Aprenda com quem faz

Segurança de Infraestrutura Cloud

Prof. Júnior A. Marostega

2023

SUMÁRIO

Capítulo 1. **Fundamentos e Conceitos sobre Cloud**

Introdução e propriedades da Cloud

Computação em nuvem é coisa do futuro, presente ou passado? Será que é algo em que possamos confiar? Isso não é para nossa empresa, prefiro ficar com minha estrutura sobre meus olhos uma vez que assim eu consigo saber de fato o que acontece. Será que vale a pena conhecer mais sobre computação em nuvem? Estas perguntas e estes pensamentos muitos profissionais se fazem, mas, a final, o que é computação em nuvem e para que serve?

Na literatura e em vários *frameworks* (ISO/IEC, NIST, CSA e outros) disponíveis existem algumas definições para o tema, de forma resumida e unificada sobre definimos o mesmo da seguinte forma, elasticidade, escalabilidade, disponibilidade e agilidade.

A computação em nuvem (*cloud computing*) é algo que surgiu para inovar, transformar e se tornou disruptivo. É um modelo que nos permite seu acesso à rede de modo onipresente, sendo conveniente sobre tudo e sob demanda a um determinado conjunto compartilhado de recursos da computação que nos permite realizar as diversas configurações. Tudo isso de forma ágil, simples e objetiva. (Fonte: NIST)

Quando definimos a elasticidade como um pilar importante da computação em nuvem, podemos entender que ela nos proporciona a flexibilidade de adição ou remoção de recursos computacionais, por exemplo, processamento e armazenamento. Estes podem ser aplicados em momentos pontuais a determinada demanda ou necessidade.

O potencial da escalabilidade em nuvem se remete a alternativa de tornar uma arquitetura flexível para variações de incremento ou redução de recursos computacionais em tempo real. Quando observado, este pilar

pode se tornar algo estratégico muito interessante para qualquer tipo de cenário e projeto, diante de determinadas situações conseguir atuar de modo estratégico e automaticamente, sem dúvidas que está ação direciona para um eixo de economia para uma estrutura computacional.

A disponibilidade é um fator que agrega em variados aspectos, uma vez que a nuvem nos permite ações sobre os pontos de falhas direcionando alternativas de redundâncias sobre os mesmos, sejam eles de equipamentos, processos ou serviços, automaticamente agregam a este pilar uma responsabilidade e alternativa de extrema relevância. As ações de disponibilidades que se tornam disponíveis são tratadas e projetadas para que tudo ocorra sem nenhuma intervenção técnica e de forma totalmente transparente aos usuários.

O fator agilidade acrescenta ao modelo de computação em nuvem elementos de decisão que podem ser observados e avaliados sob vários ângulos. Autonomia de agir imediatamente para agregar uma tecnologia, configurar um novo serviço, preparar uma arquitetura e estar disponível em poucos minutos ou segundos.

Dessa forma fica claro os pilares citados acima que definem de forma contextual a computação em nuvem (*cloud computing)*. De forma bem reduzida, foi descrito um pouco sobre as características de cada pilar. Porém, ainda existem muitas citações do mercado sobre todos esses pilares da computação em nuvem, levando em conta suas vantagens, outros contextos que podemos tratar totalmente como mitos e características que é possível avaliar para tirar os melhores contextos sobre o viés custo e benefício. São eles:

- A nuvem é sempre a melhor opção, pois reduz custos;
    - Mito: Cada situação deve ser avaliada de modo específico para se chegar a um denominador ideal.

- Você precisa estar na nuvem para ser “o” bom;
    - Mito: Ser bom ou ser ruim equivale ao aspecto estratégico e de negócio, a nuvem pode trazer benefícios que precisam ser analisados de modo relacionado a cada ambiente.
- A nuvem deve ser usada para tudo;
    - Mito: A nuvem pode sim trazer muitos benefícios, mas sempre o lado analítico é preciso entrar em ação. Não podemos confundir estruturas que nascem em nuvem com estruturas que nasceram em ambientes *on premises*. Fato é que sim, cada vez mais serviços estão sendo desenvolvidos e ganham avanços para serem realizado no modelo de nuvem, mas ambientes e situações diversas podem existir, então analise, e estratégia é o melhor caminho para, aí sim, tomar a melhor decisão.
- Precisamos de uma estratégia de nuvem que contemple um único fornecedor;
    - Mito: Atualmente muitas empresas estão trabalhando com estruturas multi-cloud, ou seja, mais de um provedor. E não existe regra se isso é certo ou errado. O que existe é resolver o seu problema da melhor maneira possível garantindo um ambiente seguro, estável e dentro de uma realidade de qual você pertence.
- A nuvem é menos segura que usar recursos locais;

- Mito: Na nuvem existem muitos recursos que se aplicados elevam o nível de segurança em uma estrutura. Os provedores visam muito a evolução e os cuidados sobre segurança, ou seja, pode ser mais vantajoso para as empresas de pequeno e médio porte que não tem recursos para inovar como provedores. Arquiteturas de *cloud* ou *on premises* necessitam de camadas de segurança, assim, ambas podem se equivaler neste quesito.

- A nuvem não é para uso de missão crítica;

  - Mito: Este é um pensamento bem comum, mas vamos refletir que os provedores nos disponibilizam uma série de ferramentas e serviços para executar estruturas tão robustas a comparação se fossemos investir em modo *on premises*. Será que as missões críticas são constantes? Lembre-se que com a nuvem podemos atribuir recursos e remover em dado momento de demanda, reflexo direto em uma operação precisa, estratégica e econômica.

Benefícios da Cloud

Atributos que podemos classificar como benefícios da adoção de arquiteturas computacionais baseadas em nuvem, segue abaixo:

- Virtualização de Recursos;
- Serviços sob demanda;
- Independência de Localização;
- Elasticidade e Escalabilidade;
- Medição de Serviços;

- Disponibilidade.

Estes são alguns destaques para definir o que podemos pensar e projetar sobre computação em nuvem. Assim, precisamos fixar que a computação em nuvem veio para abrir uma série de alternativas e agregar em aspectos econômicos.

