COMPUTAÇÃO EM NUVEM

AULA 1

Prof.ª Ana Paula Costacurta

CONVERSA INICIAL

Na primeira parte, falaremos sobre os conceitos e aspectos gerais da computação em nuvem apresentando definições importantes, características essenciais e benefícios na utilização da computação em nuvem.

Na segunda parte, conheceremos os três modelos de serviços da computação em nuvem: *software* como serviço (SaaS), plataforma como serviço (PaaS) e infraestrutura como serviço (IaaS). Falaremos sobre as responsabilidades dos atores em cada um dos modelos de serviços da computação em nuvem, incluindo as responsabilidades de gerenciamento e segurança de cada modelo de serviços da computação em nuvem.

Na terceira parte, serão apresentados os quatro modelos de implantação da computação em nuvem: nuvem privada, nuvem pública, nuvem comunitária e nuvem híbrida. Verificaremos também quais são os benefícios de cada modelo de Implantação.

Na quarta parte, falaremos sobre a definição da nuvem com base da arquitetura de referência NIST, e conheceremos em detalhes a forma de interação dos atores: consumidor e provedor da nuvem, agente da nuvem e auditor da nuvem. Também faremos uma breve passagem pelo modelo de segurança da CSA.

Na quinta parte, estudaremos sobre os componentes da arquitetura de referência NIST, detalhando as estruturas das perspectivas de orquestração, gerenciamento, segurança e privacidade de serviços. Também verificaremos as áreas de foco crítico e problemas de segurança da informação na computação em nuvem.

TEMA 1 – CONCEITOS E ASPECTOS GERAIS

Antes de iniciarmos, precisamos conhecer sobre as principais definições e as características essenciais para implantação da computação em nuvem.

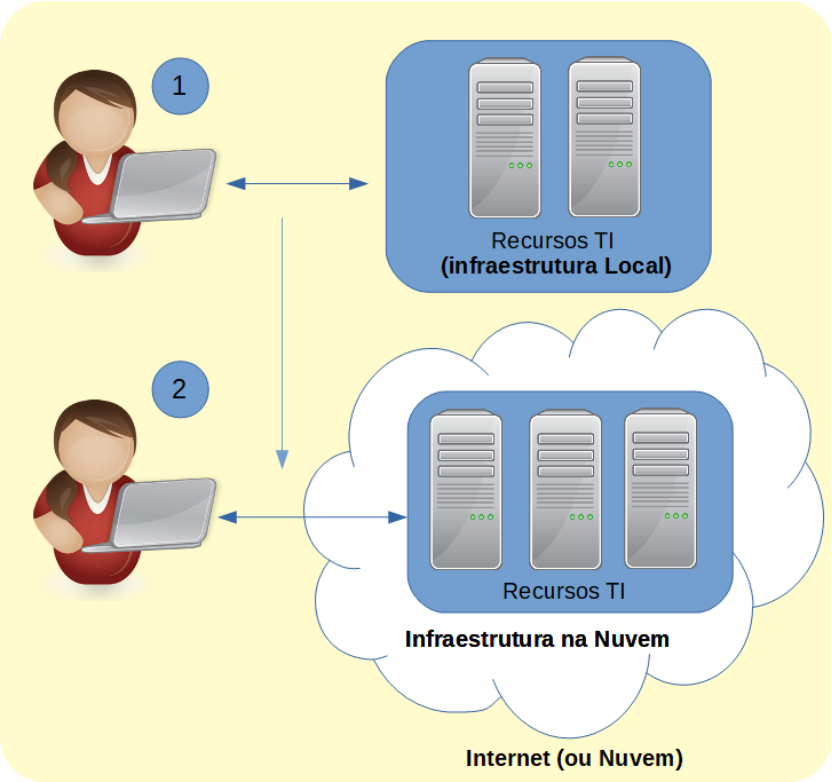
1.1 Definição

A computação em nuvem (c*loud computing*) está associada ao modelo de realizar as entregas usando TI como serviços (ITaaS). Os serviços entregues podem incluir servidores, armazenamento, bancos de dados, rede, *software*, análise e inteligência, e o meio utilizado para entrega é a internet (nuvem ou

cloud). O objetivo principal de disponibilizar TI como serviços na nuvem é a otimização de recurso sem perder a flexibilidade (Veras, 2015).

Podemos encontrar várias definições sobre computação em nuvem, mas consideraremos aqui uma definição simples que podemos encontrar: “um conjunto de recursos como capacidade de processamento, armazenamento, conectividade, plataformas, aplicações e serviços disponibilizados na internet” (Taurion, 2009, p. 2).

Figura 1 – Recursos de TI



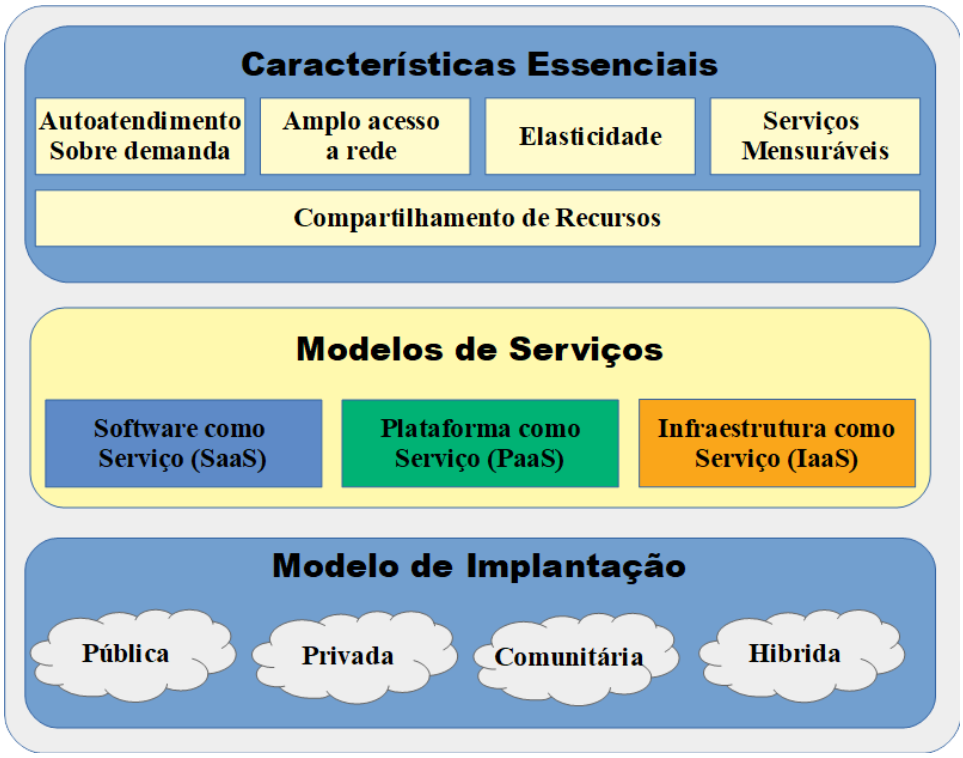
A Figura 1 ilustra duas situações de utilização dos recursos de TI:

1. Os acessos aos recursos de TI são realizados por meio de uma infraestrutura local;
2. Os recursos de TI foram transferidos para nuvem e são disponibilizados e acessados via Internet.

A ITaaS é a forma de implantar, gerenciar e manter a infraestrutura das corporações utilizando recursos de TI de parceiros ou terceiros (O*utsourcing*). Essa maneira de disponibilização dos serviços de IT beneficia a organização e torna possível simplificar, agilizar, reduzir custos de consumo e aumentar a eficiência da área de TI da corporação.

Podemos aplicar a computação em nuvem, desde serviço de armazenamento de documentos até a terceirização de toda a infraestrutura onde ficam armazenadas as aplicações e o banco de dados. Quando a organização utiliza a computação em nuvem, terceirizar algumas preocupações: com segurança, manutenção e atualização de *hardware*. A organização ganha maior flexibilidade, pois pode realizar um aumento de sua capacidade de processamento e armazenamento conforme seu crescimento, ou seja, sob demanda.

Figura 2 – Modelo de referência NIST



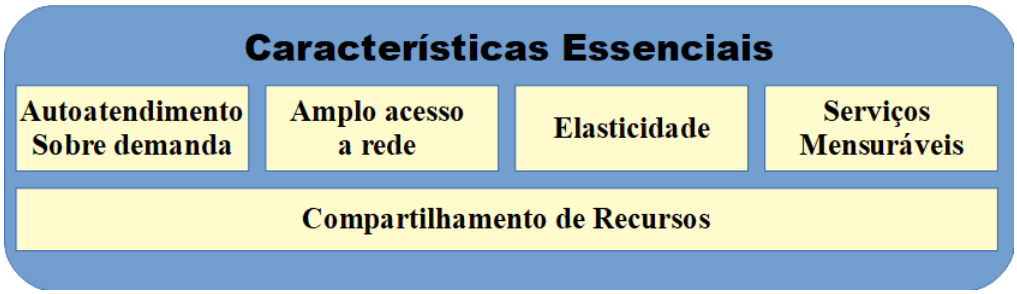
Fonte: NIST, 2011.

O NIST *(National Institute of Standards and Tecnology),* órgão do Departamento de Comércio americano, define a representação da estrutura da computação em nuvem e podemos ver representado na Figura 2.

Esse conceito proposto pelo NIST define as características essenciais, os modelos de serviços e os modelos de implantação. Esse conceito atualmente é o mais aceito para computação em nuvem. Agora iremos ver em detalhes cada componente do conceito.

1.2 Características essenciais

Figura 3 – Características essenciais dos serviços em nuvem



Fonte: NIST, 2011a.

De acordo com o NIST (2011a), são cinco as características que são consideradas essenciais para a disponibilização do serviço de IT em nuvem, conforme é apresentado na Figura 3.

A seguir, veremos em detalhes cada uma das características essenciais:

1. Autoatendimento sob demanda *(on-demand self-service)*: as funcionalidades são disponibilizadas por meio de autoatendimento sob demanda, possibilitando assim acesso fácil e rápido os recursos conforme a necessidade;
2. Amplo acesso a serviços de rede (*broad network access*): a disponibilização dos recursos em rede com padronização dos mecanismos, podendo ser utilizados por uma variedade de dispositivo, ou seja, acesso heterogêneo;
3. Compartilhamento de recursos (*resource pooling*): alocação e liberação dos recursos computacionais, físicos ou virtuais, conforme necessidade demanda dos consumidores dos serviços. Os recursos são agrupados com a finalidade de atender vários usuários. Os recursos são os seguintes: armazenamento, processamento, memória e largura de banda da rede;
4. Elasticidade (*elasticity*): o provisionamento e liberação dos recursos, em alguns casos feitos automaticamente, possibilita a rápida expansão na quantidade de recursos que realmente necessária de acordo com o crescimento da organização. O usuário fica com a sensação de recurso ilimitado, passando uma ideia de que pode ser utilizado qualquer quantidade em qualquer momento;

5. Serviços mensuráveis (*measured features*): a otimização e o controle automático do uso dos recursos, com capacidade de medição do serviço. Como exemplo de serviço, podemos citar: armazenamento, processamento, largura da banda e contas ativas. Monitoramento, controle e relatórios fornecem transparência da utilização dos recursos para o consumidor e fornecedor do serviço.

1.3 Benefícios da utilização da computação em nuvem

Na Tabela 1, podemos ver as três economias de escalas, forma de economia e motivos da economia.

