



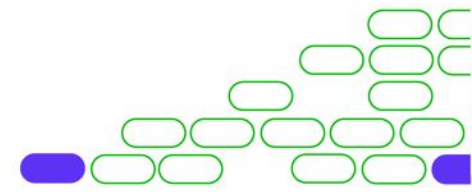
Faculdade



Segurança de Infraestrutura Cloud

CAPÍTULO 1. FUNDAMENTOS E CONCEITOS SOBRE CLOUD COMPUTING

PROF. MACGAYVER MARQUES





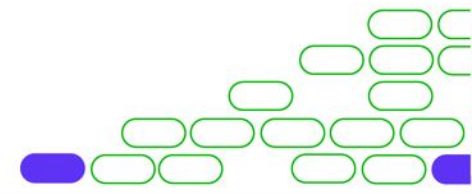
Faculdade



Segurança de Infraestrutura Cloud

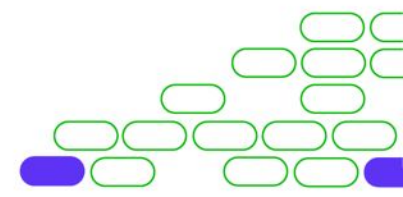
AULA 1.1. INTRODUÇÃO A CLOUD COMPUTING

PROF. MACGAYVER MARQUES



Nesta aula

- ❑ Introdução a Cloud Computing.
- ❑ Benefícios da Cloud Computing.



O que é a Cloud Computing?

A computação em nuvem é a entrega de recursos de TI sob demanda por meio da Internet com definição de preço de pagamento conforme o uso para um provedor de nuvem.

- Capacidade computacional
- Armazenamento
- Bancos de dados



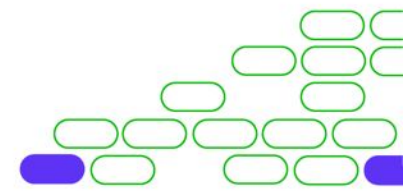
Provedores Cloud

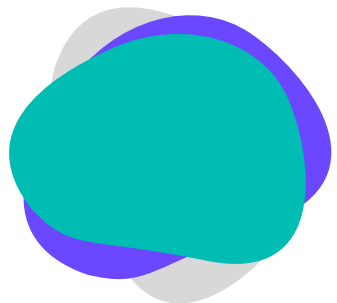




XPe

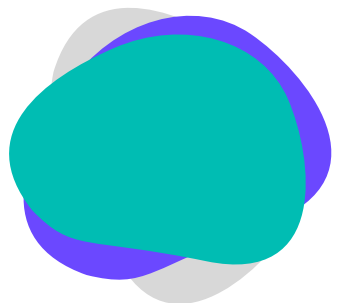
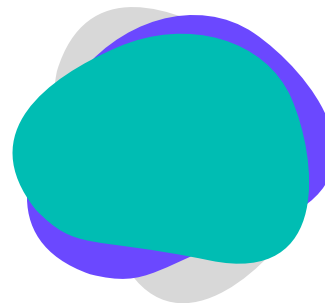
Devo utilizar Cloud Computing?





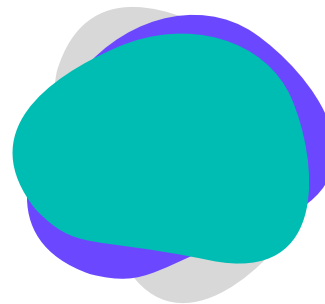
A utilização da cloud proverá as tecnologias e recursos que seu negócio precisa?

Funciona dentro do modelo financeiro da sua organização?

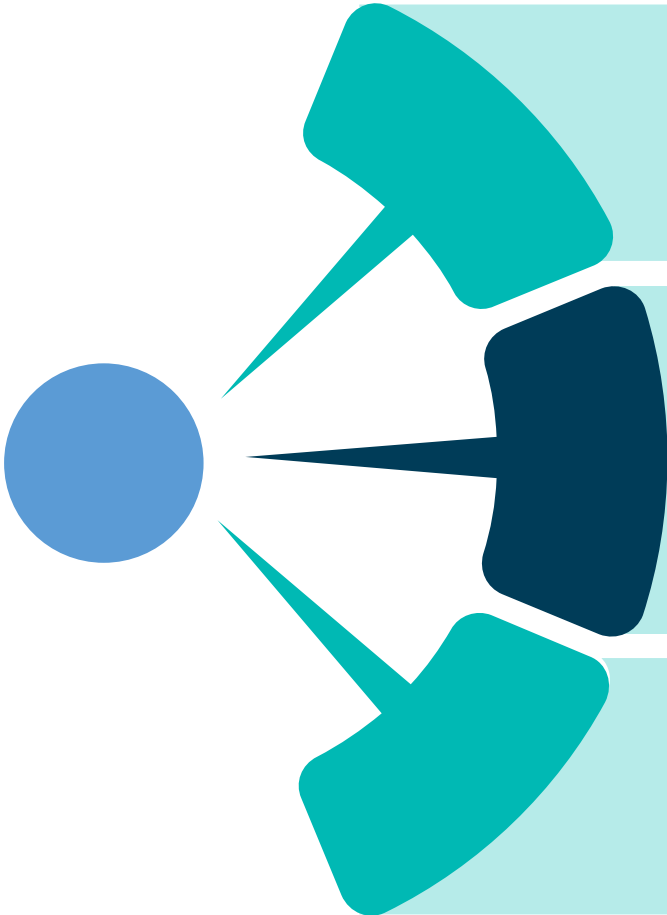


Qual opção oferece o nível de segurança de que você precisa?