> Capítulo 2

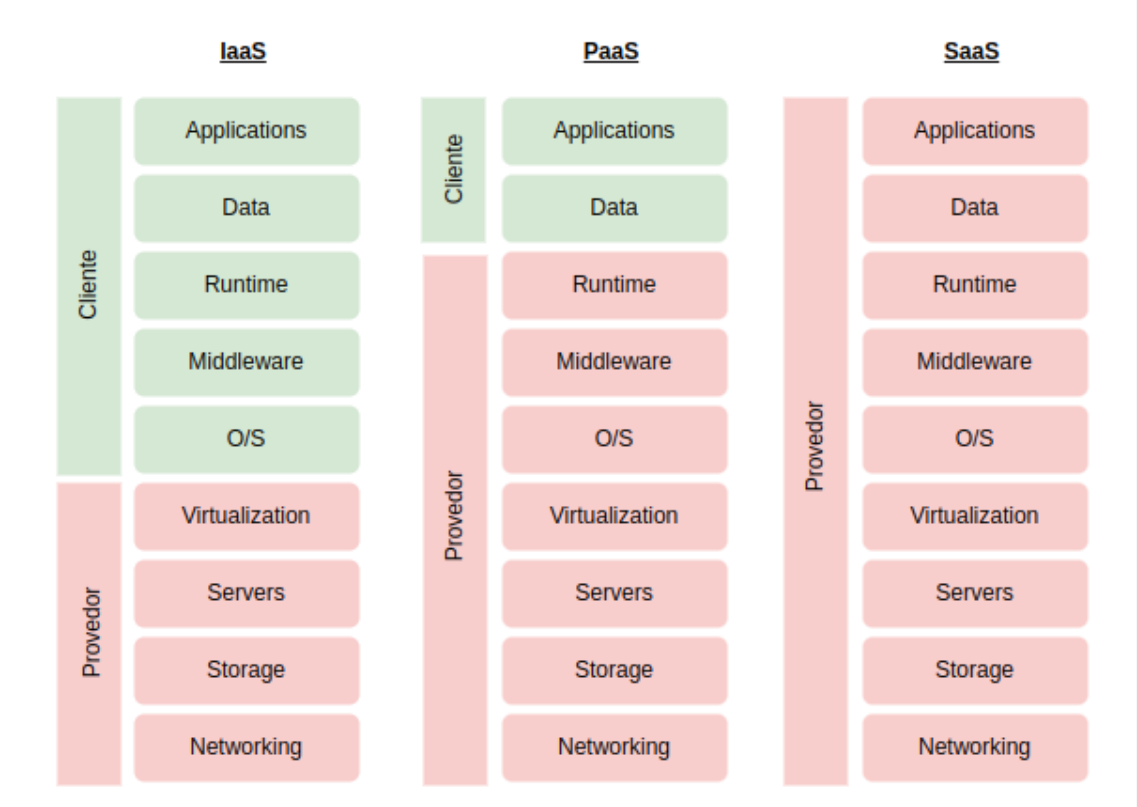
Capítulo 2. **Tipos de Serviços e Modelos Cloud**

Tipos de Serviços (IaaS, PaaS e IaaS)

É possível definir os tipos de serviços em três partes. Entende-se que diante destas partes o mercado desenvolve várias estratégias para disponibilizar ambos para o consumo e elaboração conforme determinadas necessidades. Observa-se que cada modalidade que é ofertada é um avanço sobre os recursos computacionais disponíveis e de responsabilidade do provedor e do cliente, conforme a Figura 1.

- Infraestrutura como serviço ou IaaS;
- Plataforma como serviço ou PaaS;
- Software como serviço ou SaaS.

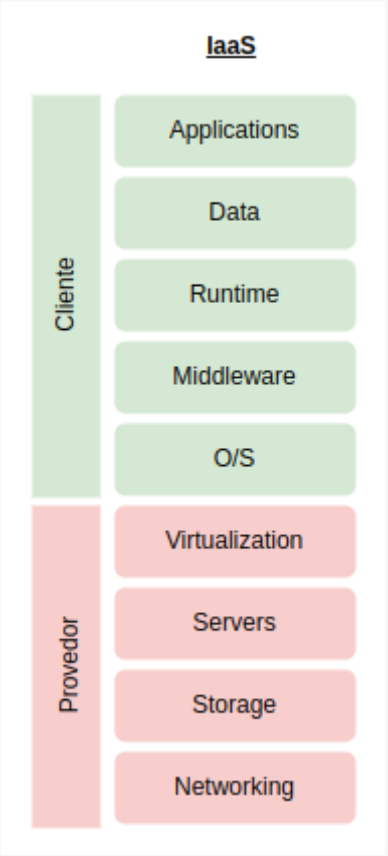
Figura 1 – Modelos de Serviços.



IaaS: Quando se escolhe a modalidade de infraestrutura como serviço, entende-se que o provedor vai entregar ao cliente os recursos mais básicos, ou seja, conforme a ilustração da Figura 2, visualizamos até a camada de virtualização. Nesta arquitetura o cliente passa a tomar ações da camada de Sistemas Operacional até aplicação.

Detalhes que devem ser levados em consideração neste modelo, uma vez que o cliente terá mais flexibilidade sobre suas ações, automaticamente suas responsabilidades também aumentam, já que a carga de recursos a ser administrada e gerenciada é maior.

Figura 2 – Modelo de Serviço IaaS.

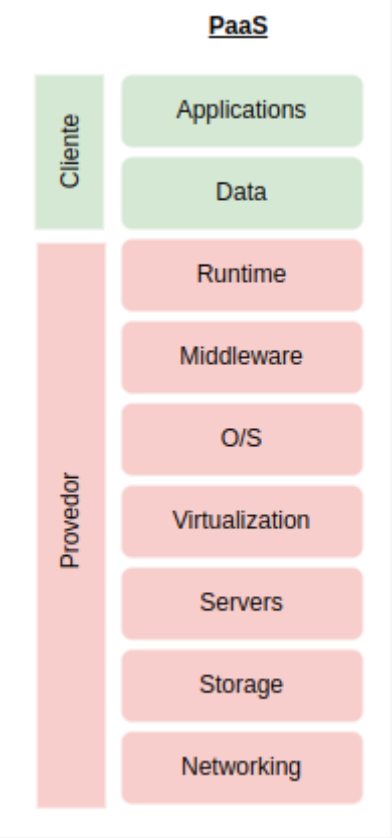


PaaS: Na opção de Plataforma como serviço, observamos que a entrega por parte do provedor é mais avançada, ou seja, a estrutura que ele vai entregar é maior, conforme Figura 3. Neste caso, o cliente tem

disponível uma plataforma pronta para que seja possível o desenvolvimento de suas atividades.

Um exemplo é a plataforma para hospedagem de um servidor web com banco de dados. Desta maneira o cliente atua apenas na camada da plataforma realizando as ações dela em diante. Vale destacar que esta modalidade entrega todos os componentes abaixo sem que o cliente final se preocupe em administrar, custear ou licenciar qualquer outro serviço, exemplo: Licença Sistema Operacional, *Hardwares* (memória, armazenamento), entre outros.

