadas pelo mundo também estão conduzindo suas estratégias de utilização de nuvens. Dessa forma foi feita uma pesquisa em artigos científicos e documentos governamentais em busca de entender o fenômeno da computação em nuvem, quais suas formas de aplicação, quais suas vantagens e desvantagens, quais os seus maiores problemas e como o serviço de computação em nuvem se relaciona com as aplicações militares.

Palavras-chave: computação em nuvem; nuvem governamental; nuvem militar.

ABSTRACT

Cloud computing is one of the fastest growing and spreading technologies today. This growth occurs consistently and systematically as corporations need to renew their technology parks. The reason for this change in the way institutions provide or consume Information Technology (IT) services is mainly due to the drastic initial reduction in implementation costs. In this same vein, the governments of countries around the world have also developed their strategies for migrating government services to the cloud. Despite presenting numerous advantages, migrating your own IT infrastructure to clouds also brings some problems that need to be addressed. In order to take advantage of the benefits that cloud computing brings, many Armed Forces around the world are also implementing their cloud usage strategies. In this way, research was carried out on scientific articles and government documents in order to understand the phenomenon of cloud computing, what are its forms of application, what are its advantages and disadvantages, what are its biggest problems and how the cloud computing service relates to with military applications.
Keywords*: cloud computing; government cloud; military cloud.*

SUMÁRIO

1 INTRODUÇÃO

A Computação em Nuvem tem tomado parte na sociedade atual de forma totalmente transparente para os usuários, ou seja, as pessoas inconscientemente estão consumindo serviços disponibilizados em nuvens o tempo todo.

Da mesma maneira, empresas e governos estão paulatinamente desenvolvendo e implementando estratégias de migração de serviços para nuvens, de forma a tirar proveito das inúmeras vantagens que esse modelo de prover e consumir serviços de Tecnologia da Informação oferece.

A computação em nuvem está provocando uma disrupção na forma como as organizações lidam com a TI no seu dia a dia, trazendo novos modelos de consumo de serviços, de gestão de TI, mudanças nas necessidades de capacitações e competências dos recursos humanos e nas formas de investimento e custeio do ambiente de TI.

Como toda tecnologia, a computação em nuvem vem com alguns problemas que precisam ser levados em conta na estratégia de adoção desse modelo de lidar com a TI pelas corporações.

Entre os principais problemas encontram-se a segurança e a privacidade dos dados, principalmente dos dados em repouso.

Neste cenário, este trabalho tem como objetivos intermediários identificar os principais problemas na adoção do modelo de computação em nuvens e entender como alguns governos estão desenvolvendo as suas estratégias de utilização de serviços em nuvem.

O objetivo final deste trabalho é entender como as Forças Armadas de alguns países estão se relacionando com serviços de nuvens e como estão lidando com os problemas intrínsecos à esta tecnologia.

Dessa forma, o problema de pesquisa deste trabalho é identificar: De que Forma a utilização de Serviços de Nuvens se Relaciona com Aplicações Militares.

Este estudo não o objetivo de apresentar propostas de técnicas para mitigar os problemas inerentes à adoção de serviços de nuvens e nem como solucioná-los. Também não fará uma análise aprofundada de um ou outro problema da computação em nuvem. Também não apresentará uma estratégia de adoção de serviços em nuvem para as Forças Armadas Brasileiras.

A relevância deste estudo reside no fato de as Forças Armadas Brasileiras, em particular o Exército Brasileiro, ser resistente a qualquer iniciativa que envolva interações

com nuvens na prestação dos serviços de TI aos seus integrantes. Neste contexto, a intenção deste trabalho é colocar uma luz sobre o tema, de forma que este assunto possa começar a ser debatido com mais propriedade e assertividade dentro da Força a fim de subsidiar futuras decisões sobre a adoção ou não da tecnologia de computação em nuvem no contexto das Forças Armadas Brasileiras.

2 REFERENCIAL TEÓRICO

Uma das definições de Computação em Nuvem mais citadas em trabalhos científicos é a apresentada pelo *National Institute os Standards and Technology* (NIST), uma agência não reguladora que promove a inovação, padrões e tecnologia de medição nos Estados Unidos da América.

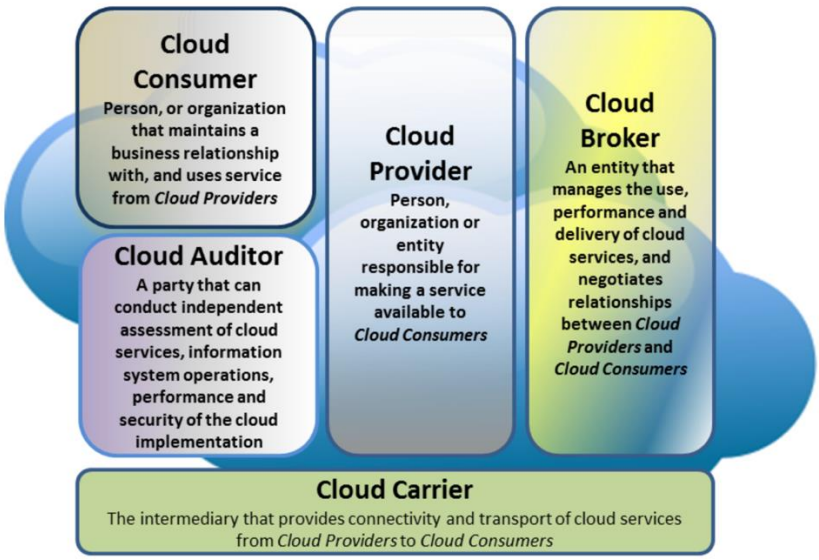
Esta publicação trazida por Hogan e Sokol (2013) diz o seguinte:

> Computação em Nuvem é um modelo para habilitar um acesso à rede onipresente, conveniente e sob demanda, a um conjunto configurável de recursos computacionais (por exemplo, redes, servidores, armazenamentos, aplicações e serviços) que podem ser provisionados rapidamente e dispensados com um mínimo de esforço de gerenciamento e/ou interação com o provedor de serviços.

Ainda de acordo com Hogan e Sokol (2013), as características essenciais da computação em nuvem são:

a. autosserviço sob demanda: o usuário pode, por si próprio provisionar capacidades computacionais, de forma automática, sem interação humana com o provedor de serviços;
b. acesso à rede em banda larga: as capacidades são disponibilizadas via rede e acessadas por mecanismos padronizados que permitem o uso de plataformas heterogêneas;
c. agrupamento de recursos: os recursos computacionais do provedor são agrupados para atender múltiplos consumidores em um modelo multiusuário, os recursos físicos e virtuais são dinamicamente alocados e realocados de acordo com a necessidade dos usuários;
d. elasticidade rápida: as capacidades podem ser elasticamente provisionadas e liberadas de forma automática para acompanhar rápidos aumentos ou diminuições de demandas; e
e. serviço medido: O serviço controla e otimiza automaticamente o uso dos recursos, utilizando uma métrica adequada ao tipo de serviço. A utilização dos recursos pode ser monitorada, controlada, auditada e reportada para prover transparência.

Figura 1: Atores de Nuvens



Fonte: Hogan; Sokol, 2013.

Três modelos de serviço são apresentados por Hogan e Sokol (2013):

a. software como Serviço (*SaaS*): A capacidade disponibilizada ao consumidor são aplicações executadas na infraestrutura de nuvem. As aplicações podem ser acessadas via um navegador de internet ou uma interface de programa;
b. plataforma como Serviço (*PaaS*): A capacidade disponibilizada ao consumidor é a implantação de aplicativos criados ou adquiridos por ele na infraestrutura de nuvem. Estes aplicativos são criados usando linguagens de programação, bibliotecas, serviços e ferramentas suportadas pelo provedor; e
c. infraestrutura como Serviço (IaaS): A capacidade disponibilizada ao consumidor é o provimento de processamento, armazenamento, redes e outros recursos computacionais fundamentais onde o consumidor pode implantar e executar softwares arbitrários que podem incluir sistemas operacionais e aplicações.