Quanta agilidade você precisa?



Benefícios da Cloud Computing



Flexibilidade: Os usuários podem dimensionar serviços para atender às suas necessidades, personalizar aplicativos e acessar serviços em nuvem de qualquer lugar com uma conexão à Internet.

Eficiência: Os usuários corporativos podem colocar os aplicativos no mercado rapidamente, sem se preocupar com os custos ou manutenção da infraestrutura subjacente.

Valor Estratégico: Os serviços em nuvem oferecem às empresas uma vantagem competitiva, fornecendo a tecnologia mais inovadora disponível.

Conclusão

- ✓ Cloud Computing deixou de ser uma tendência e já é uma realidade.
- ✓ Em grande parte dos casos, a Cloud Computing trás agilidade e economia para as organizações.



Próxima aula

01.

Virtualização de Recursos.

03.

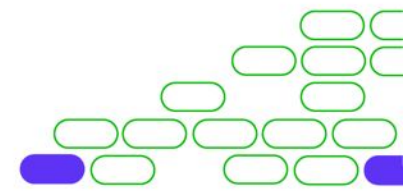
Serviços Sob Demanda.

02.

Elasticidade.

04.

Escalabilidade.





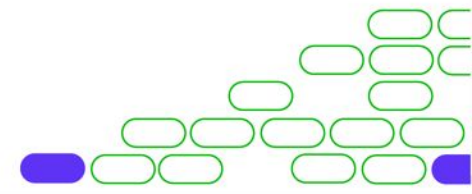
Faculdade



Segurança de Infraestrutura Cloud

AULA 1.2. PROPRIEDADES DA CLOUD COMPUTING

PROF. MACGAYVER MARQUES



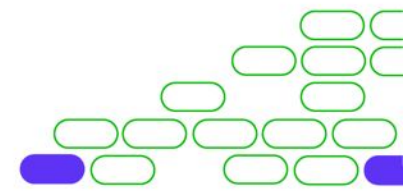
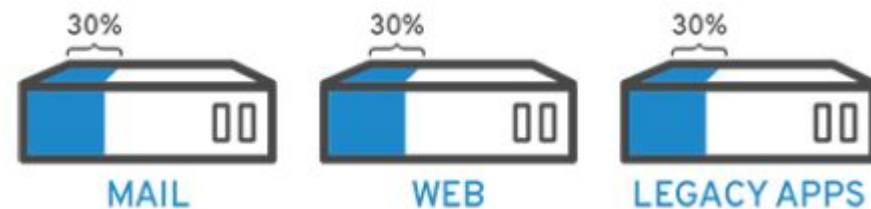
Nesta aula

- ☐ Virtualização de Recursos.
- ☐ Serviços Sob Demanda.
- ☐ Elasticidade.
- ☐ Escalabilidade.



Virtualização de recursos

A virtualização permite que o usuário use toda a capacidade de uma máquina física ao proporcionar a distribuição dos recursos entre diversos usuários ou ambientes.



Serviços Sob Demanda

A propriedade de disponibilizar recursos computacionais de forma automática, sem a necessidade de interação humana com o provedor de cada serviço na quantidade e pelo período que se **demandar**.