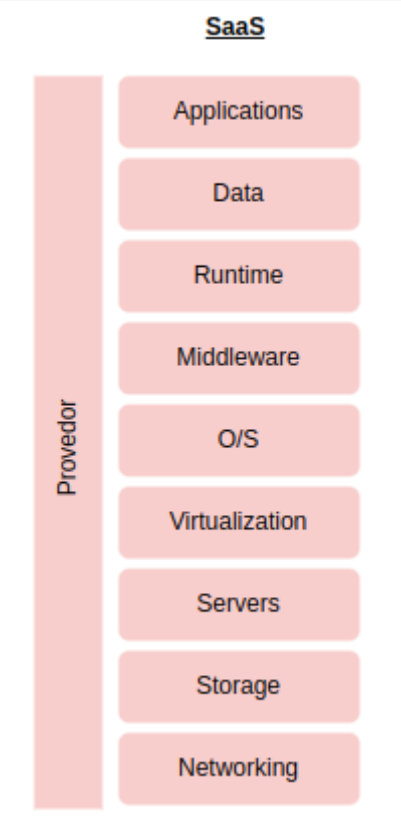
Figura 3 – Modelo de Serviço PaaS.



SaaS: Este formato entrega ao cliente toda estrutura pronta. Ele vai atuar apenas no uso e consumo do serviço. Esta modalidade isenta o cliente de qualquer ação referente a administrar os componentes da

estrutura. Este modelo é muito usado no mercado atualmente, exemplo: Google Drive, Office 365, Dropbox, serviços de *Streaming* entre outros.

Figura 4 – Modelo de Serviço SaaS.

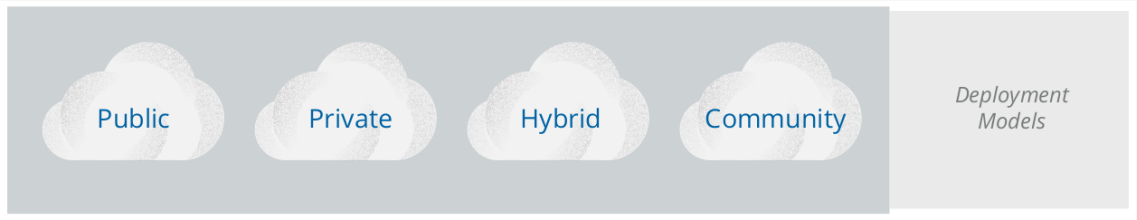


Modelos de Serviços em Computação na Nuvem

Um outro fator que é muito importante quando analisamos a estrutura de computação em nuvem (*cloud computing*) é entender que existem alguns tipos que carregam algumas características específicas. Entender sobre estes tipos significa dominar estrategicamente o negócio e adaptar-se a cada oportunidade levando em conta determinadas necessidades.

Algumas literaturas podem resumir, mas vamos levar como referência o *framework* CSA (*Cloud Security Alliance*) que destaca: Nuvem Pública, Privada, Hibrido e Comunitária.

Figura 5 – Tipos de Serviços.



Fonte: CSA Security Guidance - V4.0.

Nuvem Pública: Este serviço pertence a um provedor que compartilha os recursos computacionais e os clientes consomem sobre suas devidas características e demandas. Nesta configuração, os recursos são compartilhados para várias organizações que fazem o consumo dela através de um acesso usando internet pública.

Nuvem Privada: Este serviço, como o próprio nome já descreve, indica que é uma arquitetura baseada em uma rede e que os recursos só podem ser acessados para outros apenas sob autorização. Ou seja, existe uma arquitetura direcionada e totalmente exclusiva para um determinado cliente ou organização. Importante destacar que, por mais que sua estrutura seja privada, a mesma pode ser acessada através da internet.

Nuvem Híbrida: Este cenário é uma mescla entre nuvem pública e privada em um mesmo projeto ou ambiente. Este modelo costuma ser uma porta de entrada para empresas que estão migrando suas arquiteturas de *on premises* para *cloud*.

Nuvem Comunidade: Estrategicamente organizado por um determinado conjunto de pessoas, empresas ou projetos que combinam interesses semelhantes. Nesta estrutura os dados podem ser compartilhados como recursos computacionais. Ela pode ser consumida

em territórios restritos ou abertos (internos ou externos) de determinada comunidade, empresa ou sociedade.

> Capítulo 3

Capítulo 3. **On premises vs Cloud**

Arquiteturas

Com o passar do tempo a tecnologia ganhou novas formas, possibilidades e tudo gira entorno dessas inovações, modelos, estruturas etc. A evolução nos colocou em uma determinada característica que é o consumo de componentes de tecnologia sobre a ótica de aquisição. Ou seja, fazer aquisição dos componentes para montar sua estrutura, as empresas (pequena, média ou grande) até hoje desfrutam desse modelo.

O modelo que classifica essas ações de realizar aquisição de uma estrutura é conhecido como *on premises*. Na prática, resume que uma vez feito aquela aquisição a responsabilidade de armazenar, monitorar, proteger, prestar suporte, garantir o funcionamento dele acaba ficando sobre o círculo da companhia. Estes dispositivos podem ser vários itens: Computadores, Servidores, *Storages*, entre vários outros.

Com a evolução, novas tendências e soluções foram surgindo e a partir disso outros modelos se destacaram, como exemplo a computação em nuvem (*cloud computing*). Este modelo oferece todo um apanhado de tecnologia de forma personalizada, ágil, segura, sem a necessidade de fazer grandes investimentos imediatos. Ou seja, não há necessidade de comprar mais recursos computacionais, uma vez que temos isso disponível para montar uma estrutura computacional conforme determinada necessidade.

Como já explicado acima nos modelos e tipos de serviços de nuvens, as variedades são amplas, o que nos leva cada vez mais buscar entender cada situação para direcionar o uso adequado e entender sobre as devidas responsabilidades que cada oferece.

Desafios On premises vs Cloud

Em muitas empresas as estruturas ainda seguem todas no modelo *on premises* e certamente ainda ficarão por um bom tempo. Quando se projeta o uso de computação em nuvem é visível que existem ainda um grande medo, e talvez receio, por parte de muitos profissionais. Esse medo em muitos casos está vinculado à falta de conhecimento avançado que a modalidade nuvem pode agregar ao seu projeto ou necessidade.

A falta de entender mais detalhadamente os pontos que as estruturas de nuvem podem agregar ainda torna todo esse mecanismo de virar a página um grande dilema e desafio. Por outro lado, em muitos casos a falta de conhecimento destaca vários projetos com muitas falhas em cenários de migrações. As grandes perguntas realizadas por muitos empresários e técnicos são: a nuvem é segura? Se nós migrarmos para nuvem vamos estar seguros? Todas estas especulações circulam dentro de várias companhias e acabam tornando uma grande possibilidade passivo de fracasso.

Deve-se compreender que dentro de uma estrutura *on premises* tudo é sobre a responsabilidade da empresa, inclusive a segurança local de acessos e outros. E quando é visualizado o cenário nuvem, se o projeto desenhado e estruturado da maneira correta, coloca a empresa em um nível de segurança que ela nunca imaginou e também a deixa sem preocupações sobre estes aspectos, assim abrindo um *gap* de tempo para as empresas se preocuparem com o que as importa, seus negócios e não suas estruturas ou serviços.

