ORIENTAÇÕES DA CLOUD SECURITY ALLIANCE (CSA)

Apresentando a Cloud Security Alliance (CSA)

A Cloud Security Alliance (CSA) é a organização líder em escala global dedicada a definir e fomentar conscientização sobre as melhores práticas de segurança em ambientes de computação em nuvem.

Dica

O site cloudsecurityalliance.org mantém um blog com diversos artigos interessantes para vários níveis de conhecimento na área, além de white papers instrutivos sobre resultados de pesquisas em segurança na nuvem. Também mantém cursos e certificações e um programa de associação para membros.

A CSA fornece orientações sobre segurança na nuvem como forma de suporte aos objetivos de negócio, gerenciando e mitigando riscos associados com a adoção de soluções abrigadas em ambiente de nuvem organizadas em quatorze domínios, veja a seguir.

- **DOMAIN 1**: Conceitos e arquiteturas de computação em nuvem.
- **DOMAIN 2**: Governança e gestão de risco corporativo.
- **DOMAIN 3**: Questões legais, contratos e descoberta eletrônica.
- **DOMAIN 4**: Gestão de conformidade e auditoria.
- **DOMAIN 5**: Governança da informação.
- **DOMAIN 6**: Plano de gestão e continuidade do negócio.
- **DOMAIN 7**: Segurança de infraestrutura.
- **DOMAIN 8**: Virtualização e contêineres.
- **DOMAIN 9**: Resposta a incidentes.
- **DOMAIN 10**: Segurança de aplicativos.
- **DOMAIN 11**: Segurança e criptografia de dados.
- **DOMAIN 12**: Gerenciamento de identidade, direitos e acesso.
- **DOMAIN 13**: Segurança como serviço.
- **DOMAIN 14**: Tecnologias relacionadas.

Conceitos e Arquiteturas de Computação em Nuvem

Esse domínio provê uma estrutura conceitual (**framework**) que descreve e define computação em nuvem, propõe uma terminologia base e detalha estruturas lógicas e arquiteturais para ambientes em nuvem.

A computação em nuvem pode ser vista como uma tecnologia ou coleção de tecnologias, um modelo de operações, modelo de negócios, um paradigma etc. A definição mais enxuta para computação em nuvem, na visão da CSA, é "um novo modelo operacional e conjunto de tecnologias para gerenciar conjuntos de recursos computacionais compartilhados". Sob uma perspectiva prática e simples, a nuvem pode ser descrita como um conjunto de recursos, tais como processadores e memórias, colocado para trabalhar conjuntamente (resource pooling) em uma operação que utiliza virtualização.

Comentário

O NIST define o usuário da nuvem, mencionado aqui como cliente ou organização cliente, como "a pessoa ou organização que requisita e usa recursos", e provedor de serviços de nuvem como "a pessoa ou organização que entrega os recursos".

As técnicas-chave para criar uma nuvem são **abstração** e **orquestração**. O provedor abstrai os recursos de infraestrutura física para criar o pool e utiliza orquestração para coordenar a montagem e entrega do pool de recursos para os clientes. Essa nova abordagem é uma evolução da virtualização tradicional, com a qual se fazia possível abstrair os recursos, mas não orquestrava a operação deles de forma conjunta. Outros importantes conceitos são:

Segregação

Que "permite que o provedor de nuvem divida os recursos para os diferentes grupos"