Hogan e Sokol (2013) também apresentam os modelos de implantação de nuvens, que podem ser:

a. nuvem Privada: A infraestrutura de nuvem é provisionada exclusivamente para uma única organização. Pode ser instalada internamente ou externamente à organização e a posse, gerência e operação pode ser da própria organização ou terceirizada;

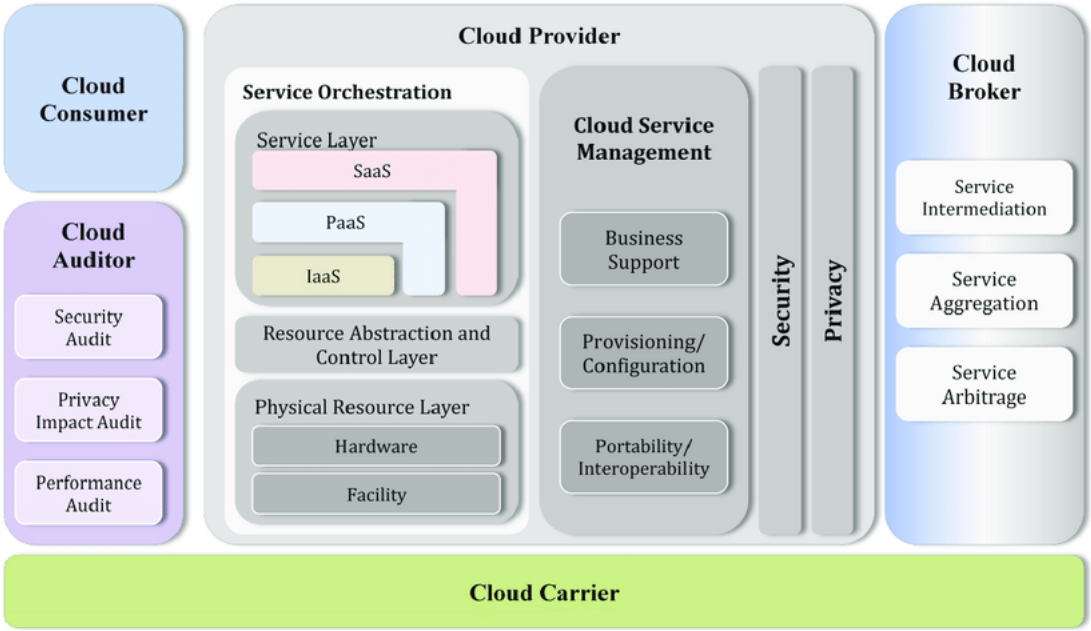
b. nuvem Comunitária: A infraestrutura de nuvem é provisionada para uso exclusivo de uma comunidade de organizações que compartilham interesses. Se assemelha às nuvens privadas nas demais características;
c. nuvem Pública: A infraestrutura de nuvem é provisionada de forma aberta para o público em geral. Pode pertencer, ser gerenciada e operada por várias organizações e é instalada nas infraestruturas do provedor de serviços; e
d. nuvem Híbrida: A infraestrutura de nuvem é uma composição de duas ou mais nuvens que permanecem independentes entre si. As várias infraestruturas são unidas por tecnologias que permitem a portabilidade de dados e aplicações.

Hogan e Sokol (2013) também definem uma Arquitetura de Referência para Computação em Nuvem, onde são apresentados, entre outros conceitos, os atores envolvidos no modelo conceitual, vide Figura 1.

Segundo Balasubramanian e Aramudhan (2012), “O provedor de nuvem é a entidade que possui e gerencia os recursos. O consumidor de nuvem é a entidade que consome os recursos e pode ser um indivíduo ou uma organização”.

Ainda existem as figuras do Intermediário de nuvem (*Broker*) que faz a ponte entre o provedor e o consumidor, o auditor de nuvem e o prestador de serviço de comunicações. A Figura 2 apresenta o modelo completo.

Figura 2: Modelo de referência de computação em nuvem definido pelo NIST



Fonte: Mohamed, 2014.

É importante ressaltar que para tirar o melhor proveito da computação em nuvem, principalmente em um ambiente *multi-cloud*, é imperativo que as aplicações sejam desenvolvidas como nativas para nuvem.

Alonso et al. (2023) afirmam que a comunidade científica ainda está estudando o conceito preciso de nativo para nuvem.

Entretanto, segundo Kosinska e Zielinski (2020) o conceito de nativo para nuvem é construído sob a filosofia de conteinerização e o gerenciamento dos contêineres através de ferramentas de orquestração.

Segundo Soltani, Ghenai e Zeghib (2018), conteinerização é uma tecnologia de virtualização mais leve e contêineres apresentam um mecanismo de empacotamento lógico no qual as aplicações podem ser abstraídas do ambiente em estão sendo executadas.

2.1 Problemas Relativos à Computação em Nuvem

Para Jathanna e Jagli (2017), a computação em nuvem está sujeita às seguintes ameaças:

a. comprometimento de credenciais e autenticação falha: Credenciais roubadas, vazadas ou usadas indevidamente ou usos de procedimentos de autenticação com baixo nível de segurança;
b. violação de dados: Vazamento de informação, os danos para a instituição serão tão mais graves quanto o nível de sensibilidade dos dados, informação pessoal, dados governamentais ou segredos industriais;
c. interfaces e API hackeadas: As API são usadas como uma interface padronizada para aplicações interagirem com o serviço de nuvem. Se as API e as interfaces possuírem fraquezas, podem se exploradas por atacantes;
d. vulnerabilidades de sistemas exploradas: Softwares e sistemas podem apresentar vulnerabilidades que podem ser exploradas por hackers. Esse problema se acentua pois os diversos usuários compartilham vários recursos computacionais;
e. sequestro de contas de acesso: As contas de acesso à infraestrutura de nuvem podem ser sequestradas por meio de fraudes, *phishing* ou exploração de falhas em softwares;
f. perda permanente de dados: No passado hackers já apagaram, permanentemente, dados na nuvem, da mesma forma desastres naturais podem

provocar perda de dados. Para evitar perda de dados os provedores de nuvens podem distribuir os dados por várias localidades diferentes;

g. diligência inadequada: Organizações aderem a serviços de nuvem sem conhecer completamente o ambiente e os riscos inerentes;
h. abusos do serviço de nuvem: Plataformas de nuvem podem ser usadas para desferir ataques de rede tais como envio de *spam*, *phishing* ou DDoS; e
i. ataques de negação de serviço: Os ataques de negação de serviço existem há um longo tempo e com o advento da computação em nuvem ele tem ganhado proeminência. Os ataques de DoS consomem muito processamento e normalmente o usuário pagará essa conta.

Segundo Behl e Behl (2012), o modelo de computação em nuvem apresenta os seguintes problemas:

a. segurança na nuvem;
b. atrelamento a um provedor;
c. multiusuários;
d. gerenciamento seguro dos dados;
e. portabilidade do serviço; e
f. gerenciamento de acordo de nível de serviço (SLA).

Para Kaur e Kaur (2015), os problemas de segurança que a computação em nuvem apresenta são:

a. controle de acesso aos dados: algumas vezes dados confidenciais são acessados ilegalmente devido a falhas no controle de acesso aos dados;
b. integridade dos dados: algumas vezes os dados são inseridos erroneamente ou acontecem erros em transmissões de dados ou mesmo o mal funcionamento do hardware provoca erros nos dados;
c. perda de dados: é um problema sério em computação em nuvem, pessoas não autorizadas podem obter acesso via rede;
d. roubo de dados: a computação em nuvem usa servidores de dados externos para otimizar custos e trazer flexibilidade para as operações;
e. problemas de privacidade: a maioria dos servidores são externos, dessa forma o provedor de serviço deve assegurar a segurança;
f. problemas ao de nível de usuário: os usuários devem tomar certos cuidados para não permitir perda ou adulteração de dados por parte de outros usuários; e
g. problemas ao nível do provedor de serviços: o provedor de serviços deve implementar uma robusta camada de segurança contra todas as ameaças.

Balasubramanian e Aramudhan (2012) afirmam que, os principais fatores para instituições que migram para nuvem são segurança e privacidade, pois vários recursos são compartilhados e colocar dados em um hardware compartilhado parece figurar como um alto fator de risco.

Para Ravi Kumar, Hervert Raj e Jelciana (2017), “Nuvem Pública é mais susceptível a problemas de segurança do que os outros modelos de nuvem porque é aberta para todos e usa a internet geral como meio de conexão”, ou seja, toda a infraestrutura computacional é compartilhada entre diferentes usuários e instituições, até mesmo os sistemas de armazenamento de dados.

Segundo Heydari, Tavakoli e Riazi (2014), entre outros problemas de segurança em nuvens públicas, existe a possibilidade de acesso aos dados do consumidor de nuvem por parte do provedor de serviços e também a possibilidade de acesso aos dados por governos estrangeiros, pois normalmente, a exata localização dos dados é incerta e os países definem diferentes leis e regulamentos para governar as atividades de armazenamento e acesso aos dados. Isso pode ser uma grande ameaça quando esses dados são segredos industriais ou de estado.

Segundo Jathanna e Jagli (2017), armazenamento e rede representam os principais conceitos de segurança em computação em nuvem. Mais uma vez é apresentada a preocupação com a forma de armazenamento dos dados.

De acordo com Reed, Rezek e Simmonds (2011), existem seis estágios no ciclo de vida dos dados: Criação, Armazenamento, Uso, Compartilhamento, Arquivação e Destruição.

Neste contexto, Ravi Kumar, Hervert Raj e Jelciana (2017) afirma que os dados devem ser protegidos em todos os estágios do seu ciclo de vida e Gallagher (1991) afirma que mesmo após a sua destruição, ainda podem restar traços físicos nos armazenamentos que possibilitam a reconstrução desses dados. Essas afirmações enfatizam a necessidade de cuidados especiais com relação à privacidade e a segurança dos dados armazenados em nuvens. A privacidade dos dados vai se configurando como a grande preocupação com a tecnologia de nuvens.

Ainda, segundo Reed, Rezek e Simmonds (2011), “Em computação em nuvem, os dados são armazenados em diferentes localidades geográficas, sujeitas a diferentes jurisdições legais”. Esta característica pode trazer complicações para o proprietário dos dados, principalmente se estes ficarem armazenados em diferentes países.

De acordo com Subashini e Kavitha (2011), os provedores de serviços de nuvem podem replicar os dados por múltiplos países com o objetivo de obter alta disponibilidade,

além disso, a natureza multiusuária da nuvem resulta em que os dados de vários usuários estarão armazenados no mesmo local e isso traz a possibilidade de um usuário invadir a área de dados de outro.