> Capítulo 4

Capítulo 4. **Segurança em Cloud**

Modelo de Processo

Quando arquitetamos uma estrutura *on premises*, o nível de análise é amplo, uma vez que envolve desde uma estrutura de armazenamento de servidores e periféricos de T.I até o comportamento dos usuários. No momento em que nossa estrutura é toda direcionada para nuvem, o nível de ação que teremos difere, já que se inicia na confiabilidade de nossos provedores e vai até ações e comportamentos usuais dos usuários.

Como escolher e modelar uma estrutura apropriada que garanta um nível de segurança adequado? Para isso existem vários *frameworks* disponíveis no mercado. Também é importante destacar que cada camada em que se deve olhar pode haver uma mescla de *frameworks*. Mas, diante das opções, é preciso entender e definir os objetivos para depois adequar cada norma, *framework* políticas, entre outros.

O que soma a escolha de um bom *framework* e desenvolvimento de boas políticas é buscar entender que muitos destes são desenvolvidos, atualizados e praticados, isso devido ao envolvimento de comunidades, órgãos competentes que focam em equalizar e padronizar determinadas estruturas. Importante entender que empresas de níveis estratégicos elevados também aderem a estes modelos, contudo, seguindo modelos de *compliance* atrelados a determinadas estratégias.

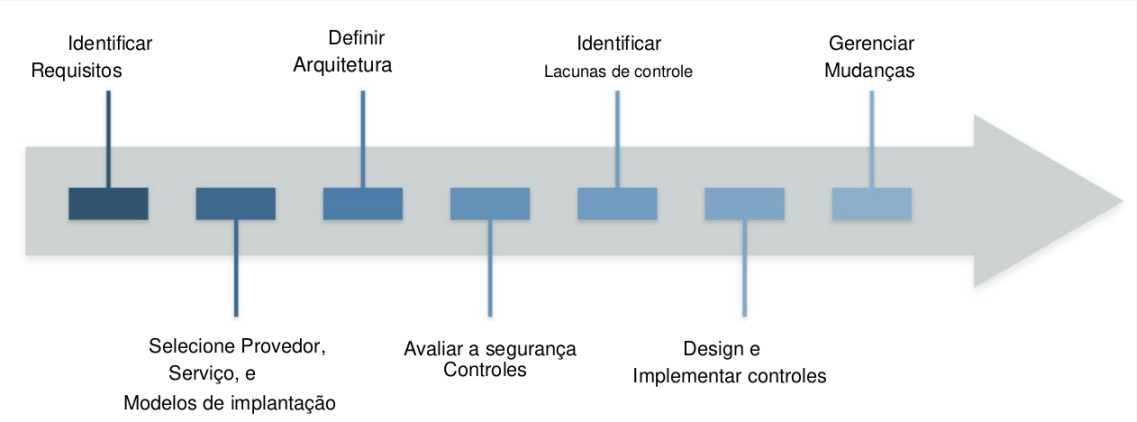
Por fim, vale deixar claro que *frameworks* são vários processos e políticas definidos e prontos para inserir na prática. Estes visam a implementação e gestão de contextos conectados à segurança da informação dentro de uma determinada organização.

Para projetar uma estrutura de segurança a uma determinada arquitetura computacional, se pode definir detalhes que facilitam este processo.

- Identificar os requisitos referente a segurança e conformidade necessários e quaisquer controles existentes.
- Selecionar um provedor de *cloud*, serviço e modelo de implantação.
- Definir os controles de segurança.
- Identificar as lacunas de controle.
- Projetar e implementar controles para preencher as lacunas.
- Gerenciar as mudanças ao longo do tempo.

Diante disso, é importante destacar que em cada projeto pode haver pontos de decisão, detalhes que independente de seus provedores devem ser avaliados de forma extremamente individual. A chave de tudo é identificar os requisitos, projetar a arquitetura e identificar as lacunas com base nos provedores (CSA -Security Guidance V4.0).

Figura 6 – Modelo de Processo de Segurança em Nuvem.



Fonte: CSA Security Guidance - V4.0.

Endpoints e Cloud Security

Os *Endpoints* são uma peça muito importante que acrescenta de forma estratégica mais uma garantia à segurança sobre o ambiente *cloud*. Para esclarecer sobre os *endpoints*, podemos definir como dispositivos de ponta (*Laptop, smartphone, desktop* e outros) que atuam em arquiteturas de uma organização. Esses dispositivos acabam conectados a uma determinada rede que tem suas variadas funções, e que também acessam serviços, aplicações e arquivos que estão vinculados à nuvem.

As ações desses dispositivos são tamanhas que os cuidados devem ser levados em conta, uma vez que os usuários de ponta estão atuando com suas variadas atividades rotineiras. Pensando em desenvolver algumas orientações que podem ser customizadas, alteradas e tratadas, pontos importantes devem ser observados, como:

- Criação de política e procedimentos;
- Gestão sobre os dispositivos (*Endpoints*);
- Criptografia sobre dados, transição de dados e armazenamento de dados;
- Prevenção na detecção de *anti-malware*;
- DLP;
- Regras sobre dispositivos e acessos terceiros;
- Isolamento de pontos de acessos.

SIEM

O SIEM é um apoiador muito estratégico para as companhias, uma vez que este atua na coleta, armazenamento e análise de informações relacionados à segurança de uma infraestrutura global, sua ação, dada às

devidas características, é apoiar em comunicação e alerta a determinados especialistas ou departamentos sobre ações pontuais de ataques.

Os ativos de uma empresa, que são atributos de preocupação e de referência para uma estratégia de proteção, podem ser conectados ou integrados aos sistemas SIEM. Assim facilitando e centralizando nas informações e monitoramento dados eventos. Como este modelo pode ser implementado através de serviço ou de forma local, destaca-se:

Modelo *Cloud* como referência:

- A *cloud* isenta aquisição de *hardwares*;
- É possível na *cloud* os incrementos de situações elásticas;
- É possível na *cloud* a escalabilidade de forma pontual;
- Ganha-se agilidade com recursos instantâneos disponíveis;
- Desenvolvimento de processos e ações automáticas quando identificado pontos de incidentes;
- Incremento de atributos de inteligência artificial.

> Capítulo 5

Capítulo 5. **Ambientes, Tecnologias e Recursos de Cloud**

Ambientes e provedores Cloud

Atualmente, nos deparamos com inúmeros provedores de serviço para a computação em nuvem, principalmente se aprofundar uma pesquisa em provedores regionais. E quando temos variedades de provedores de serviços, as escolhas se tornam mais complexas, devido a inúmeras perguntas que surgem, o que acaba sempre pesando uma escolha. Diante de várias opções, especialistas devem sempre entender os seus negócios para filtrar suas demandas a fins de encontrar soluções onde serão viáveis determinado projeto ou dado momento de necessidade.