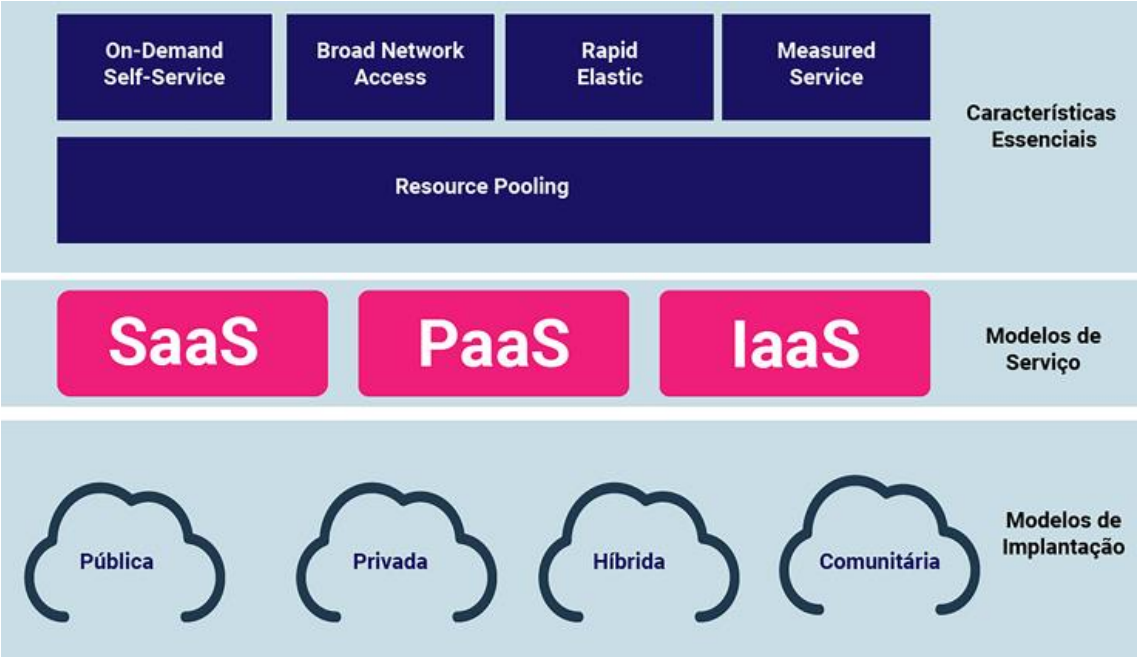
Isolamento

Que "garante que um grupo não possa ver ou modificar os ativos uns dos outros".

A junção da segregação com o isolamento é conhecida como **multilocação** e não se aplica apenas a diferentes organizações, podendo também ser usada

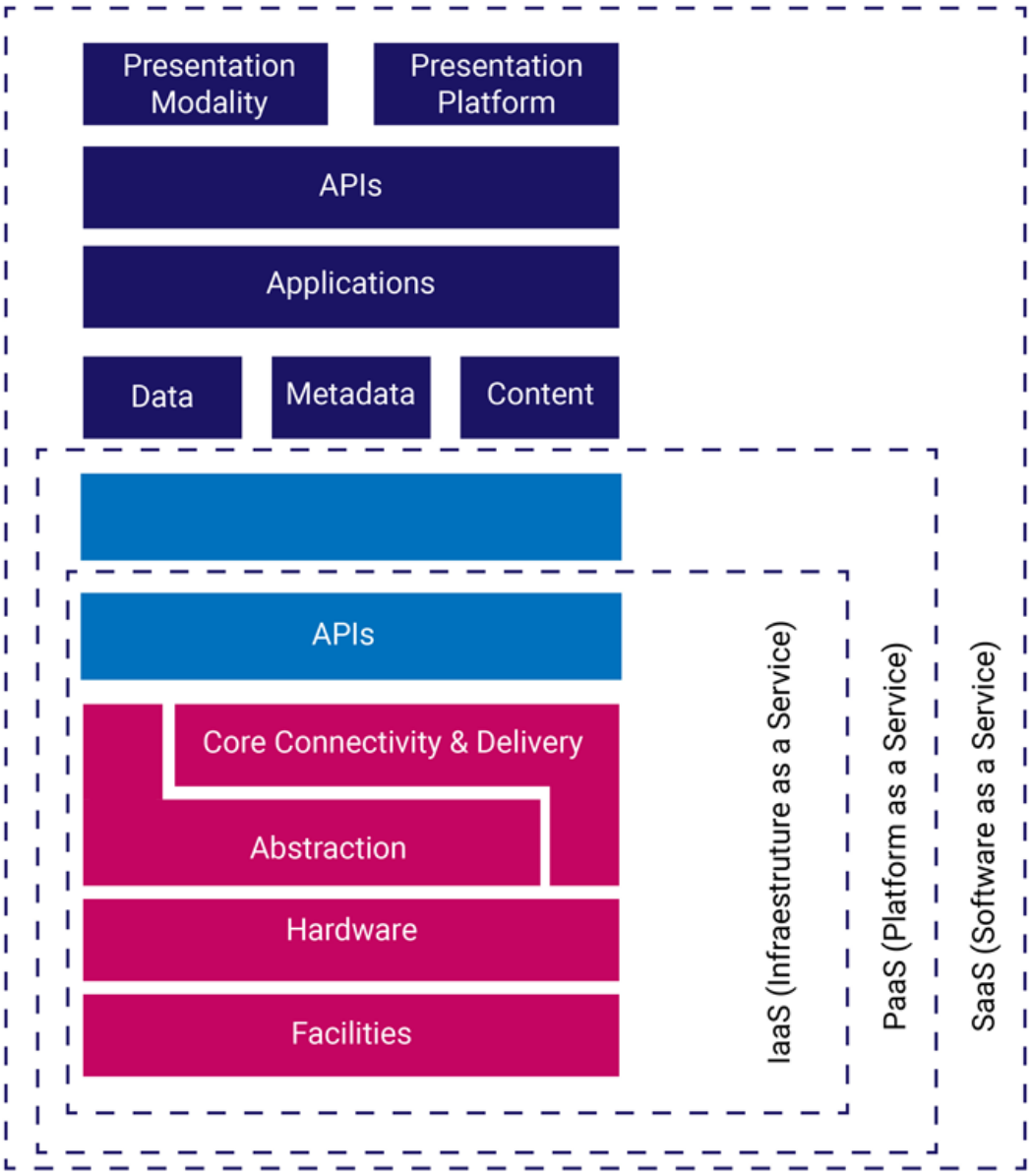
para dividir recursos entre diferentes unidades em uma única empresa ou organização.