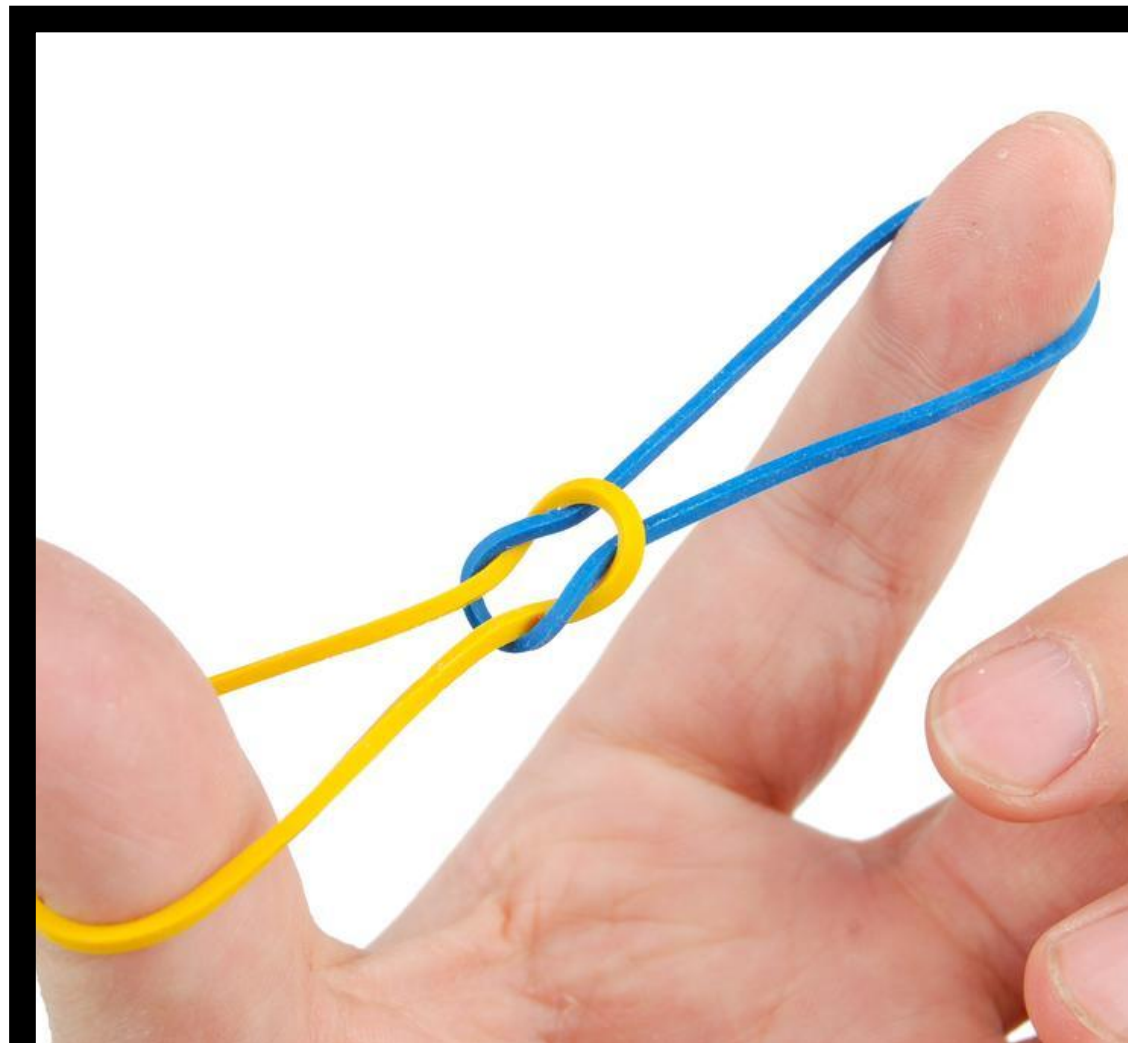
Escalabilidade

- **Aumentar** a capacidade de atender a carga de trabalho **crescente**.
- Se adapta apenas ao **aumento da carga de trabalho** pelo **provisionamento** dos recursos de maneira **incremental**.
- **Scaling up** é a capacidade de fazer com que **um componente seja mais robusto** para suportar um aumento de carga.
- **Scalling out** é a capacidade de se **adicionar mais recursos em paralelo** para lidar com uma carga maior.



Elasticidade

- Elasticidade se adapta tanto ao **aumento** quanto à **diminuição** da carga de trabalho ao **provisionar e desprovisionar** recursos de maneira **autônoma**
- No ambiente elástico, os recursos disponíveis correspondem as **demandas atuais**, tanto quanto possível.



Conclusão

- ✓ Os recursos na cloud são virtualizados.
- ✓ Escalabilidade é a propriedade de se aumentar um determinado recurso sob demanda.
- ✓ Elasticidade é a propriedade de aumentar ou diminuir recursos de forma autônoma dependendo da carga de trabalho.



Próxima aula

01.

Infraestrutura como Serviço
(IaaS).

02.

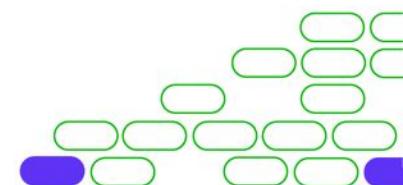
Plataforma como Serviço (PaaS).

03.

Software como Serviço (SaaS).

04.

Cloud Privada, Híbrida e Pública.





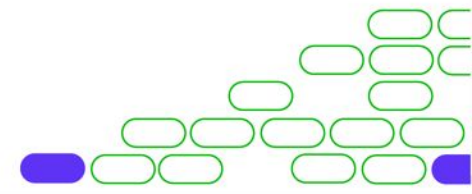
Faculdade



Segurança de Infraestrutura Cloud

AULA 1.3. TIPOS DE INFRAESTRUTURA CLOUD

PROF. MACGAYVER MARQUES



Nesta aula

- ☐ Infraestrutura como Serviço (IaaS).
- ☐ Plataforma como Serviço (PaaS).
- ☐ Software como Serviço (SaaS).
- ☐ Cloud Privada, Híbrida e Pública.