Os provedores mais conhecidos como modelo público atualmente são AWS (Amazon), Azure (Microsoft), Google (GCP), Alibaba Cloud, Oracle e IBM. Segundo o quadrante mágico de *Gartner*, os provedores que se destacam são os representados na Figura 7.

Figura 7 – Quadrante Mágico de Gartner 2021.

Fonte: https://www.gartner.com/technology/.

Tecnologia e recursos Cloud

Estamos passando por um grande momento no mercado atual em que provedores de nuvem, principalmente pública, estão em um momento de transição com relação a suas tecnologias e serviços. Momentos passados, cada provedor adotava suas estratégias pontuais e criava suas diretrizes, o que forçava muitas vezes cada empresa a tomar decisões únicas em relação a consumir determinado produto ou serviços. Como é o mercado quem demanda o ritmo em muitos casos, as empresas estão cada vez mais adotando estratégias de trabalhar com mais de um provedor em simultâneo, porém, para isso ser possível, essas arquiteturas precisam se comunicar, este é o grande ponto em que estamos cada vez mais vivenciando atualmente, a flexibilização e conexão entre esses *players*.

Os provedores entenderam que quando suas arquiteturas se fazem flexíveis a ponto de realizar a comunicação de várias tecnologias, seus clientes visam cada vez mais a prática de mudança em relação aos ambientes *on premises x cloud*. Podemos descrever o avanço diário de produtos e serviços relacionados a *Big Data*, IoT (Internet das coisas), *Data Science*, Robotização (RPA), entre várias outras. Vale reiterar que estas evoluções acontecem em vários provedores de forma simultânea, o que é muito bom para os clientes que ganham alternativas variadas para inovação. É importante citar que com o avanço da infraestrutura de rede 5G essas mudanças e demandas tendem a crescer.

Dado contexto que crescem as alternativas, ferramentas, serviços em arquiteturas de multi-cloud e tudo mais, a conexão para que tudo isso funcione e seja administrado de forma precisa e dentro de um cenário mais objetivo possível é a partir da gestão automatizada, ou seja, conforme estas arquiteturas vão ganhando cada vez mais componentes, elas precisam de formas e modos para serem manipuladas em um curto espaço de tempo, o que descrevemos como orquestração, otimização

automatizadas. Atenção, porque aqui estão surgindo muitas carreiras promissoras a fim de suprir essas necessidades.

As arquiteturas computacionais ganham cada vez mais a atenção para serem adequadas com inúmeros serviços e de fácil manipulação. O crescimento em uso de arquiteturas relacionadas a *containers* vem sendo destaque no mercado, uma vez que as empresas lançam novos serviços ou fazem o processo de migração de seus respectivos serviços locais para nuvem. Os containers são conhecidos tanto pela agilidade quanto pela sua portabilidade. Ao construir armazenamentos de dados ou serviços com essa abordagem, se facilita realizar a movimentação com eficiência em ambientes multi-cloud.

A inteligência artificial é uma tecnologia que hoje está no core de muitas empresas, inclusive nas estratégias de vendas, “o produto XYZ é baseando no uso de inteligência artificial.” Este recurso de fato é um atributo que auxilia em vários aspectos, pode ser diretamente em um produto final, pode ser em automações, comportamentos e dentre vários outros. Os provedores estão investindo cada vez mais neste atributo para levar aos clientes a flexibilidade e diversidade em usufruir do mesmo.

Ou seja, a computação em nuvem está cada vez mais incorporada nos serviços mais básicos que consumimos. Com a computação em nuvem o limite para estruturar produtos, soluções e serviços ganham benefícios tão quão específicos como dinâmicos e estratégicos. Independente do provedor que visualizarmos, precisamos atender as nossas necessidades e ter autonomia para produções de pequena a larga escala, contando com ferramentas de ponta e precisão ordenada.

> Capítulo 6

Capítulo 6.

WAF (Web Application Firewall)

Sobre Web Application Firewall

O WAF, como conhecido, é uma ferramenta que atua na camada 7 (sete) com base de referência ao modelo OSI (camada de aplicação), ou seja, ele fica localizado entre a aplicação e a internet. Seu principal objetivo é fornecer segurança garantindo que determinadas ações de chamadas, sejam elas de entradas ou saídas, sejam barradas de acordo com as regras que podem ser pré-definidas. Já sua arquitetura funciona através de uma aplicação ou através de um serviço.

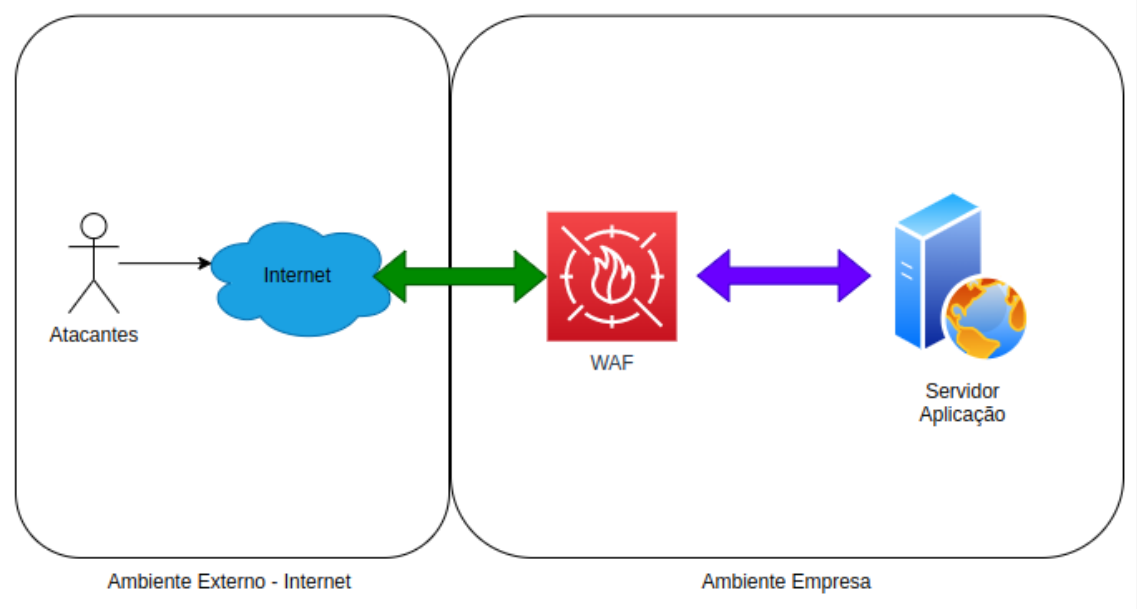
Alguns exemplos de proteção que um WAF realiza:

- Spammers;
- DDoS;
- Injeções SQL;
- Cross Site Scripting (XSS);
- Violação de protocolo HTTP;
- Injeção de comandos;
- Divisão de Respostas HTTP;
- Inclusão remota de arquivos;
- Anomalias de protocolo HTTP;
- Robôs (bots), crawlers e scanners;
- Ataques mais simples e comuns.