A CSA usa modelagem preconizada pelo NIST sintetizada na imagem: Consolidação dos aspectos introdutórios de serviços em nuvem. Endossa também o modelo preconizado pela **Norma ISO/IEC 17788:2014 – Information technology – Cloud computig – Overview and vocabulary**, um documento mais detalhado e exaustivo que apresenta um modelo de referência adicional.



Sobre a modelagem arquitetural, a CSA provê fundamentos para ajudar os profissionais de segurança a tomarem decisões embasadas, bem como uma linha de base para a compreensão de modelos emergentes mais complexos.

Podemos dizer que o modelo de arquitetura preconizado pela CSA se presta a um metamodelo para os provedores montarem e oferecerem seus serviços da forma mais adequada a seus modelos de infraestrutura e negócios no mundo real. A arquitetura de referência da CSA é apresentada na imagem adiante.



Arquitetura de referência da CSA.

Observando por um ponto de vista de mais alto nível, tanto a computação em nuvem quanto a tradicional aderem a um modelo lógico que ajuda a identificar diferentes camadas com base na sua funcionalidade. Isso é útil para ilustrar as diferenças entre os diferentes modelos de computação:

Infraestrutura

Os principais componentes de um sistema de computação, que são: computação, rede e armazenamento. São as partes móveis que funcionam como a base sobre a qual todo o resto é construído

Metaestrutura

Os protocolos e mecanismos que fornecem a interface entre a camada de infraestrutura e as demais camadas. É o amálgama que une as tecnologias e possibilita o gerenciamento e a configuração.