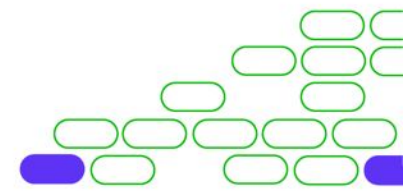
O que é “jornada para a nuvem”?



Infraestrutura como Serviço (IaaS)

Neste tipo de serviço, os provedores cloud oferecem recursos de **computação básicos** para serem utilizados arbitrariamente pelos clientes.

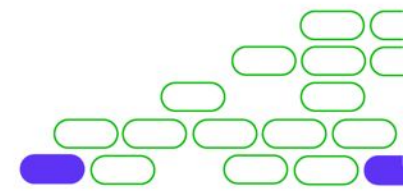
- Máquinas virtuais
- Storage
- Redes



Plataforma como Serviço (PaaS)

Neste tipo de serviço, os provedores cloud oferecem uma plataforma para que o cliente desenvolva, hospede, teste e execute um workload.

- Web server
- Banco de Dados



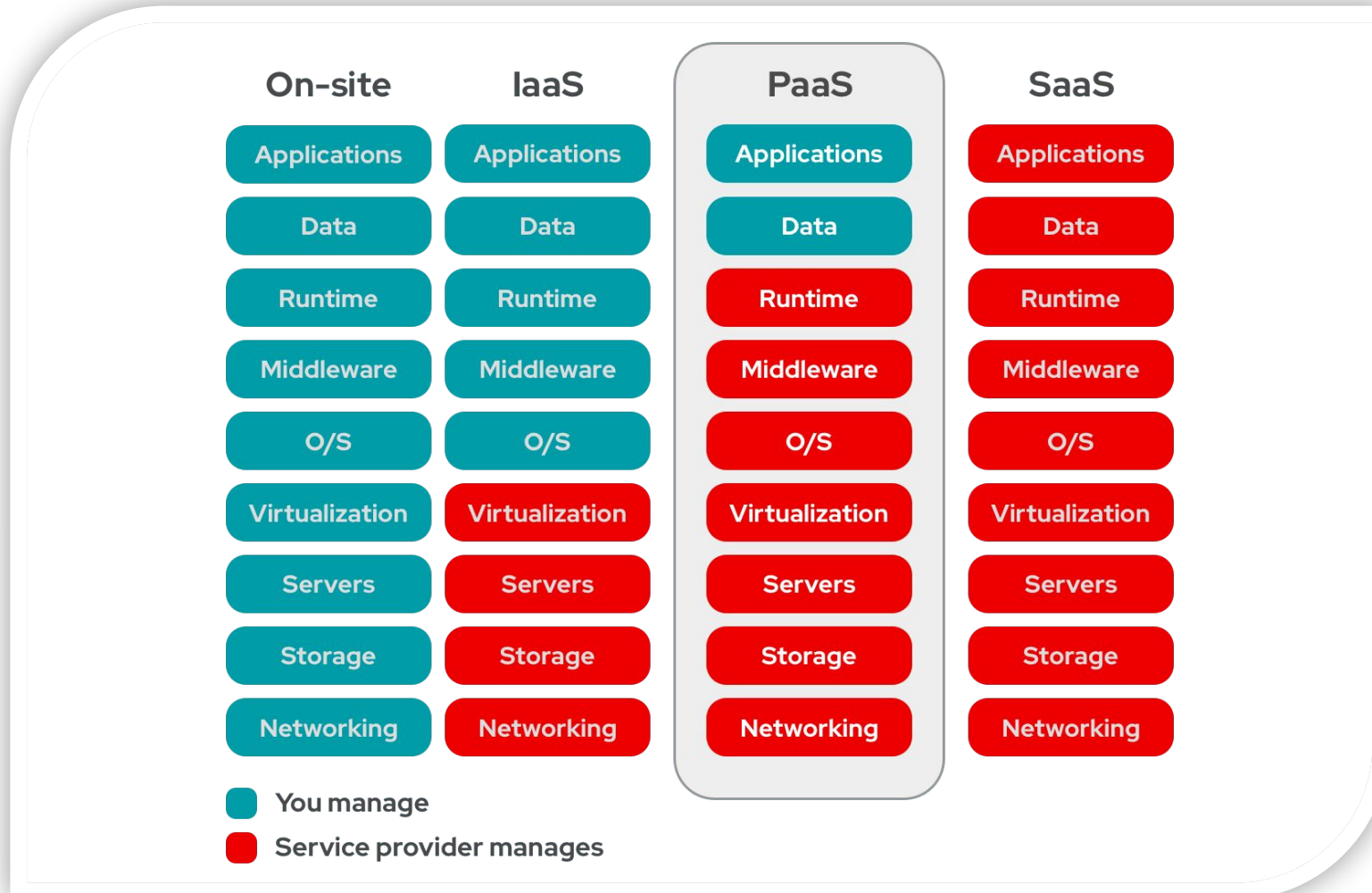
Software como Serviço (SaaS)

No modelo SaaS aplicações são fornecidas para a utilização do cliente. O provedor cloud é o responsável pelo desenvolvimento, configuração e manutenção.