Segundo Jain (2012), a existência de dados sensíveis em um ambiente de nuvem é um dos grandes problemas relativos à segurança, pois o ambiente é acessível para todos os usuários e isso é inadequado para a privacidade, existe ainda a possibilidade de roubo dos dados e de perda dos dados e a quase totalidade das medidas de proteção estão sob a responsabilidade do provedor de serviço de nuvem. Jain (2012) continua, e afirma que a localização física dos dados é de suma importância, essa localização não é transparente para o usuário e os provedores de nuvem não revelam exatamente onde os dados estão armazenados. A falta de um controle mais rígido sobre os dados por parte dos proprietários vem figurando como o grande inconveniente da computação em nuvem, principalmente as públicas.

Dessa forma, Bhadauria e Sanyal (2014), afirmam que um ambiente de nuvem pública possui muitos fatores relacionados a segurança que precisam ser tratados quando comparado a um cenário de nuvem privada.

Rackspace Technology (2023), afirma que a demora de agências reguladoras para definir requisitos de segurança para nuvens públicas cria barreiras à sua adoção para aplicações sensíveis, neste sentido para garantir os requisitos de segurança adequados, providos por *hardware* dedicado, muitas corporações estão adotando o modelo de nuvem privada de forma a aliar os benefícios da computação em nuvem aos requisitos de segurança necessários.

Bhadauria e Sanyal (2014) afirma, “vários provedores de nuvens adotam diferentes tecnologias para proteger os dados armazenados em suas infraestruturas” e pergunta: “os dados armazenados nessas nuvens estão realmente seguros?”

Ainda segundo Bhadauria e Sanyal (2014), os dados em um ambiente de nuvem pública são armazenados fora da corporação e não há como negar a possibilidade de um ataque originado por um integrante interno do provedor de serviço de nuvem, dessa forma o círculo de internos que podem perpetrar um ataque cresce bastante, já que se somam os internos do provedor aos da própria instituição consumidora do serviço.

Omotosho (2019), diz que deve haver uma relação de confiança entre o consumidor e o provedor de nuvem, dessa forma o consumidor precisa acreditar que o provedor é quem ele diz ser e que ele vai prover a proteção da privacidade e segurança dos seus dados. Um problema surge quando o provedor de serviços de nuvem é de um

país diferente do usuário, se esse usuário for um ente governamental ou uma Força Armada esse problema se acentua bastante.

Venkatesh e Eastaff (2018), fala que ao enviar os dados para a nuvem, os proprietários transferem o controle sobre eles para um terceiro e isso pode trazer problemas de segurança, algumas vezes o próprio provedor de serviço de nuvem pode usar ou corromper os dados ilegalmente. E comenta, uma vez enviados para a nuvem, os dados estão sujeitos a ataques e os atacantes podem ser internos ou externos ao provedor de serviços de nuvem.

Segundo Saxenal e Chourey (2014), “A computação em nuvem diminui os riscos e aumenta o controle quando vai da nuvem pública para a privada. A nuvem privada traz mais controle sobre a segurança e a privacidade dos dados, conformidade e qualidade de serviço (QoS)”.

Nesse contexto, é coerente inferir que o maior óbice na adoção da tecnologia de computação em nuvem, em particular nuvem pública, é com relação ao controle sobre os dados mais críticos. Os proprietários dos dados não têm controle sobre a localização física dos dados e não proveem o controle de acesso a esses dados. Ainda, os proprietários dos dados não conseguem ter uma noção precisa sobre as leis e regulamentos aos quais os dados estão sujeitos. Além disso, os dados ficam sujeitos a acessos não autorizados por internos do provedor de serviço ou por entes governamentais com jurisdição sobre a área geográfica onde os dados residem.

Uma forma de mitigar esses problemas é a adoção de nuvens privadas, porém dessa forma algumas vantagens trazidas pela tecnologia de computação em nuvem são atenuadas ou perdidas. Dessa forma, a utilização de um modelo de nuvem híbrida pode ser uma solução que mantenha a maioria das vantagens da computação em nuvem e garanta um maior controle sobre os dados armazenados.

2.2 Uso de Computação em Nuvem por Governos

Vários países vêm adotando ou estudando a possibilidade de adotar a computação em nuvem como forma de modernizar, trazer maior eficiência e otimizar os custos dos serviços de TI consumidos ou providos pelos governos.

Uma das definições de governo eletrônico mais aceitas na sociedade é a do Banco Mundial, Sudan et al. (2015) definem Governo Eletrônico da seguinte forma:

> “Governo Eletrônico” refere-se à utilização pelas agências governamentais de tecnologias de informação (tais como redes de longa distância, Internet e computação móvel) que têm a capacidade de transformar as relações com cidadãos, empresas e outros ramos do governo. Estas tecnologias podem servir uma variedade de fins diferentes: melhor prestação de serviços

> governamentais aos cidadãos, melhores interações com as empresas e a indústria, capacitação dos cidadãos através do acesso à informação ou uma gestão governamental mais eficiente. Os benefícios resultantes podem ser menos corrupção, maior transparência, maior conveniência, crescimento de receitas e/ou reduções de custos.

O uso de computação em nuvem tem um grande potencial para modernizar a prestação de serviços públicos por parte dos governos, nesse contexto Mohammed e Ibrahim (2015), afirmam que essa tecnologia tem características chave para aplicação nos governos eletrônicos (e-Gov), sejam elas:

a. fácil implementação: Não é necessário um *hardware* pesado, compra de licenças ou implementação de aplicações;
b. economia de custos: Não é necessário o investimento de capital e os custos operacionais se resumem ao que foi utilizado em termos de recursos computacionais;
c. escalabilidade: Não há a necessidade de adquirir *hardware* ou *software* para acompanhar o aumento da demanda pelos serviços;
d. acessibilidade: Permite o acesso de qualquer lugar a partir de uma ampla gama de dispositivos;
e. acesso às capacidades de TI: Permite que pequenas organizações tenham acesso a *hardware* e *software* poderosos;
f. realocação do pessoal de TI e foco nas principais competências: Permite que as organizações concentrem o seu pessoal na atividade fim; e
g. computação verde: A computação em nuvem otimiza o uso de energia.

Nesta mesma linha de pensamento, Assaf, Hamsir e Muhammad (2021) apresentam as seguintes vantagens da adoção de computação em nuvem nas atividades de Governo Eletrônico:

a. segurança mais avançada;
b. melhor efetividade de custos;
c. melhoria da escalabilidade;
d. aumento de flexibilidade;
e. mais simplicidade;
f. fácil implementação;
g. suporte para agilidade;
h. confiabilidade e disponibilidade;
i. centralização de dados;
j. recuperação de dados;

k. acessibilidade melhorada; e
l. computação verde.

Dessa forma, é fácil perceber uma convergência entre os autores sobre os benefícios da adoção da tecnologia de computação em nuvem por governos em busca de modernização de seus serviços ao cidadão e otimização de custos de TI.

Mohammed e Ibrahim (2015), também apresentam alguns desafios relacionados à adoção dessa tecnologia por entes governamentais:

a. ausência de padrões e interoperabilidade;
b. segurança e privacidade;
c. continuidade do negócio;
d. dependência da Internet; e
e. outras.

Já Assaf, Hamsir e Muhammad (2021) apresentam os seguintes desafios:

a. privacidade e segurança dos dados;
b. o risco do compartilhamento de infraestrutura;
c. ficar preso a uma empresa provedora;
d. problemas de desempenho;
e. problemas de regulação e conformidade;
f. possíveis custos adicionais pelos serviços medidos;
g. problemas de vulnerabilidades; e
h. perda de controle sobre os dados.

Como forma de apresentar um cenário sobre a adoção da tecnologia de computação em nuvem por governos de países pelo mundo, Mohammed e Ibrahim (2015) analisaram as estratégias de alguns países desenvolvidos e em desenvolvimento, e com diferentes níveis de adoção da tecnologia. Os seguintes países foram analisados no trabalho:

a. Estados Unidos: alto nível de adoção da tecnologia, usa algumas nuvens privadas e nuvens públicas em larga escala;
b. Australia: cauteloso com relação ao armazenamento dos dados fora do país, usa nuvens públicas, privadas e híbridas;
c. Japão: estratégia de criação de nuvem privada governamental (*Kasumigaseki Cloud*);
d. Reino Unido: estratégia de criação de nuvem privada governamental (G-Cloud);
e. Coréia do Sul: estratégia de criação de nuvem privada governamental e uso de provedores de nuvens nacionais (*Korea Cloud Computing* – KCC); e

f. Malásia: implementação de nuvem baseada em código aberto e nuvem privada (*Open Cirrus* e nuvem privada).

Jones et al. (2017) fez um estudo de caso em três instituições públicas do Reino Unido que adotaram os serviços de nuvem para atendimento ao cidadão, sob a luz dos riscos e ganhos da adesão a essa tecnologia. Dentre as lições aprendidas foi listada a seguinte: “As organizações do setor público precisam garantir que a solução de nuvem é segura de forma a garantir que os dados não são acessados por entes não autorizados”.

Um outro achado do estudo desenvolvido por Jones et al. (2017) foi que algumas instituições públicas, apesar de manter seus dados críticos em nuvens de terceiros, possuem localmente em suas instalações, *backups* confiáveis e criptografados desses dados como forma de obter conformidade com regulamentações locais.