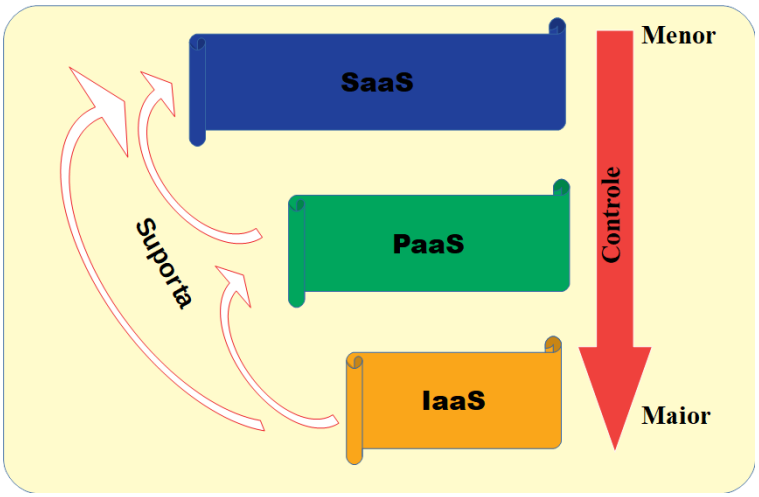
Tabela 1 – Benefícios computação em nuvem

Economia de escala	**Forma de economia**	**Motivo**
Fornecimento	Grandes centros de dados	Redução do custo de energia; Redução do custo de pessoal; Segurança e confiabilidade; Aumento do poder de compra.
Demanda	Agregação de demanda	Redução da variabilidade; Padrões de uso; Variabilidade da indústria; Incerteza crescimento do uso; Variabilidade multirrecurso.
Arquitetura multilocatário (*Multitenancy*)	Número de inquilinos por aplicativo.	Custo do aplicativo amortizado; Custo de utilização servidor amortizado.

TEMA 2 – MODELOS DE SERVIÇOS

Os três modelos de serviços principais para computação em nuvem definidos pelo NIST (2011a) são *Software as a Service* (SaaS), *Plataform as a Service* (PaaS) e *Infrastructure as a Service* (IaaS).

Figura 4 – Modelos de serviços



2.1 *Software* como serviço (SaaS)

Nesse modelo, os serviços oferecidos são os aplicativos e podem ser acessados pelos clientes pelos navegadores na internet. Os aplicativos de interesse de vários clientes podem ser disponibilizados na nuvem como uma opção alternativa para o processamento local. O provedor do serviço tem a responsabilidade de controle e gerenciamento da rede, do sistema operacional, dos servidores e da gestão do armazenamento.

Podemos citar como exemplo desse modelo de serviço: Google Apps (Drive) e SalesForce.com (CRM).

2.2 Plataforma como serviço (PaaS)

Nesse modelo, os serviços oferecidos são a capacidade para o desenvolvimento de aplicativos que estão disponibilizados e serão executados na nuvem. O serviço de plataforma na nuvem disponibiliza o modelo de computação, armazenamento e comunicação entre aplicativos. É importante mencionar também que o modelo PaaS suporta o modelo SaaS, ou seja, fornece

também os recursos, as tecnologias e as ferramentas para desenvolvimento e execução dos serviços que são disponibilizados no SaaS.

Podemos citar como exemplo desse modelo de serviço: AppEngine (Google), EC2 (Amazon) e Azure (Microsoft).

2.3 Infraestrutura como serviço (IaaS)

Esse modelo de serviço oferecido é a abstração da infraestrutura, ou seja, o provedor oferece a infraestrutura de processamento e armazenamento totalmente transparente para o cliente. O provedor detém a responsabilidade completa da gestão da infraestrutura física, e o usuário possui controle sobre as máquinas virtuais, porém com controle limitado. É importante mencionar ainda que o modelo IaaS suporta PaaS, ou seja, fornece todos os recursos computacionais (*hardware* e *software*) para PaaS.

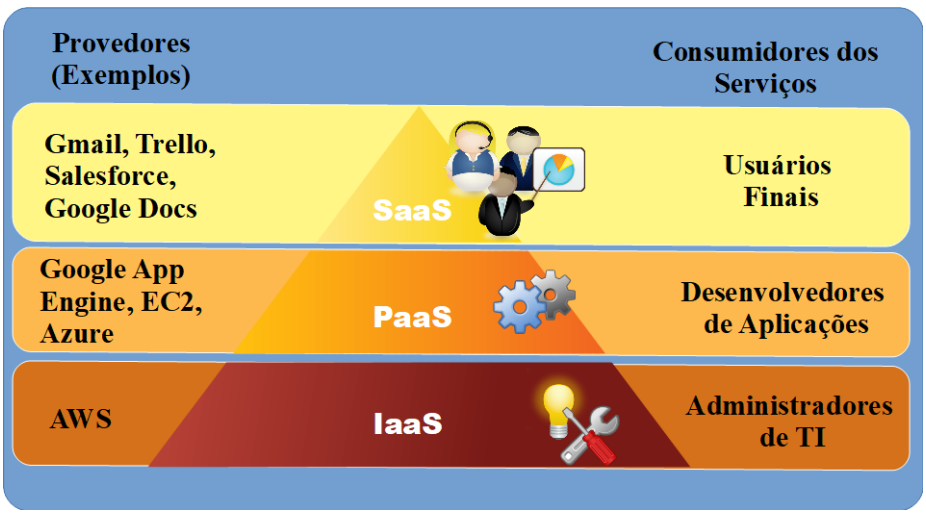
Podemos citar como exemplo desse modelo de serviço: Amazon Web Services (AWS).

2.4 Atores nos modelos de serviços

De acordo com os papéis na utilização da arquitetura em nuvem, os serviços são fornecidos por um provedor e quem consome o serviço pode assumir vários papéis simultaneamente segundo os interesses.

Os provedores de serviços (SPs ou *service providers)* têm o papel de desenvolver e disponibilizar os serviços para os usuários por meio das interfaces da nuvem.

Figura 5 – Atores de modelos de serviços



Na Figura 5, apresentamos um resumo dos modelos de serviços e seus consumidores e provedores.