- Dropbox
- Office 365
- G-Suite
- Slack



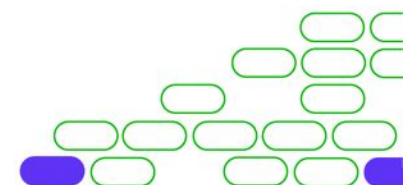
Resumindo...





Cloud Privada

Uma **cloud privada** consiste na utilização de recursos computacionais **dedicados** para uma única empresa, podendo estar localizados em um datacenter da própria empresa ou hospedada por um provedor cloud terceiro.



Cloud Híbrida

Uma **cloud híbrida** oferece às organizações vantagens como maior **flexibilidade**, mais opções de implantação, segurança, conformidade e obtenção de mais valor da **infraestrutura existente** que elas possuem.



Cloud Pública

Através do modelo de cloud pública, os clientes conseguem realizar a implementação de recursos computacionais, **sem ter que fazer a aquisição destes**, pois eles pertencem a um provedor de serviços cloud e o **cliente paga apenas pela hospedagem** de suas aplicações e dados pelo tempo que estes recursos foram utilizados no provedor cloud.



Google Cloud



Conclusão

- ✓ O melhor modelo de cloud a ser adotado **depende** da necessidade da organização.
- ✓ Modelos de PaaS e SaaS, normalmente, são mais baratos do que IaaS.
- ✓ Cloud Híbrida é o modelo mais adotado por organizações que já possuem datacenter local.





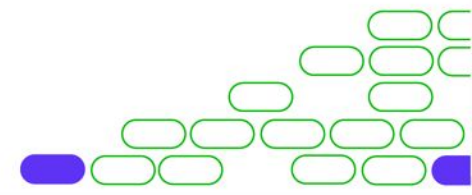
Faculdade



Segurança de Infraestrutura Cloud

CAPÍTULO 2. ON PREMISES VS. CLOUD

PROF. MACGAYVER MARQUES





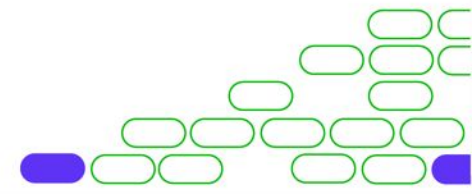
Faculdade



Segurança de Infraestrutura Cloud

AULA 2.1. ON PREMISES VS CLOUD

PROF. MACGAYVER MARQUES



Nesta Aula

- ❑ Modelo de Responsabilidade Compartilhada.
- ❑ Principais diferenças entre On Premises e Cloud.



Desenvolvimento

On premises: **Localmente** e responsabilidade de sustentação de toda a solução e todos os processos relacionados.

Cloud: Localizado no **datacenter do provedor cloud** e fornece mais agilidade no processo.



Controle

On premises: Responsabilidade total pelo controle de acesso físico e lógico em seu datacenter e aplicações.

Cloud: Responsabilidade compartilhada.