Prática Web Application Firewall

Vamos entender um pouco mais, na prática, mostrando alguns exemplos de arquiteturas WAF.

Figura 8 – Exemplo I - Atuação do WAF.



Na Figura 8 a representação é simples, ou seja, a localização do WAF é depois da aplicação e antes da internet, dessa forma todas as requisições que são recebidas da Internet o WAF atua antes de chegar até a aplicação.

Existem muitas soluções de WAF disponíveis no mercado, entre elas:

- CloudFlair;
- Barracuda;
- Topia;
- Trend Micro Cloud One;
- Stackpath.

> Capítulo 7

Capítulo 7.

Contingência e Continuidade Cloud

Plano de Contingência e Disaster Revery

A continuidade do negócio e a recuperação de desastres precisam de atenção, levados em consideração e categorizados como pontos de extrema importância em arquiteturas de computação em nuvem. Aqui os fatores podem ser mais complexos que ambientes *on premises.*

No *framework* CSA, destaque-se três aspectos:

- A garantia da continuidade e recuperação em um determinado provedor de nuvem (*cloud*).
- A preparação e gerenciamento de interrupções de provedores de nuvem.
- Alternativas de realizar a migração ou portabilidade de uma infraestrutura entre provedores.

Conforme uma arquitetura é projetada e elaborada, o grau de ações, responsabilidades sobre os aspectos de contingência e recuperação variam, ou seja, arquiteturas de IaaS, PaaS e SaaS possuem diferentes pontos de responsabilidades.

Sobre o plano de continuidade, quando realizado um planejamento sobre uma determinada arquitetura se faz valer sobre a viabilidade de um projeto, os provedores de nuvem possuem muitos recursos para diferentes abordagens de continuidades, é preciso entender que o excesso pode comprometer um cenário de tecnologia demandando um alto custo de gestão sobre e um elevado custo financeiro para manter.

A estratégia de identificar um provedor que vai atender a determinadas demandas, ter informações precisas da operação dele, como

estatísticas da estrutura em manutenção, off-line ou qualquer demanda que possa comprometer uma operação, se fazem de extrema importância para uma escolha de um serviço adequado, com plano de contingência que faz sentido.

Os provedores de nuvem se encontram espalhados por “n” países, “n” regiões e enfrentam problemas de funcionamento e disponibilidades. Ignorar isso é um equívoco, mas entender os pontos em que recursos pontuais podem estar disponíveis para determinadas estratégias demonstra maturidade e preservação de um cenário ativo.

Para auxiliar, vamos destacar alguns pontos abaixo:

- A elaboração de uma arquitetura para falhas.
- Entender que qualquer ponto existe um risco, levar este em consideração e tomar precauções sobre.
- Arquitete e elabore um projeto pensando sempre em disponibilidade, entendendo o que o provedor tem de opções para este.
- Tenha um plano para falhas pontuais do provedor de nuvem.
- Atenção nas escolhas e focar em provedores com maiores índices de disponibilidade.

Concluímos este assunto reiterando sobre entender cada problema, desenvolver um projeto adequado, esboçar e identificar pontos críticos, calcular sobre uma viabilidade e aceitação de cada negócio ou risco do projeto, escolher um provedor que mais se enquadra com as características e ficar atentos às melhorias, alterações, tecnologias para manter toda operação e viabilidade do projeto no aceite e riscos adequados para as operações.

Backup em Cloud

Uma estrutura de cópia dos dados baseada em nuvem adere a ações que entregam alguns pontos estratégicos diferentes para serem analisados em suas arquiteturas computacionais. Os *players* (empresas) atualmente têm disponíveis uma série de serviços, planos e recursos para que toda a estrutura de cópia seja realizada junto ao provedor.

Quando falamos de cópia (*backup*) em nuvem, é preciso entender que existem diversos tipos e para diversas situações, desde aquele backup para ser realizado uma vez por ano e arquivado por vários anos até aquele que deve ser realizado no intervalo de horas ou minutos entre si. Logicamente, cada necessidade retém de uma variação de requisitos e dos custos.

Não podemos pensar em arquiteturas em nuvem e não entender e projetar uma estrutura de cópia (*backup*), seja ela de uma arquitetura completa, dados, aplicações ou outros pontos. A importância de projetar uma boa estrutura de *backup* vai até ao ponto em que garantimos a sobre vida de uma organização.

As opções são variadas, sendo possível desenvolver estratégias de execução e alocação dos *backups* em cenários como multi provedores de nuvem. Desta forma os dados não ficam retidos em um único ponto ou provedor. Isso não quer dizer que os provedores são ou possuem um rótulo de confiança, mas isso vem ao encontro de muitas políticas de empresas que adotam as políticas de distribuição de serviços em mais de um ponto.

> Capítulo 8

Capítulo 8. **Segurança de Dados e Aplicações**

Governança da Informação

Quando o assunto é segurança da informação a premissa básica, é garantir a proteção dos dados, aplicações e ativos de uma determinada companhia. Este modelo de flexibilidade no âmbito computacional que a computação em nuvem agrega, ao mesmo tempo, ela desafia em pontos como uma boa governança, gestão, técnicas, ferramentas, processos, entre outros.

Podemos definir Governança de Informações, de acordo com *framework* (CSA -Security Guidance V4.0), como:

"Garantir que o uso de dados e informações esteja em conformidade com as políticas, padrões e estratégias organizacionais - incluindo objetivos regulatórios, contratuais e de negócios".

No Brasil hoje temos a Lei Geral de Proteção de Dados que nos coloca a um degrau a mais para entender e nos precaver da forma em que tratamos e manipulamos os nossos dados pessoais. Dentro de uma companhia, a mescla de dados corporativos e pessoais se misturam e torna este atributo de proteção algo a ser planejado e revisado de forma constante.