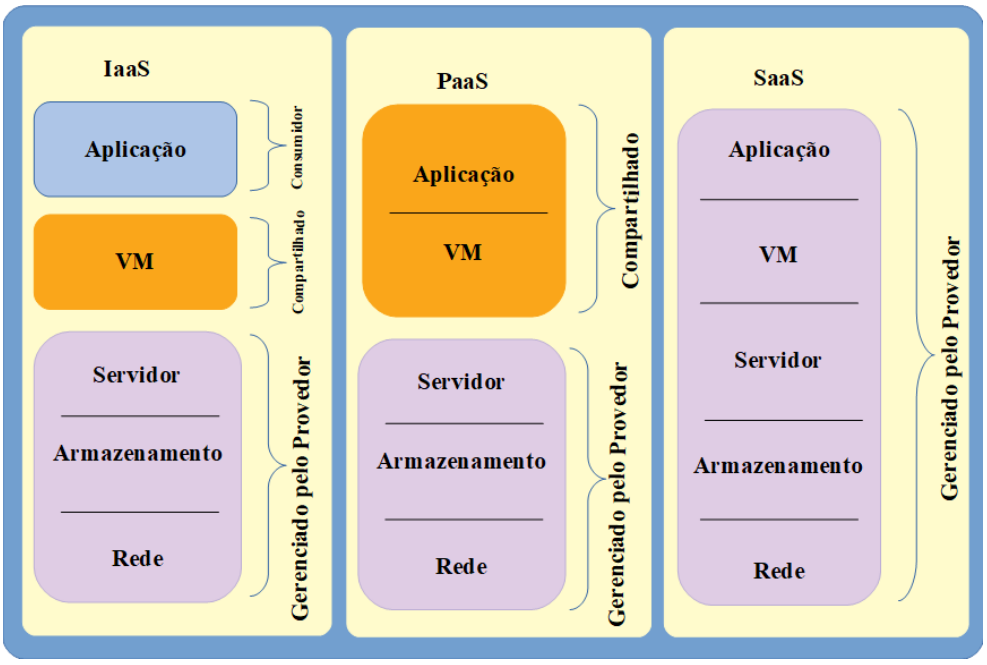
2.5 Gerenciamento e segurança dos modelos de serviços

Em cada modelo, as responsabilidades são diferentes:

1. No modelo SaaS, a responsabilidade do gerenciamento total e segurança é do provedor do serviço;
2. No modelo PaaS, o cliente é responsável pelo gerenciamento das aplicações e a gestão da segurança é feita pelo provedor;
3. No modelo IaaS, o provedor é responsável pela infraestrutura e o cliente é responsável pelo gerenciamento das aplicações, banco de dados e segurança.

Na Figura 6, podemos visualizar graficamente as responsabilidades.

Figura 6 – Responsabilidades modelos de serviço

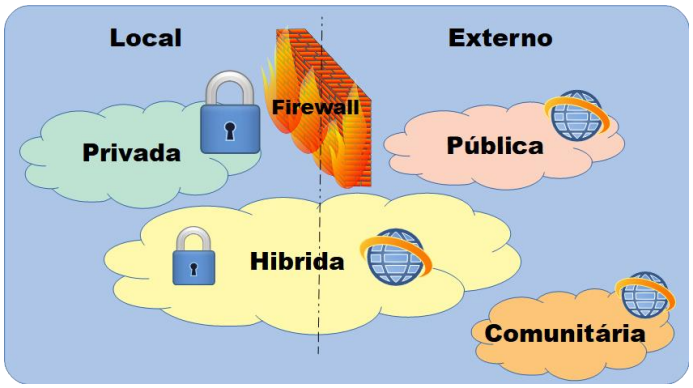


TEMA 3 – MODELO DE IMPLANTAÇÃO

Baseado no modelo NIST (2011b), os modelos de implantação são quatro: nuvem privada, nuvem pública, nuvem comunitária e nuvem híbrida. A

Figura 7 apresenta os 4 modelos e, na sequência, estudaremos em detalhes cada um dos modelos.

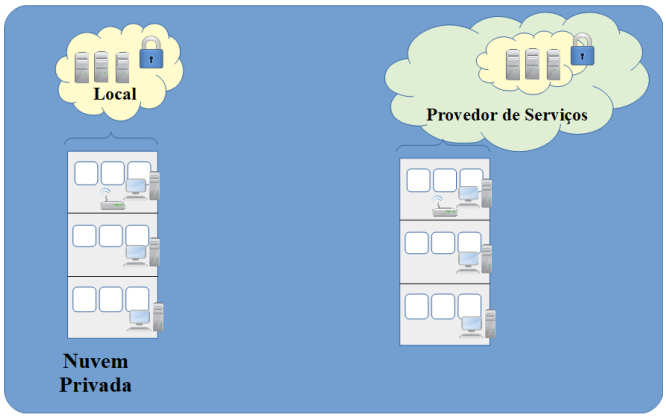
Figura 7 – Modelos de Implantação



3.1 Nuvem privada (*private cloud*)

Esse modelo de implantação pode ser gerenciado pelo cliente ou por terceiros, cujos serviços são oferecidos para utilização própria da organização. A infraestrutura não é compartilhada com outros usuários. Essa definição de privacidade não está relacionada com a propriedade e a localização. Existem dois tipos básicos de nuvem privada: *hospedada na empresa* (local) ou *hospedada em provedor* (virtual). A Figura 8 ilustra os dois tipos de nuvem privada.

Figura 8 – Nuvem privada

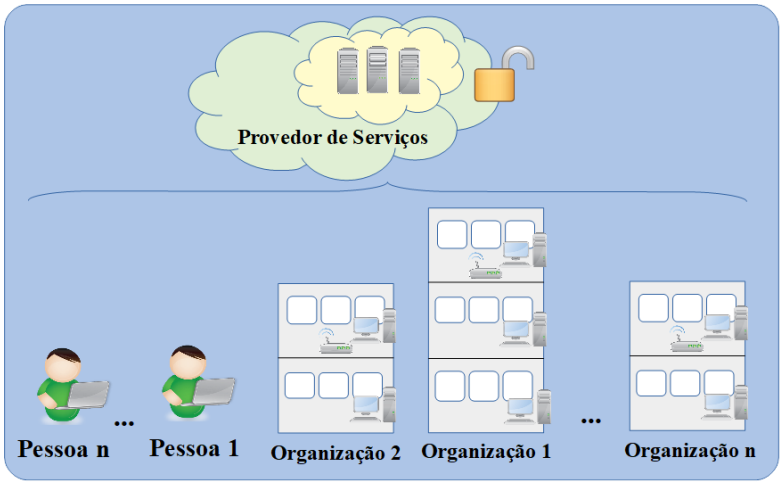


3.2 Nuvem pública (*public cloud*)

Nesse modelo de implantações, várias empresas compartilham máquinas físicas que são oferecidas por um provedor que tem capacidade de

processamento e podem ser oferecidas por organizações públicas ou grande grupos industriais. O serviço é entregue por meio de uma rede aberta e de utilização pública.