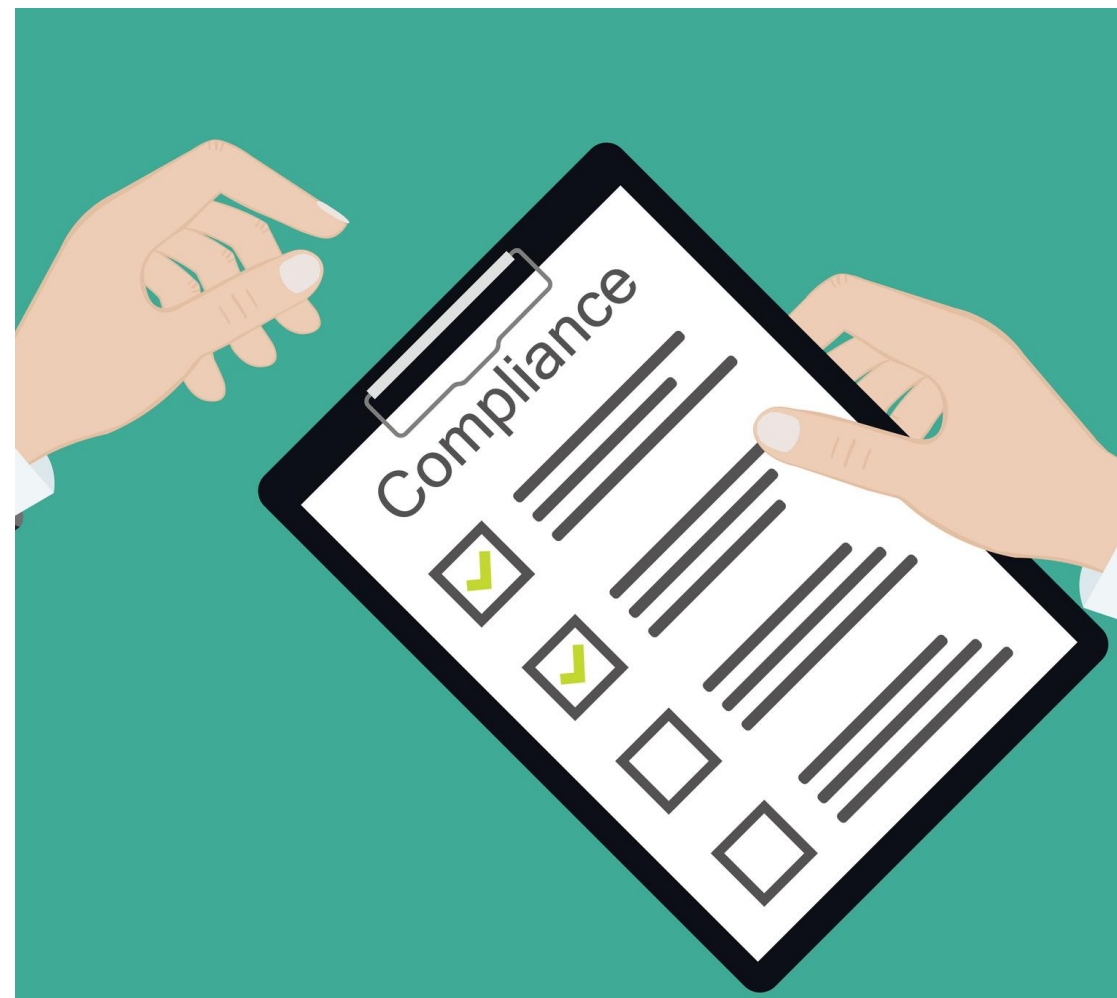


Segurança



Conformidade

- Controles regulatórios
- Segurança de dados sensíveis
- Privacidade
- Auditorias



Custos

On-Premises

9%
software licenses

Customization &
implementation

Hardware

IT personnel

Maintenance

Training



Ongoing costs

- Apply filters, patches, upgrade
- Downtime
- Performance tuning
- Rewrite integrations
- Upgrade dependent applications
- Ongoing burden on IT
- Maintain/upgrade hardware
- Maintain/upgrade network
- Maintain/upgrade security
- Maintain/upgrade database