Dessa forma, todas as referências indicam que a grande questão das instituições governamentais para a adoção da computação em nuvem na prestação de serviços públicos repousa principalmente sobre a necessidade de garantias relativas a segurança e a privacidade dos dados.

Wyld (2010) afirma que nos Estados Unidos a computação em nuvem é usada em várias áreas do governo federal, como na NASA, agências de defesa e até mesmo no Exército. E propõe uma estratégia de seis passos para as instituições públicas migrarem para nuvem:

a. aprender;
b. fazer avaliação organizacional;
c. elaborar projeto piloto
d. avaliar a prontidão para a nuvem;
e. estabelecer uma estratégia de implementação de nuvem; e
f. efetuar a melhoria contínua da nuvem.

Dessa forma, é importante que os governos que desejarem fazer adesão à tecnologia de computação em nuvem desenvolvam uma estratégia para tal, avaliando bem os riscos e as possibilidades trazidas.

Assaf, Hamsir e Muhammad (2021) concluem seu trabalho dizendo que os benefícios mais relevantes para que governos adotem a tecnologia de computação em nuvem são a efetividade dos custos, o aumento da escalabilidade e a segurança avançada, e em contrapartida, os principais riscos identificados são aqueles relacionados à privacidade e segurança dos dados.

É importante observar que a segurança aparece tanto como uma vantagem como um risco na adoção da computação em nuvem, porém trata-se de aspectos diferentes. Quando a segurança aparece como uma vantagem, diz respeito à existência de ferramentas de segurança gerenciadas por especialistas para a proteção da rede e dos dados, quando aparece como risco está voltada para a privacidade dos dados que estão numa infraestrutura de terceiros, neste caso é necessária uma relação de confiança entre o governo e o provedor de serviços que nem sempre é possível estabelecer.

Balasubramanian e Aramudhan (2012) afirmam que, em alguns setores, entre eles organizações governamentais, nos quais a absoluta segurança dos dados é necessária, as coisas devem ser feitas internamente, na própria instituição.

Nesse sentido, toma força a seguinte afirmação de Ahmed e Hossain (2014), “quando lidamos com computação em nuvem e seus problemas de segurança, tanto os fatores técnicos como epistemológicos são igualmente importantes para levar em consideração”.

Os Estados Unidos é, sem dúvida, o país mais avançado na utilização de serviços de nuvem para a prestação de serviços governamentais ao cidadão. Em 2011 o NIST já havia publicado a “NIST *Cloud Computing Standards Roadmap*” o que já preparava o caminho para a utilização de serviços de nuvem pelos entes governamentais americanos. Em 2013 foi publicada a segunda versão desse documento.

Em 2011, os Estados Unidos definiram a estratégia “*Cloud First*” para a modernização dos sistemas de TI governamentais por meio do documento, Vivek Kundra - U.S. Chief Information Officer (2011) “*Federal Cloud Computing Strategy*”.

Em 2019, este documento foi atualizado, Suzette Kent - U.S. Federal Chief Information Officer (2019) e mudou a estratégia *Cloud First* para *Cloud Smart*, como forma de acelerar o processo de migração dos serviços governamentais para a nuvem.

Nesta nova estratégia, Suzette Kent - U.S. Federal Chief Information Officer (2019), afirma que: “oferece guias práticos para implementação das missões do governo para atualizar a promessa e o potencial das tecnologias baseadas em nuvem enquanto garante uma execução que incorpore as realidades práticas”.

Essa tecnologia foi bastante amadurecida nos Estados Unidos, colocando este país na vanguarda na área de computação em nuvem. Não é de admirar que as grandes corporações fornecedoras de serviços de nuvem são americanas: Microsoft, Amazon, Oracle e Google.

Cabe salientar que o fato de os grandes provedores de serviço de nuvem serem americanos, faz com que os problemas relativos à segurança e privacidade dos dados são muito atenuados, pois é fácil manter a segurança trazida pela diversidade geográfica que a nuvem traz sem precisar armazenar os dados em território de países estrangeiros.

No Brasil, a Secretaria de Governo digital, por intermédio da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal, apresenta a estratégia governamental sobre a utilização de serviços de nuvem.

No que se refere a serviços de nuvem Brasil (2022) diz o seguinte:

> 4. CONTRATAÇÃO DE INFRAESTRUTURA DE CENTRO DE DADOS, SERVIÇOS EM NUVEM, SALA-COFRE E SALA SEGURA:
> 4.1. Os órgãos e entidades que necessitem **criar, ampliar ou renovar infraestrutura de centro de dados deverão fazê-lo por meio da contratação de serviços de computação em nuvem**, salvo quando demonstrada a inviabilidade em estudo técnico preliminar da contratação.
> 4.2. As contratações de serviços em nuvem devem **observar as normas correlatas publicadas pelo Gabinete de Segurança Institucional da Presidência da República - GSI/PR**.
> 4.2.1. Os órgãos e entidades devem exigir mediante justificativa prévia, no momento da assinatura do contrato, que fornecedores privados de serviços em nuvem possuam certificações de normas de segurança da informação aplicáveis ao objeto da contratação, assim como outros requisitos que objetivem mitigar riscos relativos à segurança da informação.
> 4.2.2. Os órgãos e entidades devem assegurar, por meio de cláusulas contratuais, que os serviços em nuvem a serem contratados permitirão a portabilidade de dados e softwares e que as informações do contratante estarão disponíveis para transferência de localização, em prazo adequado.
> 4.3. É vedada a contratação para criação ou ampliação de salas-cofre e salas seguras, salvo nos casos em que o órgão ou entidade tenha obtido autorização prévia do Órgão Central do SISP. (grifo nosso).

Em complemento à IN SGD/ME nº 94, a Secretaria de Governo Digital publicou as “Diretrizes para Contratação de Serviços de Computação em Nuvem” cujo extrato é apresentado a seguir, Brasil (2023):

> 1. Fica vedada a contratação de salas-cofre e salas seguras por órgãos integrantes do SISP.
> i. Solicitações de excepcionalização ao disposto no caput deverão ser submetidas pelo órgão, com as devidas justificativas, à apreciação da STI.
> 2. Compete à autoridade máxima do órgão, com apoio do Comitê de Governança Digital, do Comitê de Segurança da Informação e Comunicações e do Comitê Estratégico de Tecnologia da Informação, a definição dos **serviços de Tecnologia da Informação e Comunicação (TIC), no todo ou em parte, que possam comprometer a segurança nacional, conforme os requisitos de confidencialidade, integridade, disponibilidade e autenticidade das informações envolvidas,** em conformidade com a IN Nº 01 GSI/PR/2008 e suas Normas Complementares, e considerando os princípios de acesso à informação e sua imprescindibilidade à segurança do Estado e da sociedade, dispostos pela Lei nº Este documento de Boas práticas, Orientações e Vedações tem força normativa legal, estando vinculado à Portaria MP/STI nº 20, de 14 de junho

> de 2016, na forma de anexo, tendo sido assinado, em sua última versão, pelo Secretário de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão em 13/05/2016 e publicado na mesma data. 12.527, de 18 de novembro de 2011, Decretos nº 7.724, de 16 de maio de 2012, e nº 7.845, de 14 de novembro de 2012, e outras legislações específicas.
> 3. Para os casos de serviços de TIC que **não comprometam a segurança nacional**, incluindo Serviços de TIC Próprios, recomenda-se aos órgãos contratar preferencialmente **Nuvem Híbrida, como Modelo de Implantação,** de fornecedor público ou privado. Com isso, é possível valer-se dos benefícios dos modelos de nuvem pública (elasticidade e agilidade) e privada (desempenho garantido devido ao recurso dedicado), e ao mesmo tempo minimizar os riscos e otimizar os custos advindos de cada modelo.
> 4. Os órgãos deverão exigir, no momento da contratação de serviços em nuvem de fornecedores privados, que o ambiente do serviço contratado esteja em conformidade com a norma ABNT NBR ISO/IEC 27001:2013, sem prejuízo de outras exigências, objetivando mitigar riscos relativos à segurança da informação.
> 5. Para os casos de **serviços de TIC que possam comprometer a segurança nacional,** os órgãos devem contratar serviços de computação em nuvem com os órgãos ou entidades da Administração Pública Federal ou podem **realizar diretamente Serviços de TIC Próprios**.
> i. No caso dos Serviços de TIC Próprios, **quando comprometer a segurança nacional, sua operação não poderá ser compartilhada ou contratada de terceiros**. (grifo nosso).

A Instrução Normativa INSTRUÇÃO NORMATIVA Nº 5, DE 30 DE AGOSTO DE 2021 do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal, Brasil (2021), traz em seu Art. 17. o seguinte:

> Art. 17. Em relação ao tratamento da informação em ambiente de computação em nuvem, o órgão ou a entidade, além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais, deve observar as seguintes diretrizes:
> I - informação sem restrição de acesso poderá ser tratada em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação;
> II - **informação classificada** em grau de sigilo e documento preparatório que possa originar informação classificada **não poderão ser tratados em ambiente de computação em nuvem**; e
> III - poderão ser tratados em ambiente de computação em nuvem, observados os riscos de segurança da informação e a legislação vigente:
> a) a informação com restrição de acesso prevista na legislação, conforme o Anexo a esta Instrução Normativa;
> b) o material de acesso restrito regulado pelo próprio órgão ou pela entidade;
> c) a informação pessoal relativa à intimidade, vida privada, honra e imagem; e
> d) o documento preparatório não previsto no inciso II do **caput**. (GRIFO NOSSO)

Ainda nesta Instrução Normativa, o seu Art. 11. Define o seguinte:

> Art. 11. Antes de transferir serviços ou informações para um provedor de serviço de nuvem, os órgãos ou as entidades deverão, no mínimo:
> ...
> IV - utilizar, para os sistemas estruturantes, somente os modelos de implementação de nuvem privada ou de nuvem comunitária, desde que restritas às infraestruturas de órgãos ou de entidades;

Os Sistemas Estruturantes estão definidos em Brasil (2019).