Elaborar um bom plano de governança sobre uma organização, projeto ou qualquer outro atributo específico é entender que quando se tem um dado puro, este pode não possuir nenhum tipo de valor sobre si, mas quando é unificado, um conjunto de dados, estes vão gerar uma informação. Desta forma, entender a geração, armazenamento, controle, manipulação dos dados pode definir tecnologias, estratégias e

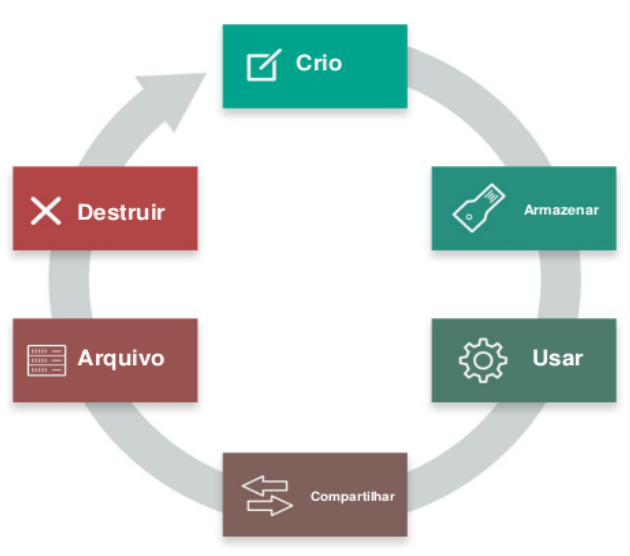
preocupações diferentes sobre cada detalhe dentro de uma arquitetura computacional.

Computação em nuvem caminha por vários domínios de uma governança. Atributos em que podemos pontuar:

- Classificação da Informação;
- Política de Gestão da Informação;
- Política de Localização;
- Autorização;
- Propriedade;
- Custódia;
- Privacidade;
- Controles Contratuais;
- Controles de Segurança.

Existe uma situação que é destacada como Ciclo de Vida de Segurança dos Dados em que dá uma visão sobre as várias etapas em que os dados podem ser classificados. Este ciclo é definido em seis fases que são elas:

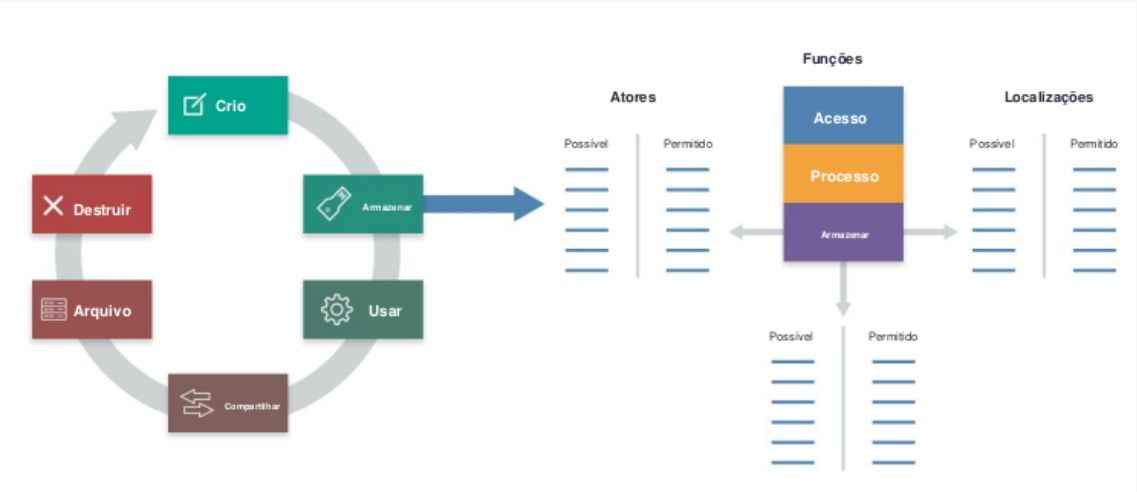
Figura 9 – Ciclo de Vida de Segurança dos Dados.



Fonte: CSA Security Guidance - V4.0.

Cada etapa caracteriza um determinado momento sobre os dados, quando se tem um mapeamento é possível entender a maturidade daquele dado para determinar o seu nível de proteção, gestão e tomar ações para estratégias refinadas e precisas dentro de pontos específicos. Vejamos a próxima figura que pode direcionar uma impressão sobre entender o aspecto do ciclo de vida para poder direcionar a usabilidade dele.

Figura 10 – Mapeamento do ciclo de vida para funções e controles.



Fonte: CSA Security Guidance - V4.0.

A compreensão sobre o desenvolvimento de uma governança direciona qualquer evolução em termos de migrações de arquiteturas. O alinhamento para que todas as políticas e práticas se adequem a cenários de arquiteturas em nuvem e arquiteturas *on premises* podem tornar qualquer movimento mais simplificado e organizado. **Entender sobre os dados facilita na modelagem e organização de níveis estratégicos que podem estar em constantes manuseios e evoluções.**

Proteção de Dados na Cloud

Conforme as empresas migram suas estruturas para nuvem, muitos desafios começam, desde o ponto em que temos que entender sobre a nossa responsabilidade acerca da nossa segurança em determinado

cenário, como também entender que os desafios mudam de estruturas *on premises* (locais) para arquiteturas de computação em nuvem. A dinâmica e funcionamento dessas arquiteturas acabam sendo um tanto que distintas e isso acaba se tornando um desafio para determinados contextos.

A diversidade de serviços que são executados na nuvem aumenta a cada dia, a variedade de ferramentas e serviços inseridos para que tudo isso aconteça é cada vez mais alto. Juntamente com todas essas opções, os desafios de garantir que tudo execute de modo mais simplificado, garantindo todos os pilares de segurança, torna todo esse cenário, no mínimo, desafiador.

Como fazer com que um ambiente execute sobre um modelo de segurança eficaz? Iniciando por pontos como:

- Aplicar uma boa gestão de senhas;
- Monitorar a infraestrutura de modo preciso;
- Aplicar cenários de *backups*;
- Adotar cenários de *recovery* para validação destes *backups*;
- Estressar pontos/aplicações com testes de penetração;
- Aplicar *patches* de atualizações.

Dessa maneira precisamos entender quais cuidados devem ser explorados para evitar problemas graves. A segurança dos dados em nuvem merece atenção, planejamento e investimento para rondar de vários modos a complexidade e garantia de barreiras adequadas.

Dois dos principais tipos de proteção de dados podem ser definidos como controle de acesso e monitoramento de recursos. Uma vez que um

atua em fazer a gestão de acesso ao conteúdo e outro opera na ação de identificar e bloquear ameaças ou vulnerabilidades.

> Capítulo 9

Capítulo 9.

Melhores Práticas de Segurança em Cloud

Melhores Práticas de Segurança em Cloud

Os melhores *frameworks* hoje no mercado que abordam sobre as melhores práticas são: SOC2, ISSO/IEC27001, NIST PCI DSS, SP800-53 e FedRAMP. Muitos *players* (empresas) do mercado acabam seguindo esses *frameworks* para elevar suas políticas e a confiabilidade dos seus serviços ao cliente final.

Para avançar e direcionar os esforços em pontos estratégicos, definimos quatro pilares que devem ser visualizados e focados:

- Visibilidade e Conformidade;
- Segurança baseada em computação;
- Proteção de Rede;
- Segurança de Identidade.