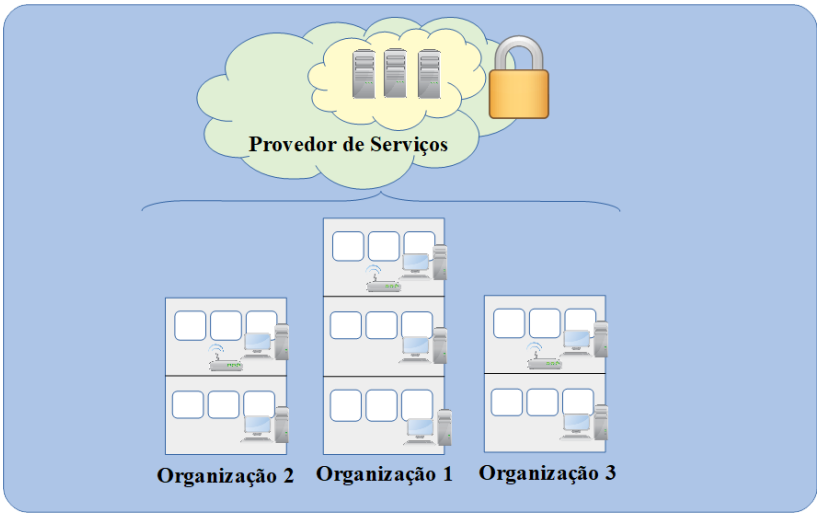
Figura 9 – Nuvem pública



3.3 Nuvem comunitária (*community cloud*)

Esse modelo de implantação é compartilhado por várias organizações, que possui interesses próprios e contratam uma única infraestrutura privada para uso comunitário. É semelhante ao funcionamento da nuvem pública, porém com um número limitado de organização. A localização e o gerenciamento podem ser realizados pelas organizações envolvidas ou por terceirizado.

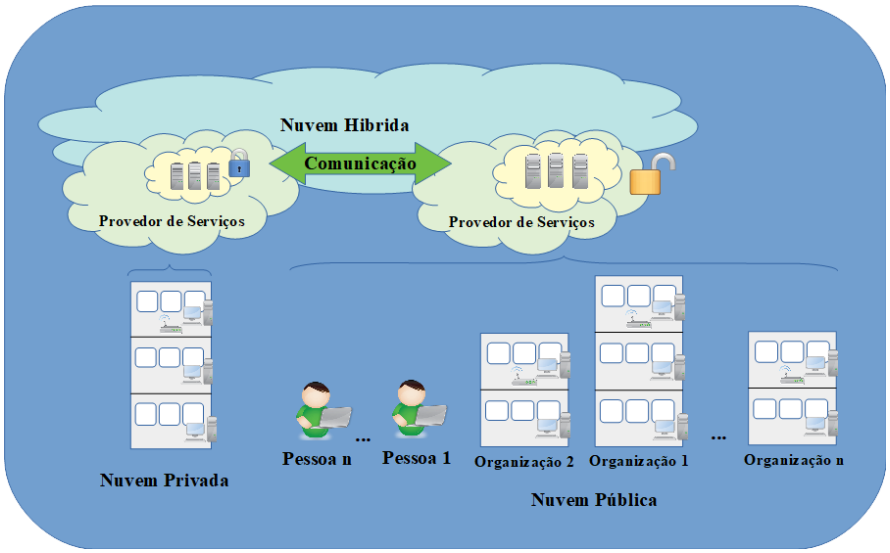
Figura 10 – Nuvem comunitária



3.4 Nuvem híbrida (*hydrid cloud*)

Esse modelo de implantação é uma combinação de dois ou mais modelos (privada, pública, comunitária) que são conectadas por tecnologias próprias ou padronizadas, que possibilitam a portabilidade de dados e aplicação.

Figura 11 – Nuvem híbrida



3.5 Vantagens e algumas desvantagens dos modelos de implantação

Cada modelo de implantação possui uma vantagem para ser implantada, veremos algumas a seguir.

1. Nuvens privadas e nuvens pública: possuem alta eficiência e disponibilidade, elasticidade e de rápida implantação;
2. Nuvem pública: apresenta baixos custos, economia de escala, gerenciamento simples e pagamento como despesas operacionais, porém tem um maior risco com a privacidade dos dados;
3. Nuvem privada: são de fácil integração, possuem mais baixos custos totais, um maior controle em segurança, conformidade e qualidade de serviço e pagamento como despesas de capital e despesas operacionais.