Do exposto, fica evidenciado que vários países, mais ou menos desenvolvidos, já possuem ou estão desenvolvendo suas estratégias de uso de serviços de nuvem para melhorar o atendimento ao cidadão e otimizar os gastos públicos no investimento e custeio dos sistemas de tecnologia da informação.

Nesta esteira, o Brasil também começou a sua jornada neste sentido e já dispõe de Instruções Normativas e Diretrizes orientando os entes governamentais, porém ainda carece de uma estratégia detalhada para que este processo seja mais rápido, para que as adequações nas aplicações desenvolvidas para a nuvem e para que os riscos sejam minimizados, inclusive o risco de insucesso na migração para a nuvem e o retorno para a solução interna.

2.3 Utilização de Serviço de Nuvens por Instituições Militares

À medida que a tecnologia de computação em nuvem foi introduzida nos governos dos países em todos os continentes, a possibilidade de esta ser usada em proveito das forças armadas surgiu naturalmente. Hoje vários departamentos ou ministérios de defesa e forças armadas já tiram proveito das vantagens da computação em nuvem.

Segundo Zaerens (2011), os sistemas em nuvem que já foram apresentados publicamente, que trabalham em prol de forças armadas, não continham informações operacionais, de combate ou de missão crítica e os benefícios da computação em nuvem para as aplicações militares são os mesmos que são usufruídos por instituições civis.

As aplicações militares, não raramente, utilizam dados que podem comprometer a segurança nacional ou criar problemas diplomáticos, nesse sentido, Zaerens (2011) afirma que “Especialmente em sistemas militares, é crucial saber pelo menos onde os dados são processados e quais organizações e autoridades administrativas têm acesso a eles”.

No contexto militar, a utilização de serviços de nuvem deve ser analisada com cautela, deve ser levada em conta a possibilidade de o país entrar em algum tipo de conflito com o país sede do provedor de acesso à nuvem ou com algum país aliado a este.

Neste sentido, Zaerens (2011) ainda explica que nuvens privadas podem ser mais adequadas para certas atividades e do aspecto militar pode ser adequada a utilização de nuvens híbridas, desde que o acesso da nuvem privada para a pública

forneça uma visão ampla, mas o inverso deve ser limitado ou totalmente fechado, a nuvem pública não ter acesso à nuvem privada.

Dessa forma as atividades militares que tiverem relação com operações ou lidem com informações sigilosas seriam atendidas por uma nuvem privada e as atividades administrativas poderiam ser atendidas por nuvens públicas. Assim, Zaerens (2011) conclui: “Nós afirmamos que o núcleo operacional e sistemas táticos devem estar limitados pelas fronteiras da nuvem privada. Porém entendemos que a nuvens híbridas podem trazer mais capacidade para todo o sistema”.

De uma forma mais específica, Koo, Kim e Lee (2019) afirmam que a as Forças Armadas da Coreia do Sul estão considerando utilizar a computação em nuvem no sistema de comando e controle da defesa nacional e nesse contexto enfatizam a necessidade de uma arquitetura de segurança compatível com os requisitos militares.

Ainda segundo Koo, Kim e Lee (2019), os militares da Coreia do Sul estabeleceram o Data Center Integrado da Defesa (*Defense Integrated Data Center* – DIDC), que concentra os recursos computacionais das três forças armadas e provê o modelo de computação em nuvem (privada) de Infraestrutura como Serviço (IaaS) para alguns sistemas militares, porém ainda não há um esquema detalhado para a utilização de nuvem.

Segundo Koo, Kim e Lee (2019), existem problemas de segurança relativos à nuvem que não existem no modelo tradicional de computação, dessa forma é necessário adicionar alguns requisitos de segurança relativos à tecnologia de computação em nuvem para atender às necessidades do sistema de comando e controle militar.

O país mais avançado na utilização de serviços de nuvem pelas forças armadas são os Estados Unidos, este serviu de inspiração para os estudos de Koo, Kim e Lee (2019) e será objeto de uma análise mais detalhada mais adiante neste trabalho.

O Ministério da Defesa do Reino Unido possui uma diretriz estratégica para computação em nuvem para suas necessidades de tecnologia da informação, (FORTE, 2023).

Neste sentido, o referido documento, Forte (2023), diz: “O objetivo deste Roteiro Estratégico de Nuvem para Defesa é declarar a visão e a mudança transformadora necessária para que a Defesa consuma mais recursos de nuvem de classe mundial”.

No passado, o Ministério da Defesa do Reino Unido estabeleceu a MODCloud, Nuvem do Ministério da Defesa, que é uma mistura de serviços de nuvens públicas, privadas e híbridas.

Também foi lançado o CIRRUS para racionalizar os data centers, fechar os sistemas legados e suportar as suas migrações para a nuvem.

O planejamento para 2025 do Ministério da Defesa do Reino Unido consiste em:

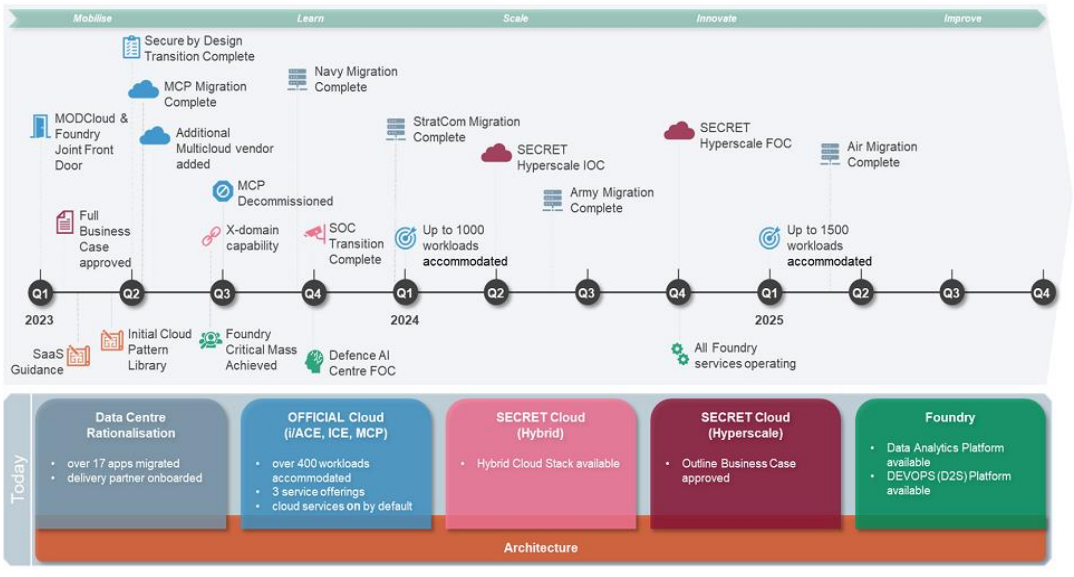
a. manter o princípio da MODCloud e continuar a adoção de nuvens públicas de acordo com a política "*Cloud First*" do governo;
b. adotar nuvens com múltiplas classificações sigilosas com uma mistura de nuvens públicas, privadas e híbridas, levando em conta as lições aprendidas nos requisitos existentes na MODCloud para informações secretas e ultrassecretas; e
c. fazer parcerias com grandes atores na prestação de serviços de nuvem.

Para implementar a grande nuvem da Defesa, os serviços serão entregues como IaaS, PaaS e SaaS, oferecendo o uso de nuvens públicas, privadas e híbridas.

A nuvem será o núcleo da integração dos serviços digitais da Defesa, dessa forma, será necessária também uma racionalização dos *data centers* da Defesa para tratar a obsolescência e prover uma hospedagem de sistemas com boa relação custo-benefício.

O objetivo do Ministério da Defesa do Reino Unido é utilizar ao máximo os serviços providos pelos grandes fornecedores de serviço de nuvem, porém ainda mantém alguma informação com classificação sigilosa sob sua posse direta. A Figura 3 apresenta o planejamento do Ministério da Defesa do Reino Unido.

Figura 3 – Planejamento do MD do RU para os próximos 3 anos



Fonte: Forte, 2023.

Com relação à utilização de serviços de nuvem pelas forças armadas dos Estados Unidos, estas estão em sintonia com as diretrizes do governo central de “*Cloud First*” e “*Cloud Smart*”.

Já no ano de 2012, o Departamento de Defesa dos Estados Unidos (DoD) publicou a sua Estratégia de Computação em Nuvem, indicando a utilização de serviços comerciais de nuvem de forma a incentivar a adoção dessa tecnologia.