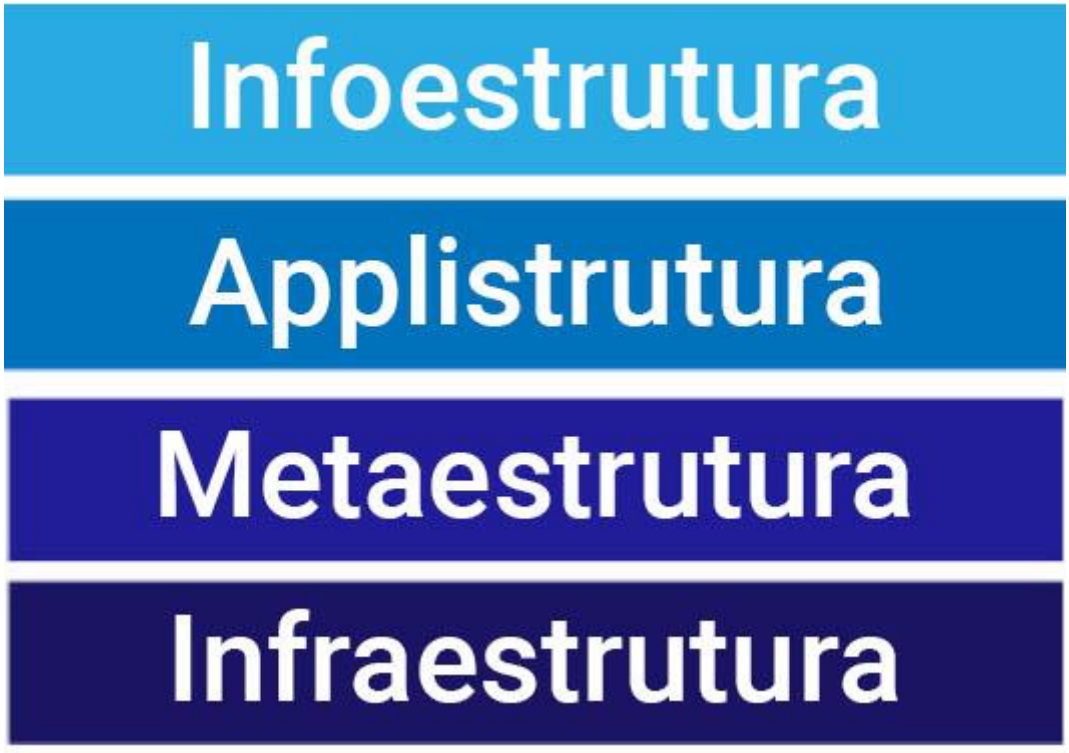
Appliestrutura

A palavra é uma contração que representa os aplicativos implantados na nuvem e os serviços de aplicativos subjacentes usado para construí-los. Por exemplo, recursos de plataforma como serviço, filas de mensagens, análise de inteligência artificial ou notificação, e todos de mais alto nível de abstração.

Infoestrutura

Os dados e informações que podem ser o conteúdo em um banco de dados, armazenamento de arquivos etc.

A imagem a seguir apresenta a pilha de camadas que representa essa arquitetura na visão funcional.



Arquitetura funcional de computação e nuvem.

Os enfoques de segurança variam de acordo com a camada, mas guardam os mesmos princípios básicos de segurança da informação: confidencialidade, integridade e disponibilidade. Computação tradicional ou em nuvem se diferenciam sobretudo pela camada de metaestrutura. A nuvem inclui os componentes para gerenciamento dos recursos das camadas superiores. A

infraestrutura da nuvem também se diferencia pelo já explicado conceito da multilocação.

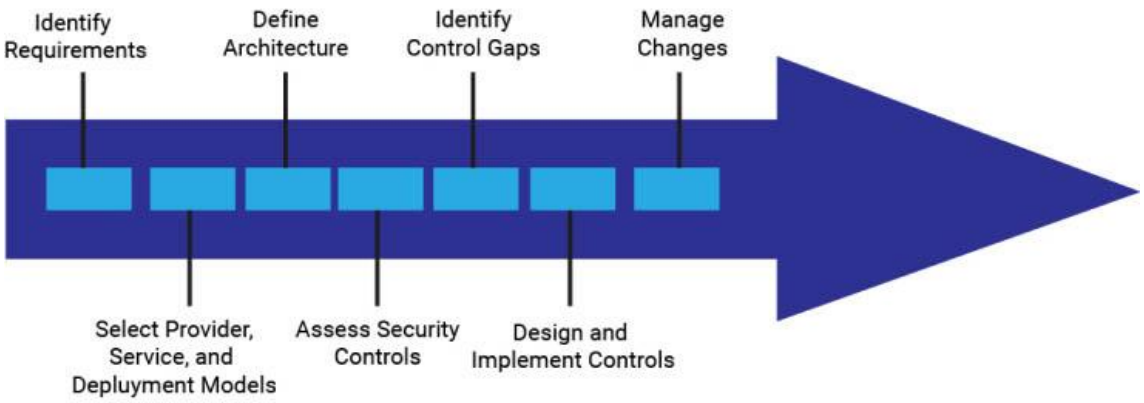
Os modelos de segurança na nuvem são ferramentas para ajudar a orientar as decisões de segurança. O CSA recomenda alguns modelos:

- CSA Enterprise Architecture;
- CSA Cloud Controls Matrix;
- NIST – Cloud Computing Security Reference Architecture (NIST Special Publication 500-299);
- ISO/IEC FDIS 27017 – Information technology – Security techniques – Code of pratice for information security controls based on ISO/IEC 270002 for cloud services.

A CSA estabelece um processo de alto nível, relativamente simples para gerenciar a segurança em nuvem, descrito textualmente pelos passos:

- Identificar os requisitos de segurança e conformidade necessários a quaisquer controles existentes;
- Selecionar o provedor de nuvem, serviço e modelos de implantação;
- Definir a arquitetura;
- Avaliar os controles de segurança;
- Identificar lacunas de controle;
- Projetar e implementar controles para preencher as lacunas;
- Gerenciar as mudanças ao longo do tempo.

Veja a seguir sintetizados na imagem a seguir:



Processo para gestão de segurança em nuvem.

Uma vez estudado o domínio mais fundamental das orientações de segurança em nuvem do CSA, apresentaremos uma visão geral sintetizada dos outros treze domínios. Eles destacam áreas com as quais a computação em nuvem deve se preocupar. Os domínios restantes são divididos em duas grandes categorias: governança e operação.