Práticas de Segurança em PaaS

Este formato de serviço está cada dia mais crescendo seu uso pelas companhias. Provedores como AWS e AZURE descrevem algumas situações que podem ser observadas para garantir uma base de segurança.

- Identidade como perímetro de segurança primária:
  - Proteger as chaves e as credenciais para proteger a implantação de PaaS.
  - Em hipótese nenhuma armazenar as credenciais e outros segredos no código-fonte nem fontes públicas, fóruns e outros. Exemplo: GitHub.

- Uso de MFA (autenticação de múltiplos fatores).
- Utilizar protocolos de segurança padrão OAuth2 e Kerberos.

- Adotar proteção de camada 7 - Como um *Firewall* WAF.
- Aplicar a restrição de acesso com referência no IP.
- Criptografar os dados em repouso e em trânsito:
  - Habilitação do *Always Encrypted*.
- Realizar *backups*.

Práticas de Segurança em IaaS

Para este formato, infraestrutura como serviço, provedores como AWS e AZURE descrevem algumas situações que podem ser observadas para garantir uma base de segurança.

- Proteção sobre as VMS:
  - Definir políticas para VMs em grupos de recursos.
  - Reduzir a variabilidade na configuração de VMs com *templates*.
  - Abordagem de privilégios mínimos.
  - Usar mais de uma VM para melhorar a disponibilidade.
  - Proteção contra *Malware*.
  - Gerenciar atualizações de VM.
  - Realização de *backups*.

- Monitoramento de segurança e desempenho.
- Criptografar discos.
- Restringir conexão direta com a Internet.

Os cuidados que são importantes usando Cloud e a LGPD

A Lei Geral de Proteção de Dados (LGPD), de número 13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais no Brasil. A LGPD se aplica a empresas que têm estabelecimento no Brasil, e/ou oferecem produtos e serviços ao mercado brasileiro e/ou coletam e tratam dados de pessoas que estejam no país. A lei prevê os deveres das empresas em casos de incidentes de segurança ou violação de dados pessoais, como roubo de um dispositivo de armazenamento, invasão ao sistema, perda do controle sobre a base, vazamento de informações, *ransomware*, entre outros.

É muito importante o conhecimento sobre leis que são práticas nos países em que há esse tipo de preocupação e regulamentação, uma vez que arquitetamos sistemas em nuvem o nível de envolvimento e projeção podem ser atributos que será preciso levar em consideração.

A LGPD, por se tratar de uma lei brasileira, pontua algumas situações sobre onde os dados pessoais estão sendo armazenados. Isso não quer dizer sobre a proibição da elaboração de arquiteturas ou armazenamento em solo internacional, mas sim da compreensão, estratégia e esclarecimentos destes dados armazenados aos titulares dos dados.

A LGPD segue a base da GDPR (Regulamento Geral sobre a Proteção de Dados) pertencente a União Europeia. Ou seja, quando se desenvolve leis para tornar as empresas responsáveis por ações e cuidado com o que hoje é mais valioso (dados) o nível estratégico em que uma

corporação e ou uma nação demonstra, direciona significativamente para uma maturidade estratégica de vários aspectos.

A LGPD ainda é um grande desafio para várias empresas ao nível nacional, uma vez que existem muitos pontos ainda confusos, situações que geram incertezas e dúvidas, mas é preciso olhar para a mesma e esboçar ou iniciar essa adequação de um modo que eleve o nível estratégico do negócio, cuidados e situações bem desenhadas para garantir que tanto os processos quanto às preocupações sejam prioridades em projetos de arquiteturas computacionais.

Dessa forma, dado momento em que um projeto for desenvolvido, olhar para determinadas políticas é fundamental para direcionar seus esforços em observar, melhorar e tratar políticas, regras, normas, como também contextos de fluxos baseados na coleta, armazenamento, tratamento e descarte de camadas de dados ou informações. Lembre-se, falta de planejamento sobre uma arquitetura de nuvem pode comprometer sistemas, dados e informações. Quando isso acontece, um esforço grande deve ser colocado em prática para reverter, porém, a imagem de uma empresa pode ficar manchada e isso pode resultar em situações bem complexas. Então, planeje, execute, organize, revise e mantenha sua estrutura em constante evolução.

Referências

ALIBABA Cloud. c2009-2022. Disponível em: https://us.alibabacloud.com/. Acesso em: 31 ago. 2022.

AWS Security Best Practices. **AWS**, c2022. Disponível em: https://docs.aws.amazon.com/pt_br/whitepapers/latest/aws-security-best-practices/welcome.html. Acesso em: 31 ago. 2022.

AWS. c2022. Disponível em: https://aws.amazon.com/pt/. Acesso em: 31 ago. 2022.

AZURE. **Microsoft**, c2022. Disponível em: https://azure.microsoft.com/. Acesso em: 31 ago. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 31 ago. 2022.

CLOUD Security Alliance. c2009-2022. Disponível em: https://cloudsecurityalliance.org/education/ccsk/. Acesso em: 31 ago. 2022.

DA ROSA RIGHI, Rodrigo; GALANTE-GUILHERME, Guilherme. Explorando a Elasticidade em Nuvem para a Computação de Aplicações Paralelas. **ResearchGate**, abr. 2016. Disponível em: https://www.researchgate.net/profile/Guilherme-Galante/publication/311589613_Explorando_a_Elasticidade_em_Nuvem_para_a_Computacao_de_Aplicacoes_Paralelas/links/584fe49208aecb6bd8d1de8b/Explorando-a-Elasticidade-em-Nuvem-para-a-Computacao-de-Aplicacoes-Paralelas.pdf. Acesso em: 31 ago. 2022.

DE ALBUQUERQUE, Matheus Carvalho; FREITAS, Marcio. Computação em Nuvem. In: **5º Seminário de Tecnologia Gestão e Educação**, v. 3, n. 1, 2021. Disponível em: http://raam.alcidesmaya.edu.br/index.php/SGTE/article/download/327/319. Acesso em: 31 ago. 2022

GARTNER. c2022. Disponível em: https://www.gartner.com/en. Acesso em: 31 ago. 2022.

GOOGLE Cloud. Disponível em: https://cloud.google.com/?hl=pt-br. Acesso em: 31 ago. 2022.

IBM Cloud. Disponível em: https://www.ibm.com/br-pt/. Acesso em: 31 ago. 2022.

MICROSOFT. **Microsoft Docs**, c2022. Disponível em: https://docs.microsoft.com/en-us. Acesso em: 31 ago. 2022.

YELURI, Raghuram; CASTRO-LEON, Enrique. **Building the Infrastructure for Cloud Security**: A Solutions View. Springer Nature, 2014. Disponível em: https://library.oapen.org/bitstream/handle/20.500.12657/28174/1001820.pdf?sequence=1. Acesso em: 31 ago. 2022.