Em 2018 esse documento foi atualizado, Shanahan (2018), e indicou a estratégia de múltiplas nuvens e múltiplos fornecedores de serviço (*multi cloud & multi vendor*) incorporando Nuvens de Propósito Geral e Nuvens de Propósitos Específicos (*General Purpose Cloud & Fit for Purpose Clouds*).

A Nuvem de Propósito Geral é a solução institucional para nuvem, e é chamada de JEDI (*Joint Enterprise Defense Infraestructure*), a maioria dos sistemas e aplicações ficam hospedados aí. Esta nuvem oferece serviços nos modelos IaaS e PaaS.

As Nuvens de Propósito Específico são usadas quando a JEDI não é capaz de atender aos requisitos da missão. Essas nuvens podem ser providas por fornecedores comerciais ou serem próprias do DoD. Serviços como correio eletrônico, chat e colaboração seriam fornecidos por uma empresa contratada, já o ambiente operacional fornecido pela Agência de Sistemas de Informação da Defesa (DISA) seria usado para as aplicações seguras do DoD.

Figura 4: Caminho do DoD para um ambiente de nuvens híbridas e múltiplos fornecedores

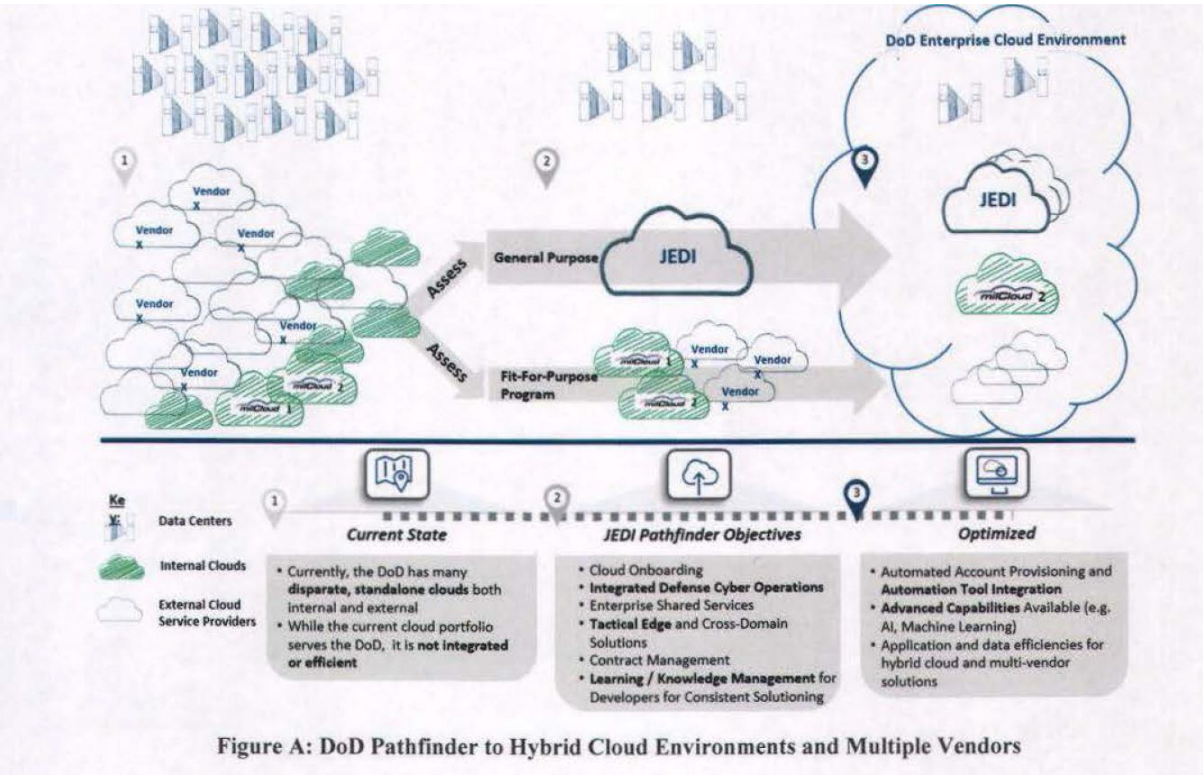


Figure A: DoD Pathfinder to Hybrid Cloud Environments and Multiple Vendors

Fonte: Shanahan, 2018.

Outro documento importante neste sentido foi publicado em 2019, a Estratégia de Modernização Digital do Departamento de Defesa, Norquist (2019), o documento é organizado em Metas, Objetivos e Estratégias.

As metas são:

1. inovar para ganhar vantagem competitiva;
2. otimizar para eficiência e aumento de capacidade;
3. evoluir a ciber segurança para uma postura de defesa ágil e resiliente; e
4. cultivar talentos para uma força de trabalho preparada digitalmente.

Dentro da Meta 1, o segundo objetivo “Entregar um ambiente corporativo de nuvem ao DoD para alavancar a inovação comercial” aparecem os seguintes elementos estratégicos, entre outros:

a. entregar a nuvem corporativa de propósito geral com capacidades computacionais e de armazenamento (JEDI); e
b. prover o ambiente de nuvem privado do DoD.

Neste contexto, o DoD não está abandonando a possibilidade de manter sistemas considerados críticos dentro de datacenter próprios, por intermédio de uma nuvem privada.

Ainda neste sentido, o objetivo 4 da Meta 1, “Tratar os dados como um ativo estratégico” traz, entre outros, o seguinte elemento estratégico: Investir e manter a infraestrutura necessária para tornar os dados do DoD visíveis, acessíveis, entendíveis, confiáveis e interoperáveis.

Já o objetivo 2 da Meta 2: “Otimizar os data centers do DoD” fala por si só. Este objetivo tem como um de seus elementos estratégicos: Migrar as aplicações e sistemas do DoD que não podem ser hospedados em nuvens comerciais para os data centers próprios.

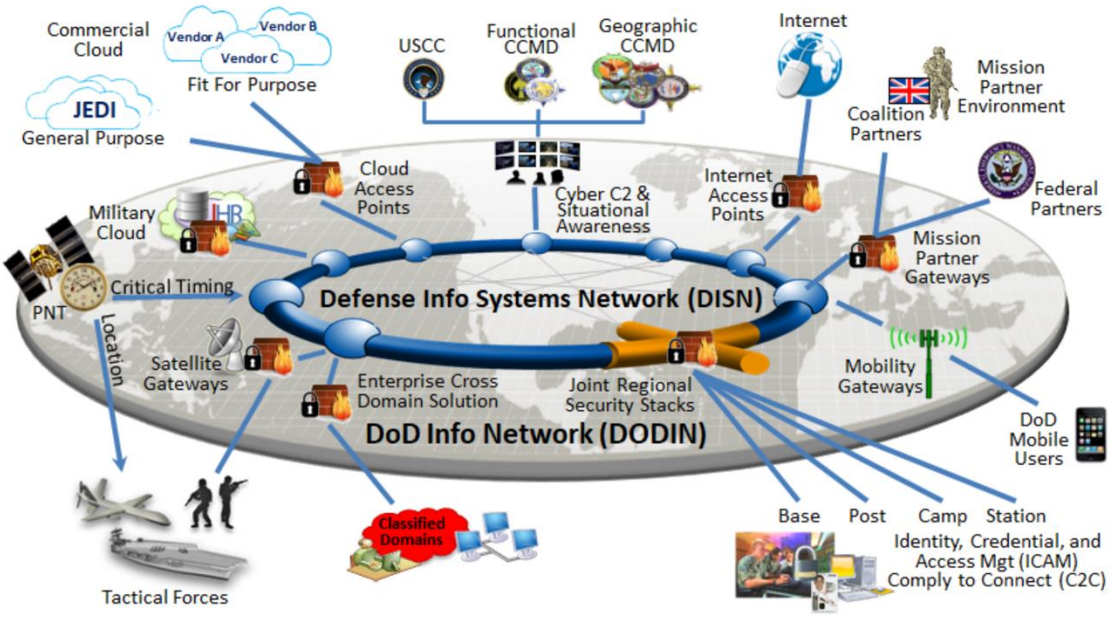
Dessa forma nota-se que a utilização dos serviços de nuvem públicas comerciais pelo DoD vai se dar de forma criteriosa e seletiva.

Norquist (2019) apresenta o Ambiente Conjunto de Informação (JIE – J*oint Information Environment*), uma estrutura com as iniciativas de modernização do DoD para obter superioridade de informação. Essa estrutura é apresentada no Figura 5.

Nessa estrutura pode-se perceber a existência de nuvens públicas comerciais, tanto a JEDI como as de propósito específico e também, a nuvem militar, própria do DoD.

Segundo Lebeda, Zalatoris e Scheerer (2018), seguindo a esteira do DoD, o Exército dos Estados Unidos também publicou a sua Estratégia de Computação em Nuvem no ano de 2015, porém foi além na definição do conceito de nuvem definido pelo NIST, considerando que a tecnologia de computação em nuvem também seria usada em condições operacionais (militares).

Figura 5: Escopo da estrutura do JIE



Fonte: Norquist, 2019.

Em 2022 o Exército dos Estados Unidos publicou o “Plano de Nuvem do Exército dos Estados Unidos”, Iyer e Puckett III (2022). Esta estratégia prevê a otimização de data centers nos Estados Unidos continental (CONUS) e implantações táticas de data centers fora dos Estados Unidos continental (OCONUS) de forma a obter segurança, resiliência e escalabilidade.