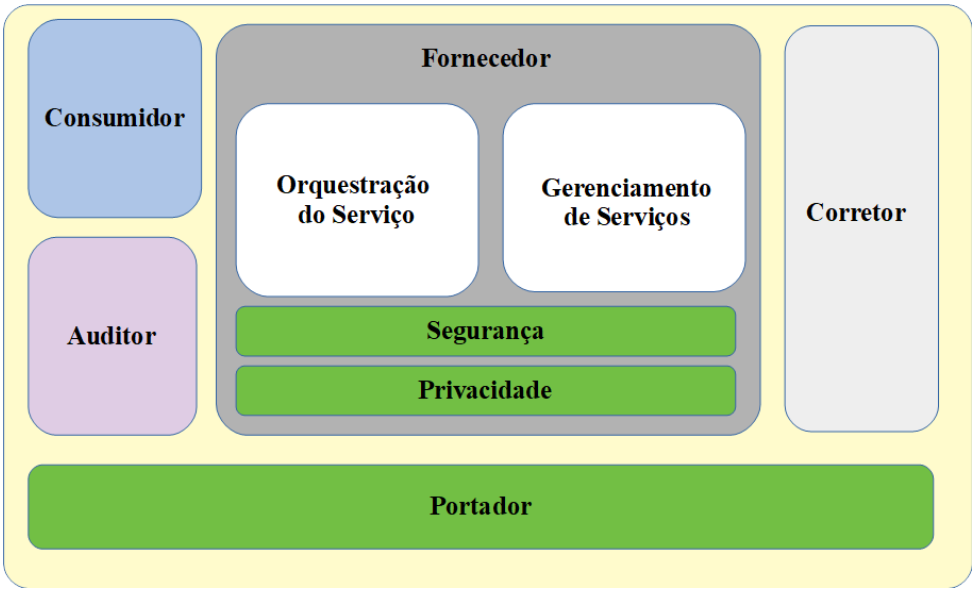
TEMA 4 – ARQUITETURA

Estudaremos a arquitetura de referência do NIST (2011a), os componentes da arquitetura e o modelo de segurança da CSA.

4.1 Arquitetura de referência NIST

O NIST (2011a) desenvolveu um modelo de referência (Figura 12), que atualmente é o modelo conceitual mais aceito. Esse modelo é uma ferramenta para discussão dos requisitos, definição das estruturas de arquitetura e análise do funcionamento das soluções que são baseadas na computação em nuvem. O modelo de referência NIST descreve os atores envolvidos, as atividades, as responsabilidades e as funções. Na Figura 12, podemos ver a representação gráfica do modelo do NIST, e este será o modelo utilizado para nossos estudos.

Figura 12 – Modelo de referência



Fonte: NIST, 2011a.

O modelo do NIST descreve 5 atores principais, sendo eles:

1. Provedor (*cloud provider*) é o fornecedor dos serviços;
2. Consumidor (*cloud consumer*) é o indivíduo ou organização que contrata ou utiliza os produtos e serviços;
3. Agente (*cloud broker*) é o intermediário entre os consumidores e fornecedores e auxilia os consumidores com as ofertas de serviços e também podem criar serviços;
4. Auditor (*cloud auditor*) é o responsável por monitoramento do desempenho e segurança e realiza auditorias independentes;
5. Operador (*cloud carrier*) é responsável por assegurar o canal de comunicação entre os consumidores e fornecedores, ou seja, operam a

infraestrutura de comunicações normalmente fornecidas por operadoras de telecomunicação.

4.2. Consumidor e provedor da nuvem

Na Tabela 2, temos exemplos de alguns cenários de utilização dependendo do serviço solicitado e podemos perceber que as atividades e os cenários podem ser diferentes entre os consumidores.

Tabela 2 – Cenários de uso dos modelos de serviços

Modelo de serviço	**Atividades do consumidor**	**Atividades do provedor**
SaaS	Usuário final utiliza o aplicativo	Instalação, gerencia, mantém o aplicativo na nuvem.
PaaS	Desenvolvedor de aplicativos realiza a criação, testa, faz a implementação e gerenciamento dos aplicativos hospedados na nuvem.	Ferramentas de desenvolvimento, implantação e administração da plataforma de desenvolvimento.
IaaS	Criação, instalação, gestão e monitoramento da infraestrutura da nuvem.	Ambiente de hospedagem, processamento físico, armazenamento e rede da infraestrutura da nuvem.

Podemos dividir as atividades dos provedores em 4 perspectivas: orquestração de serviços, gerenciamento de serviços, segurança e privacidade. Veremos em detalhes cada uma destas 4 perspectivas no capítulo 5.

4.3 Agente de nuvem

A integração de serviços pode ser complexa para a gestão pelos consumidores, assim o agente é acionado pelo consumidor para entrar em contado com o provedor da nuvem. O agente se torna um ponto único para

entrada de vários serviços da nuvem. A principal diferença do agente é a forma única de oferecer a interface para vários provedores. Normalmente o agente possui três categorias de serviços:

- Intermediário (*service intermediation*): aprimoramento de um serviço, com o melhoramento de um recurso;
- Agregação (*service aggregation*): combinação e integração de vários serviços em um novo serviço;
- Arbitragem (*service arbitrage*): flexibilidade da agregação em que pode escolher serviços de vários de provedores.

4.4. Auditor de nuvem

As auditorias são realizadas pelos auditores da nuvem, com o objetivo de verificar a conformidade com os padrões, podendo ser avaliados os serviços que são oferecidos por provedores em termos de segurança, privacidade e desempenho.

4.5 Modelo de segurança CSA

A Cloud Security Allice (CSA) desenvolveu um guia de segurança que define padrões de segurança em nuvem. Esse guia é um conjunto de melhores práticas de segurança que envolve 14 domínios. Neste momento, analisaremos o domínio arquitetura e no capítulo 5 vamos ver sobre os demais domínios. O Guia da CSA, que está na terceira edição, estabelece uma base estável e segura para operações em nuvem.

O CSA identificou o multilocatário (multi-inquilino ou *multitenancy*) como um elemento importante da nuvem, apesar de não ser essencial. Multilocatário consiste na utilização de um mesmo recurso ou aplicação por vários consumidores pertencentes a uma mesma organização ou a várias organizações.

Quanto mais embaixo da pilha o serviço, mais o controle de segurança fica sob responsabilidade do consumidor.