Cloud Computing

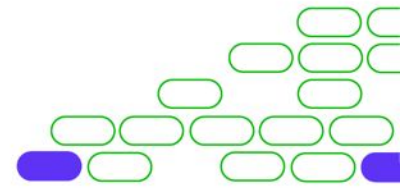
68%
subscription fee

Implementation,
Customization &
training

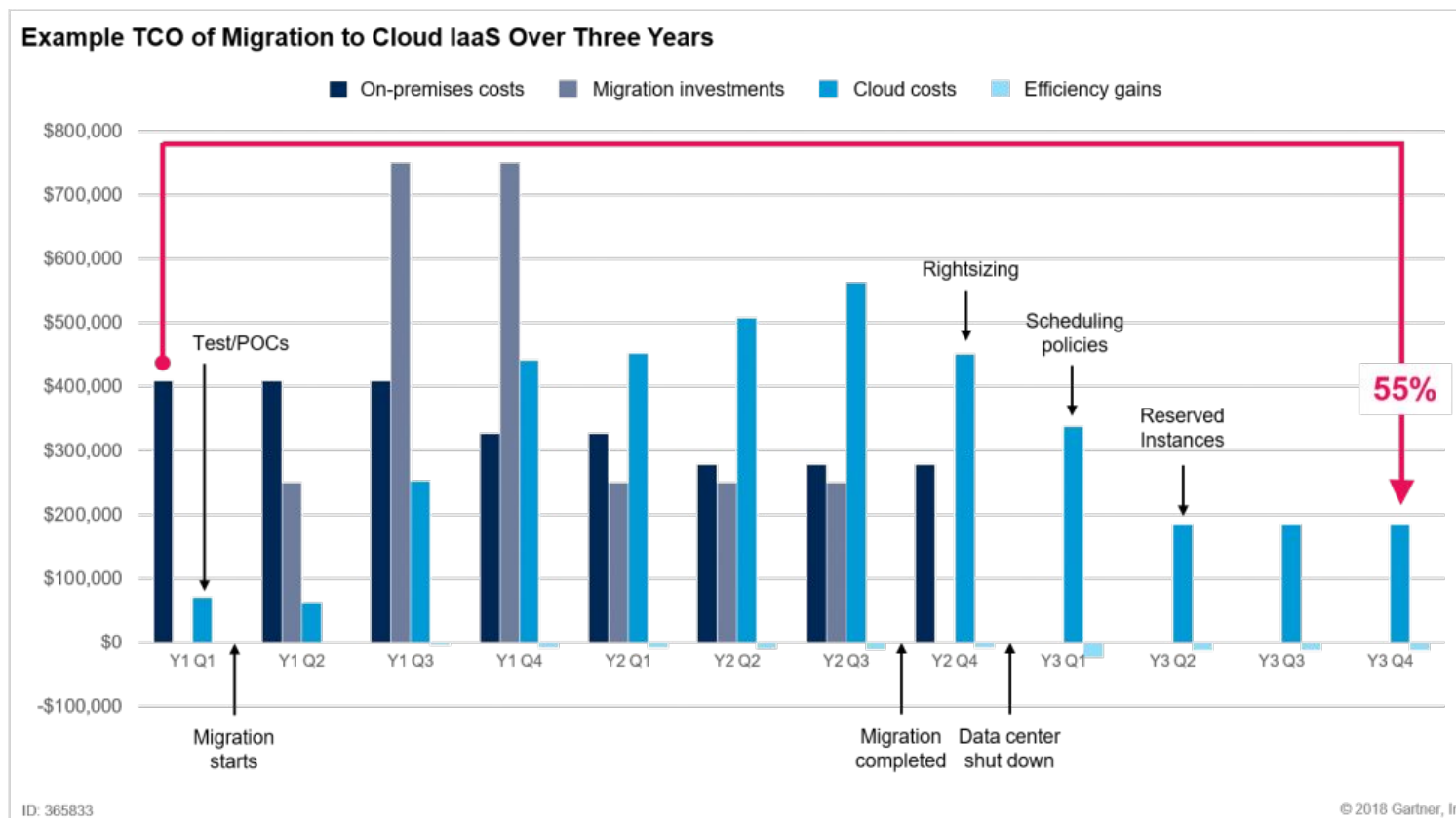


Ongoing costs

- Subscription fee



Custos de migração Gartner



Conclusão

- ✓ Existem diversos benefícios quando comparamos ambiente cloud com on premises, mas temos que nos atentar às necessidades **regulatórias**.
- ✓ A **segurança** na **cloud** é **compartilhada**.
- ✓ Os custos na cloud são ajustados ao longo do tempo.



Próxima aula

01.

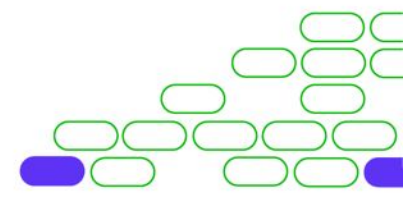
Quem é AWS.

03.

Recursos AWS e Azure.

02.

Quem é Azure.





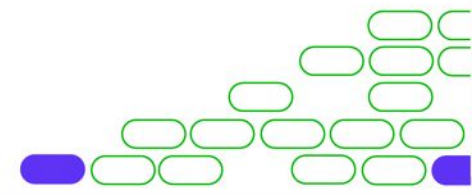
Faculdade



Segurança de Infraestrutura Cloud

CAPÍTULO 3. AMBIENTES, TECNOLOGIAS E RECURSO DE CLOUD (AWS E AZURE)

PROF. MACGAYVER MARQUES





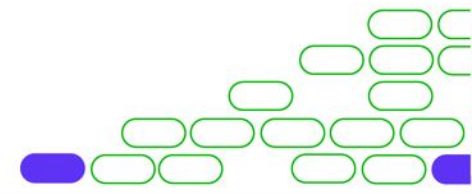
Faculdade



Segurança de Infraestrutura Cloud

AULA 3.1.1. AMBIENTE, TECNOLOGIAS E RECURSO DE CLOUD AWS E AZURE (PARTE 1)

PROF. MACGAYVER MARQUES



Nesta Aula

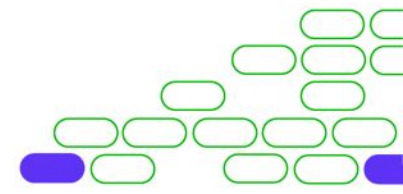
- ☐ Quem é AWS?
- ☐ Quem é Azure?
- ☐ Computação.
- ☐ Containers e orquestradores.
- ☐ Serverless.
- ☐ Database.



Por que AWS e Azure?

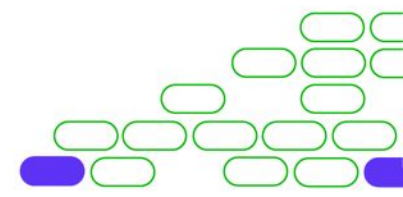


Figure 1. Magic Quadrant for Cloud Infrastructure and Platform Services



Quem é a AWS?

- Empresa de Jeff Bezos.
- Em 2006, a Amazon Web Services (AWS) começou a oferecer serviços de infraestrutura de TI para empresas por meio de serviços web – hoje conhecidos como cloud computing.
- A nuvem da AWS abrange 80 zonas de disponibilidade em 25 regiões geográficas em todo o mundo, com planos anunciados para mais 18 zonas de disponibilidade e mais 6 regiões da AWS na Austrália, Índia, Indonésia, Espanha, Suíça e Emirados Árabes Unidos (Emirados Árabes Unidos).