Os objetivos estratégicos dessa publicação são:

1. expandir a nuvem;
2. implementar a arquitetura de zero confiança;
3. permitir o desenvolvimento de softwares de forma rápida e segura;
4. acelerar decisões dependentes de dados;
5. melhorar as operações na nuvem;
6. desenvolver uma força de trabalho para nuvem; e
7. prover transparência de custos e contabilização.

Ainda segundo Iyer e Puckett III (2022), a Agência de Gerenciamento de Nuvens Corporativas (ECMA) e alguns parceiros estabeleceram o ecossistema de multi nuvem e nuvens híbridas do Exército dos Estados Unidos, cARMY. Esta nuvem corporativa é formada por nuvens públicas de propósito geral e privadas trabalhando em harmonia e

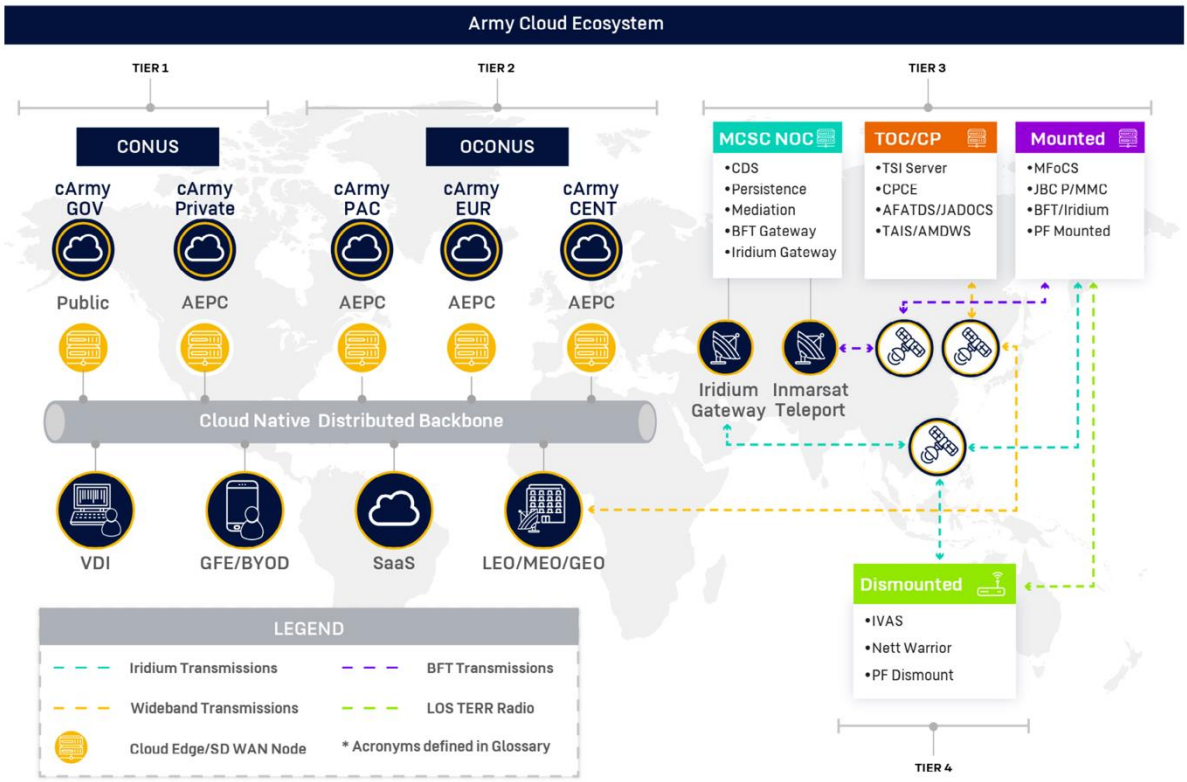
oferecendo os modelos de IaaS e Paas. Para os serviços de SaaS a cARMY serve como um intermediário para conectividade de forma a garantir a segurança e conectividade para todo o Exército.

O desenho desse novo ecossistema de nuvem do Exército americano é mostrado na Figura 6.

Com esse Plano de Nuvem do Exército dos Estados Unidos, Iyer e Puckett III (2022) definiram a seguinte intenção estratégica:

> O Exército deve adaptar os seus processos para ser mais ágil, suas redes para serem mais resilientes, seus ambientes de nuvens híbridas públicas e privadas para serem mais elásticos, os projetos de software comuns e direcionados para o campo de batalha mais nativos para nuvem, e as estruturas organizacionais e treinamentos para serem mais efetivos na guerra da informação.

Figura 6: Futuro ecossistema de nuvem do Exército americano.



Fonte: Iyer, Puckett III, 2022.

Apesar de ser o país sede da maioria dos grandes provedores de serviços de nuvem, o Exército dos Estados Unidos ainda prevê nas suas estratégias de adoção de serviços de nuvem a existência de infraestrutura própria, criando uma nuvem privada, para hospedar os dados mais críticos e as aplicações operacionais.

Mesmo entendendo que os dados classificados e operacionais, ficariam armazenados em território americano, as análises de risco não permitiram que o DoD ou

o Exército dos Estados Unidos deixassem esses dados sob controle de um ente privado civil, mesmo que sediado no território nacional.

Do exposto, pode-se entender que a estratégia mais implementada pelas forças armadas de uma forma geral é a utilização de nuvens públicas para as atividades mais administrativas e relacionadas à governança da instituição e a utilização de nuvens híbridas ou privadas para atividades mais táticas e operacionais ou que lidem com informações com classificações sigilosas.

Dessa forma, é fácil observar que a tecnologia de computação em nuvem está se espalhando em muitas forças armadas pelo mundo, pois é inegável que traz vantagens que podem ser exploradas por essas instituições, trazendo benefícios relevantes para as atividades tanto administrativas como operacionais e táticas.

A adoção da tecnologia de computação em nuvem já virou uma quase unanimidade entre as forças armadas, porém as formas de implementação variam de acordo com os benefícios pretendidos e os requisitos de segurança necessários e estabelecidos por cada país.

Nas Forças Armadas Brasileiras ainda não há estudos sobre a utilização da tecnologia de computação em nuvem de uma forma institucional, porém no exército Brasileiro já há iniciativas com o intuito fazer provas de conceito nessa área envolvendo os data centers institucionais.

3 CONSIDERAÇÕES FINAIS

A computação em nuvem é uma tecnologia que chegou para ficar, suas vantagens a tornam uma solução muito atrativa tanto para as organizações privadas quanto para instituições governamentais.

Dentre as principais vantagens da computação em nuvem estão otimização de custos, pois diminui drasticamente os custos de aquisição de hardware, a terceirização dos serviços especializados de TI, permitindo a instituição direcionar sua força de trabalho para a atividade fim e a elasticidade, de forma que a capacidade computacional disponível para o consumidor de nuvem pode crescer rapidamente frente a um aumento repentino da demanda pelos serviços e da mesma forma diminuir rapidamente quando a demanda diminuir, tudo isso de forma automática.

Dentre os principais problemas da tecnologia estão a segurança e a privacidade dos dados, pois os dados estarão sob a posse do provedor de nuvem e há uma incerteza sobre a localização física exata dos dados. Assim, os dados ficam sujeitos à acessos indevidos tanto por parte de outros consumidores do serviço de nuvem, quanto a funcionários do provedor de nuvem ou a governos com jurisdição sobre a região geográfica onde os dados estão armazenados.

Vários governos de nações estão usando ou possuem uma estratégia de uso de serviços de nuvem para a gestão dos seus serviços de TI e para oferecer serviços digitais ao cidadão (e-Gov). Cientes dos problemas inerentes à tecnologia, cada governo adota um modelo que esteja alinhado aos requisitos dos serviços e dos dados.

O país com a adoção de serviços de nuvem por parte do governo em estado mais avançado são os Estados Unidos. Para atingir esse nível de maturidade, desde o ano de 2011, várias diretrizes e estratégias foram lançadas, amadurecidas e atualizadas pelo governo central.

Em busca dos benefícios alcançados pelas empresas privadas e entes governamentais, os ministérios da defesa e forças armadas de vários países também apresentaram iniciativas no intuito de adotar serviços de nuvem para aumentar a eficiência administrativa e intensificar o poder de combate com base na guerra da informação.

Face aos problemas de segurança apresentados pelo modelo de computação em nuvem, as diferentes forças armadas tem adotado, em sua maioria, um modelo de nuvem híbrida, de forma que as atividades mais administrativas são atendidas por nuvens públicas e os dados com classificação sigilosa e as aplicações operacionais e táticas são atendidas por nuvens privadas ou híbridas, de forma a manter o total controle

sobre a localização geográfica, sobre a privacidade, sobre a segurança e sobre os preceitos legais e regulatórios existentes sobre os dados.

Assim, tecnologia de computação em nuvem é adequada para as aplicações militares. Para isso, deve ser elaborada uma estratégia abrangente para a adoção da tecnologia, as aplicações devem desenvolvidas de forma nativa para nuvem e a classificação dos dados e aplicações deve ser feita de forma meticulosa. Para isso, devem conviver os vários modelos de serviço em nuvem, IaaS, PaaS e SaaS além dos diferentes modelos de implantação, nuvem pública, nuvem privada, nuvem comunitária e nuvem híbrida, por conseguinte, os modelos e formas de implantação mais adequados aos requisitos individuais de dados e aplicações podem ser adotados de forma a atender plenamente as exigências de cada aplicação e conjunto de dados.