Os **domínios de governança** são amplos e abordam questões estratégicas e políticas em um ambiente de computação em nuvem. Já os **domínios de operação** se concentram em questões de segurança mais táticas e implementação dentro da arquitetura.

Domínios de Governança

Governança e gestão de risco empresarial

É a capacidade de uma organização governar e gerir o risco corporativo introduzido a partir da adoção da computação em nuvem. Em termos práticos, tais preocupações encampam, por exemplo:

- A capacidade de as organizações clientes avaliarem adequadamente os riscos associados aos serviços do seu provedor de nuvem.
- Precedência legal para os casos de violações de acordos.
- Delegação de responsabilidades na proteção de dados confidenciais quando ambas as partes podem ser culpadas por vazamentos, perdas e outros danos associados aos dados.
- Como as questões jurisdicionais, limites internacionais etc. podem afetar esses problemas.

Aspectos legais

Possíveis problemas legais no uso da computação em nuvem. Incluem requisitos de proteção para informações e sistemas computacionais; leis de não divulgação e de violação de segurança; requisitos regulatórios; requisitos de privacidade; leis internacionais etc.

Compliance e gerenciamento de auditorias

Manter e comprovar a conformidade no uso da computação em nuvem. As questões relacionadas à avaliação de como a computação em nuvem afeta a conformidade com as políticas de segurança interna bem como vários requisitos de conformidade (regulamentares, legislativos e outros) estão incluídos nesse domínio, que engloba ainda algumas orientações sobre como provar a conformidade durante uma auditoria.

Governança da informação

Governança dos dados que são colocados na nuvem. Tais preocupações devem encampar a identificação e o controle de dados na nuvem, bem como controles de compensação que possam ser usados para lidar com a perda de controle físico ao mover dados para a nuvem. Além disso, também lida com questões como quem é responsável pela confidencialidade, integridade e disponibilidade dos dados.

Domínios de Operação

Plano de gestão e continuidade do negócio

Proteção do plano de gestão e de todas as interfaces administrativas usadas para acessar a nuvem, incluindo consoles da web e APIs. Além disso, observa as garantias para a continuidade dos negócios nas implantações em nuvem.

Segurança da infraestrutura

Fundamentos para se operar seguramente. Seus aspectos incluem a segurança dos níveis inferiores da pilha de serviços, como segurança física das instalações, hardware para processamento, memória e armazenamento, rede, e software para orquestração do pool de recursos.

Virtualização e conteinerização

Neste vídeo, será explicado os detalhes sobre o domínio de operação “Virtualização e Conteinerização”.

Aspectos de segurança que cobrem uma grande camada de tecnologia associada à abstração do pool de recursos, especificamente a computação, a rede, os armazenadores e os contêineres em sua relação com o serviço de

virtualização. Em termos práticos refere-se à segurança dos hipervisores, contêineres e redes definidas por software.

Compreender os impactos da virtualização na segurança é fundamental para arquitetar e implementar adequadamente a segurança na nuvem.

Em termos práticos, refere-se à segurança dos hipervisores, contêineres e redes definidas por software.

Resposta a incidentes

Detecção, resposta, notificação e remediação de incidentes de formas apropriadas. Estabelece os limites de responsabilidade por ações compartilhadas entre provedor e cliente para permitir o tratamento adequado de incidentes e a análise forense.

Segurança das aplicações

Neste vídeo, serão explicados os detalhes sobre o domínio de operação “Segurança das aplicações”.

Proteção dos softwares aplicativos que estão sendo executados ou implantados na nuvem. Na prática, inclui questões como saber se é apropriado migrar ou projetar um aplicativo para ser executado na nuvem e, em caso afirmativo, que tipo de plataforma de nuvem é mais apropriada (SaaS, PaaS ou IaaS).

Criptografia e segurança de dados

Implementação dos mecanismos de segurança e criptografia de dados e toda a garantia de gerenciamento de chaves, considerando os aspectos de escalabilidade dos serviços e dos aplicativos que rodam no ambiente da nuvem.

Gerenciamento de acessos, privilégios e identidades

Gerenciamento de identidades apoiado nos serviços de diretório para fornecer controle de acesso. Identidades, privilégios e acessos (IAM) são profundamente impactados pela computação em nuvem. Tanto na nuvem

pública quanto na particular, as duas pontas (provedor e cliente) são necessárias para gerenciar o IAM sem comprometer a segurança, e a divisão exata das responsabilidades é um aspecto extremamente crítico.

Tecnologias relacionadas

Tecnologias estabelecidas e emergentes que tenham estreito relacionamento com a computação em nuvem, incluindo Big Data, Internet das Coisas (IoT), computação móvel etc.