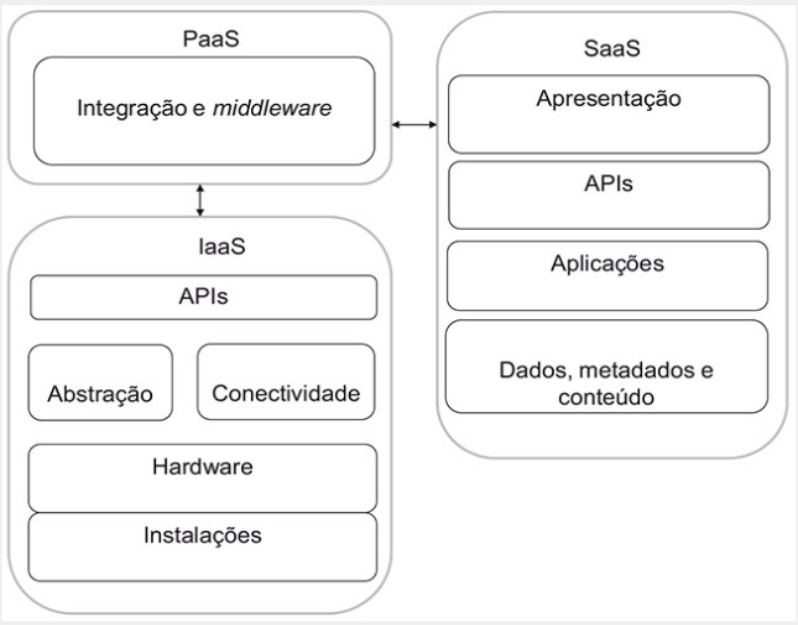
Na Tabela 3, poderemos ver o funcionamento do modelo de segurança.

Tabela 3 – Modelo de segurança dos modelos de serviços

Modelo	**Construção**	**Recursos e serviços**
IaaS	Fundamento	Recursos de pilha, conectividade física e lógica dos recursos, conjunto de APIs para integração e gestão de infraestrutura
Paas	Base na IaaS	Camada adicional de integração sobre IaaS, *framework* de desenvolvimento de aplicativos, recursos de *middleware* (funções de banco de dados, mensagens e filas)
SaaS	Base nas PaaS	Ambiente autocontido, entrega dos recursos do usuário (conteúdo, apresentação, aplicações e gestão)

Na Figura 13, apresentamos as relações e dependências dos modelos de serviços.

Figura 13 – Dependências entre modelos de serviços



Fonte: Veras, 2015.

TEMA 5 – COMPONENTES DA ARQUITETURA

Agora vamos ver em detalhes os seguintes componentes: orquestração de serviço, gestão de serviço, segurança e privacidade

5.1 Orquestração de serviços

Esse componente se refere a organizar, coordenar e gerenciar a infraestrutura para fornecimento de recursos. O modelo NIST utiliza estrutura de três camadas, sendo eles:

1. Camada de serviço (*service layer*) que define e provisiona cada uma dos tre modelos de serviços;
2. Camada intermediária (*resoucer abstraction and control layer*) contém os componentes do sistema que o provedor utiliza, normalmente contém *software*, *hypervisors*, máquinas virtuais, armazenamento de dados e outros componentes de abstração e gerenciamento;
3. Camada recursos físicos (*physical resource layer*) contém todos os recursos de computação físicos, incluindo *hardware* (CPU, memória), redes (roteadores, *firewall*, *switches*, *links* e interfaces), armazenamento (HD's) e outros elementos de infraestrutura física.

5.2 Gerenciamento de serviços

Esse componente se refere à função necessária para gerenciamento e operação dos serviços na nuvem. O modelo NIST utiliza as perspectivas: suporte, provisionamento e configuração e requisitos de portabilidade e interoperabilidade.

1. Suporte a negócios (*bussiness dupport management*) – endereçam questões referentes à gestão dos contratos, contabilidade e preços;
2. Fornecimento e configuração (*provision and configuration*) – requisitos referentes à instalação, à operação e à manutenção dos serviços, inclusive a medição do serviço e SLAs;
3. Questões de portabilidade e interoperabilidade dos dados, sistemas e serviços.

5.3 Segurança e privacidade

Vamos ver agora as áreas críticas, problemas de segurança da computação em nuvem. As áreas críticas são divididas em dois domínios:

- Domínio de governança: questões estratégicas e políticas, assuntos ligados a governança e gestão de riscos corporativos;

- Domínio operacional: questões de segurança e implantação desta, assuntos ligados segurança, continuidade e recuperação de incidentes.

5.4 Áreas de foco crítico na computação em nuvem

Os controles de segurança da computação em nuvem são implantados em função do risco e podem ser implantados em uma ou mais camadas, que vão desde segurança física, de rede, de sistemas e de aplicações.

De acordo com o modelo de serviço, os controles de segurança e responsabilidades são exercidos por um determinado ator, como pode ser visto na Figura 6 no item 2.5.

Nesta aula, veremos rapidamente os domínios operacionais e por que se concentram em questões de segurança táticas e implantação dentro da arquitetura.

Na Tabela 4, poderemos conhecer o conteúdo tratado em cada uns dos domínios da segurança operacional.

Tabela 4 – Conteúdo tratado nos domínios operacionais

Domínio	Conteúdo
Segurança tradicional, continuidade de negócios e recuperação de desastres	Discussão e análise dos possíveis riscos para aumentar o conhecimento sobre os modelos de gestão de risco. Com foco em diminuir riscos para crescimentos em outras áreas.
Operações de Centro de Dados	Avaliação da arquitetura e operações dos provedores, para ajudar a identificar as características comuns que podem prejudicar os serviços em operação, e levantar os pontos fundamentais para criar estabilidade contínua.

Resposta aos incidentes, notificação e correção	Forma correta e adequada de detectar, responder, notificar e corrigir os incidentes, com o objetivo de ajudar a compreensão das complexidades que o modelo computação em nuvem traz no tratamento de incidentes.
Segurança de aplicações	Proteger a execução ou desenvolvimento das aplicações, incluindo também migração ou criação da aplicação para ser executada em nuvem verificando qual o tipo de plataforma mais adequada (SaaS, PaaS ou IaaS)
Criptografia e gerenciamento de chaves	Identificação do uso da criptografia e da gestão de chaves; é mais informativa para entender a necessidade e identificar os problemas e proteger acesso a recursos e dados.
Gerenciamento de identidade e acesso	Avaliação de quanto a organização tem a capacidade de realizar baseado em nuvem, a gestão de identidade e os diretos de acesso
Virtualização	Riscos em relação ao multilocatário e máquinas virtuais, o foco é em segurança que envolve sistema e *hardware* quando envolve a virtualização.
Segurança como um serviço (*Security as a Service*)	Delegar a terceiros a responsabilidade de detectar, corrigir e governança da infraestrutura de segurança.