REFERÊNCIAS

AHMED, Monjur; HOSSAIN, Mohammad Ashraf. Cloud computing and security issues in the cloud. **International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1**, [*S. l.*], p. 25 - 36, 16 jan. 2014.

ALONSO, Juncal *et al*. Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review. **Journal of Cloud Computing: Advances, Systems and Applications**, [*S. l.*], p. 1 - 34, 12 jun. 2023.

ASSAF, Arief; HAMSIR, Ayub Wahab Iis; MUHAMMAD, Miftah. Benefits and Risks of Cloud Computing in E-Government Tasks: A Systematic Review. **E3S Web of Conferences 328, 04005 (2021)**, [*S. l.*], p. 1 - 7, 4 mar. 2021.

BALASUBRAMANIAN, R.; ARAMUDHAN, M. Security Issues: Public vs Private vs Hybrid Cloud Computing. **International Journal of Computer Applications**, v. 55, n. 13, p. 35-41, 25 out. 2012.

BEHL, Akhil; BEHL, Kanika. An Analisys of Cloud Computing Security Issues. *In*: WORLD CONGRESS ON INFORMATION AND COMMUNICATION TECHNOLOGIES, 2012. **Proceedings** [...]. [*S. l.*: *s. n*.], 2012. p. 109 – 114.

BHADAURIA, Rohit; SANYAL, Sugata. Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. **International Journal of Computer Applications**, [*S. l.*], 30 maio 2014.

BRASIL. Ministério da Economia. **Sistemas Estruturadores**: Administração Pública Federal. Brasília, DF: ME, 2019. Disponível em: https://www.gov.br/economia/pt-br/assuntos/sistemas-estruturadores. Acesso em: 4 out. 2023.

BRASIL. Ministério da Economia. Secretaria de Governo Digital. **Diretrizes para Contratação de Serviços de Computação em Nuvem nº 1, de 26 de junho de 2023**. Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem. Brasília, DF: ME, 2023.

BRASIL. Ministério da Economia. Secretaria de Governo Digital. **Instrução Normativa nº 94, de 23 de dezembro de 2022**. Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal. Brasília, DF: ME, 2022.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa nº 5, de 30 de agosto de 2021**. Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal. Brasília, DF: GSI, 2021.

FORTE, Charlie. **Paper Policy**: cloud strategic roadmap for defence. [*S. l.*]: Digital Functional Lead, 2023.

GALLAGHER, P. R.. A Guide to Understanding Data Remanence in Automated Information Systems. **The Rainbow Books**, 1991.

HEYDARI, Atefeh; TAVAKOLI, Mohammad Ali; RIAZI, Mohammad. An Overview of Public Cloud Security Issues. **International Journal of Management Excellence**, v. 3, n. 2, p. 440-445, June 2014.

HOGAN, M.; SOKOL, A. NIST Cloud Computing Standards Roadmap Version 2. Gaithersburg, MD: NIST, 2013. p.1-113. NIST Special Publications 500-291.

JAIN, Prince. Security Issues and their Solution in Cloud Computing. **International Journal of Computing & Business Research**, [*S. l.*], 2012.

JATHANNA, Rohan; JAGLI, Dhanamma. Cloud Computing and Security Issues. **Int. Journal of Engineering Research and Application**, [*S. l.*], p. 31 - 38, 21 jun. 2017.

JONES, Steve; IRANI, Zahir; SIVARAJAH, Uthayasankar; LOVE, Peter E. D. Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies. **Inf Syst Front (2019) 21**, [*S. l.*], p. 359 - 382, 12 abr. 2017.

KAUR, Randeep; KAUR, Jagroop. Cloud Computing Security Issues and its Solution: a review. *In*: INTERNATIONAL CONFERENCE ON COMPUTING FOR SUSTAINABLE GLOBAL DEVELOPMENT (INDIACOM), 2., 2015. **Proceedings** [...]. [*S. l.: s. n*.], 2015. p. 1198-1200.

KOO, Jahoon; KIM, Young-Gab; LEE, Sang-Hoon. Security Requirements for Cloud-based C4I Security Architecture. *In*: INTERNATIONAL CONFERENCE ON PLATFORM TECHNOLOGY AND SERVICE (PLATCON), 2019. **Proceedings** [...]. [*S. l.: s. n*.], 2019. p. 1-4.

KOSINSKA, Joanna; ZIELINSKI, Krzysztof. Autonomic management framework for cloud-native applications. **J Grid Computing,** [*S. l.*], p. 779 - 796, 26 set. 2020.

KUMAR, P. Ravi; RAJ, P. Herbert; JELCIANA, P. Exploring Data Security Issues and Solutions in Cloud Computing. *In*: INTERNATIONAL CONFERENCE ON SMART COMPUTING AND COMMUNICATIONS, ICSCC, 6., 2017. **Proceedings** [...]. [*S. l.*], 2017. p. 691-697.

LEBEDA, Frank J.; ZALATORIS, Jeffrey J.; SCHEERER, Julia B. Government Cloud Computing Policies: Potential Opportunities for Advancing Military Biomedical Research. M**ilitary Medicine**, v. 183, n. 11/12, p. e438-e447, Nov. 2018.

MOHAMMED, Fathey; IBRAHIM, Othman Bin. Drivers of Cloud Computing Adoption for E-Government Services Implementation. **International Journal of Distributed Systems and Technologies**, [*S. l.*], p. 1-14, 20 mar. 2015.

MOHAMED, Mohamed. **Generic monitoring and reconfiguration for service-based applications in the cloud**. 2015. Thesis (Doctorate degree Networking and Internet Architecture) - Institut National des Télécommunications, [*S. l.*], 2014.

OMOTOSHO, Oluyinka. I. A Review on Cloud Computing Security. **International Journal of Computer Science and Mobile Computing** , [*S. l.*], p. 245–257, 9 set. 2019.

RACKSPACE TECHNOLOGY (ed.). **Address cloud computing security concerns with private cloud**. [*S. l.*]: Rackspace Technology, 2023. Disponível em: https://docs.rackspace.com/docs/address-cloud-computing-security-concerns-with-private-cloud. Acesso em: 24 set. 2023.

REED, A.; REZEK, C.; SIMMONDS, P.. Security Guidance for Critical Area of Focus in Cloud Computing V3.0. **Cloud Security Alliance (CSA)**, 14 Nov. 2011.

SAXENAL, Tunisha; CHOUREY, Vaishali. A **Survey Paper on Cloud Security Issues and Challenges**. [New York]: IEEE Xplore, 2014.

SHANAHAN, PATRICK M. **DoD Cloud Strategy**. Washington, DC: Department of Defense, 2018. Disponível em: https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF. Acesso em: 29 set. 2023.

SHANAHAN, PATRICK M. **DoD Digital Modernization Strategy**. Washington, DC: Department of Defense, 2019. Disponível em: https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF. Acesso em: 29 set. 2023.

SHANAHAN, PATRICK M. **The U.S. Army Cloud Plan**. [*S. l.*]: Army, 2022. Disponível em: https://api.army.mil/e2/c/downloads/2022/10/14/106b220e/army-cloud-plan-2022.pdf. Acesso em: 30 set. 2023.

SOLTANI, Boubaker; GHENAI, Afifa; ZEGHIB, Nadia. Towards Distributed Containerized Serverless Architecture in Multi Towards Distributed Containerized Serverless Architecture in Multi Cloud Environment. *In*: INTERNATIONAL CONFERENCE ON MOBILE SYSTEMS AND PERVASIVE COMPUTING (MOBISPC), 15., 2018). **Proceedings** [...]. [*S. l.: s. n.*]. 2018. p. 121-128.

SUBASHINI, A.; KAVITHA,V.. A survey on security issues in service delivery models of cloud computing. **Journal of Network and Computer Applications**, v. 34, n. 1, p.1-11, 2011.

SUDAN, Randeep; BHATIA, Deepak; MELHEM, Samia; LEWIN, Anat; PETROV, Oleg. **E-Government.** New York: World Bank, 2015. Disponível em: https://www.worldbank.org/en/topic/digitaldevelopment/brief/e-government. Acesso em: 26 set. 2023.

SUZETTE KENT. Strategy. **Federal Cloud Computing Strategy**, [*S. l.*], 24 June 2019.

VENKATESH, A.; EASTAFF, Marrynal S. A Study of Data Storage Security Issues in Cloud Computing. **International Journal of Scientific Research in Computer Science, Engineering and Information Technology**, [*S. l.*], p. 1741–1745, 27 Feb. 2018.

VIVEK KUNDRA. Strategy. **Federal Cloud Computing Strategy**, [*S. l.*], 08 Feb. 2011.

WYLD, David C. The cloudy future of government it: cloud computing and the public sector around the world. **International Journal of Web & Semantic Technology (IJWesT),** v. 1, n. 1, p. 1 - 20, 12 Jan. 2010.

ZAERENS, Klaus. Enabling the Benefits of Cloud Computing in a Military Context. *In*: ASIA - PACIFIC SERVICES COMPUTING CONFERENCE, 2011. **Proceedings** [...]. [New York]: IEEE, 2011. p. 166-173.