5.5 Problemas de segurança da informação na computação em nuvem

A utilização da computação em nuvem pode gerar novos riscos à organização, por isso é importante conhecê-los.

Na Tabela 5, podemos ver a descrição das principais preocupações levantadas.

Tabela 5 – Preocupações de segurança

Preocupação	Descrição
Disponibilidade da rede	Os serviços de nuvem precisam de alta disponibilidade da rede e banda larga. Se um dos dois pontos do serviço estiver indisponível, afetará os serviços na nuvem.
Viabilidade do provedor	Utilização de tecnologia de interface proprietária. O consumidor fica preso ao provedor ou em situação difícil na migração em caso de fechamento do provedor.
Recuperação de desastres e continuidade do negócio	Necessidade de preparação e criação de planos de recuperação e continuidade do negócio dos provedores que são contratados. Ter a segurança de que o provedor em caso de desastre não afetará os processos e serviços.
Incidentes de Segurança	Notificação e resposta a incidentes de segurança é uma preocupação importante. Conhecimento e suporte dos incidentes para que estes sejam tratados rapidamente.
Transparência	Conhecimento das políticas de segurança dos provedores para verificação se estão adequadas à política de segurança do consumidor.
Perda de controle físico dos dados	Garantia de que os dados estão sendo tratados da forma adequada em relação ao armazenamento, processamento, criação e deleção dos dados.
Aspectos legais e regulatórios	Obtenção de padrões mínimos regulatórios nos seguimentos que o provedor atua.

Fonte: Silva, 2013.

FINALIZANDO

Na primeira parte, estudamos os conceitos e os aspectos gerais da computação em nuvem, em que vimos:

- As definições mais importantes da computação em nuvem e aprendemos a importância de usar a TI como serviços (ItaaS);
- As cinco características essenciais da computação em nuvem: autoatendimento sobre demanda, amplo acesso à rede, elasticidade, serviços mensuráveis e compartilhamento de recursos;

- Os benefícios de economia de escala de fornecimento, de demanda e de arquitetura multilocatário.

Na segunda parte, estudamos os três modelos de serviços:

- *Software* como serviço: aplicativos utilizados pelos usuários finais que gerenciamento e segurança é forma total realizado pelo provedor;
- Plataforma como serviço: ferramentas utilizadas pelos desenvolvedores de aplicativos que o gerenciamento das aplicações é responsabilidade do consumidor e a segurança é com o provedor;
- Infraestrutura como serviço: fornecimento de infraestrutura de processamento e armazenamento utilizado pelos administradores de TI. O consumidor tem a responsabilidade de gerenciamento das aplicações, banco de dados e segurança e o provedor gerencia os recursos físicos;

Na terceira parte, estudamos os quatro modelos de implantação:

- Nuvem privada: utilizada por uma única organização, podendo ser hospedada local ou terceirizada em uma rede fechada;
- Nuvem pública: várias organizações sem limitação e restrição de interesse em uma rede aberta;
- Nuvem comunitária: várias organizações com limitação e restrição de acesso por apenas algumas organizações com mesmo interesse em uma rede fechada;
- Nuvem hibrida: combinação de dois ou mais modelos de outras implantações com tecnologias para comunicação entre elas.

Ainda na terceira parte conhecemos os benefícios em comum aos modelos de nuvem privada e nuvem publica, sendo alta eficiência e disponibilidade, elasticidade e rápida implantação. E também conhecemos benefícios específicos de cada um dos modelos:

- Nuvem privada: baixo custo, economia em escala, fácil gerenciamento e despesas operacionais, porém com um maior risco de privacidade dos dados;
- Nuvem pública: integração fácil, baixo custo total, controle de segurança, conformidade e qualidade do serviço e despesas de capital e operacional.

Na quarta parte, estudamos sobre a arquitetura de referência NIST, que é o modelo mais aceito atualmente. Conhecemos os atores principais e os

cenários de utilização, dependendo do serviço. Conhecemos também o modelo de segurança CSA com o elemento multilocatário. Ainda na quarta parte, também estudamos:

- As categorias de serviços dos agentes de nuvem: intermediário, agregação e arbitragem;
- Os tipos de auditorias realizados pelos auditores de nuvem: segurança, privacidade e desempenho.

Na quinta parte, estudamos os componentes da arquitetura:

- Orquestração de serviços com as camadas de serviço, intermediária e recursos físicos;
- Gerenciamento de serviços com as perspectivas de suporte a negócios, fornecimento e configuração, portabilidade e interoperabilidade;
- Segurança e privacidade.

Vimos os dois domínios das áreas críticas de segurança: governança e operacional. Conhecemos as oito áreas de foco críticos do domínio da segurança operacional:

E para encerrar, vimos os sete problemas de segurança da informação na computação em nuvem que geram novos riscos às organizações:

- Disponibilidade da rede;
- Viabilidade do provedor;
- Recuperação de desastres e continuidade do negócio;
- Incidentes de segurança;
- Transparência;
- Perda de controle físico dos dados;
- Aspectos legais e regulatórios.

REFERÊNCIAS

LIU, F. et al. NIST cloud computing reference architecture. **NIST SP**, special publication, v. 500, n. 292, set. 2011. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf>. Acesso em: 19 jun. 2020.

NIST. The NIST definition of cloud computing. **NIST SP**, special publication, v. 800, n. 145, set. 2011. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. Acesso em: 19 jun. 2020.

SILVA, P. M. N. **Recomendações de segurança da informação para soluções de tecnologia da informação e comunicação baseadas em computação em nuvem.** Relatório (Graduação em Redes de comunicação) – Universidade de Brasília. Brasília, 2013.

TAURION, C. **Cloud computing**: computação em nuvem. Rio de Janeiro: Brasport, 2009.

VERAS, M. **Computação em nuvem:** nova arquitetura de TI. Rio de Janeiro: Brasport, 2015.