Quem é o Azure?

- Empresa de Bill Gates.
- O Microsoft Azure é uma plataforma destinada à execução de aplicativos e serviços, baseada nos conceitos da computação em nuvem.
- A apresentação do serviço foi feita no dia 27 de outubro de 2008 durante a Professional Developers Conference, em Los Angeles e lançado em 1 de Fevereiro de 2010 como Windows Azure, para então ser renomeado como Microsoft Azure em 25 de Março de 2014.



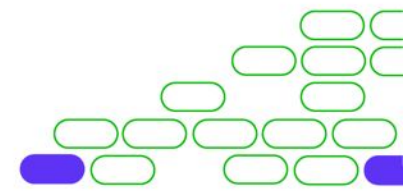
Computação



- Elastic Computing Cloud (EC2)
- Batch
- Auto Scaling
- VMWare Cloud on AWS
- Parallel Cluster



- Máquinas Virtuais
- Batch
- Virtual Machine Scale Sets
- Azure VMWare Solution
- Cycle Cloud



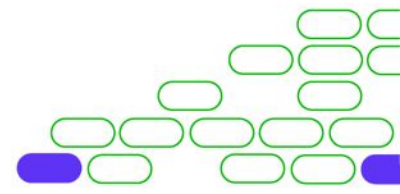
Containers e orquestradores



- Elastic Computing Service (ECS)
- Elastic Container Registry
- Elastic Kubernetes Service (EKS)



- Container Instances
- Container Registry
- Azure Kubernetes Services (AKS)



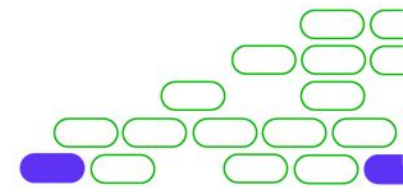
Serverless



- Lambda



- Functions



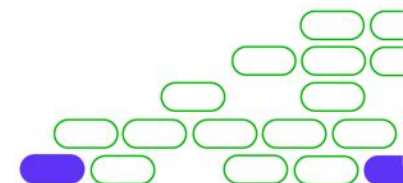
Database



- Bancos de dados relacionais:
 - RDS
- NoSQL/Document:
 - DynamoDB
 - SympLeDB
 - Amazon DocumentDB
- Caching:
 - ElasticsChashe



- Bancos de dados relacionais
 - SQL Database
 - Database for MySQL
 - Database for PostgreeSQL
- NoSQL/Document:
 - CosmosDB
- Caching:
 - Cashe for Redis



Conclusão

- ✓ AWS e Azure são os maiores players de cloud pública da atualidade.
- ✓ Ambos possuem serviços diferentes com finalidades idênticas.



Próxima aula

01.

Recursos AWS e Azure.





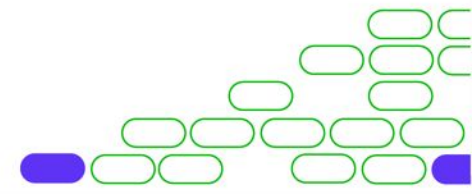
Faculdade



Segurança de Infraestrutura Cloud

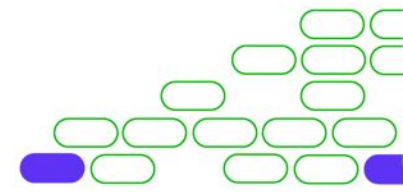
AULA 3.1.2. AMBIENTE, TECNOLOGIAS E RECURSO DE CLOUD AWS E AZURE (PARTE 2)

PROF. MACGAYVER MARQUES



Nesta Aula

- DevOps e Monitoramento
- Gerenciamento
- Mensagens e eventos
- Networking
- Autenticação e Automação
- Criptografia
- Firewall
- Security
- Storage
- Web Applications



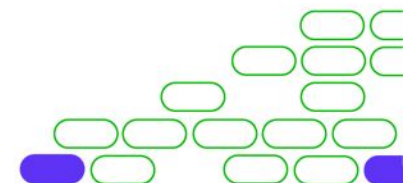
DevOps e monitoramento



- Cloud Watch, X-Ray
- CodeBuild
- Developer Tools
- Cloud Formation
- Command Line Interface
- AWS Cloud Shell
- OpsWorks



- Monitor
- DevOps
- Developer Tools
- Resource manager, Azure Automation
- CLI, PowerShell
- Azure Cloud Shell
- Automation



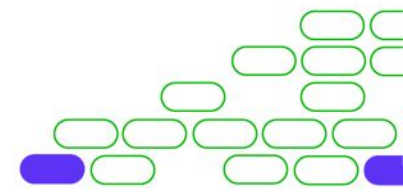
Gerenciamento



- Trusted Advisor
- Usage and Billing Report
- Management Console
- Application Discovery Service
- EC2 System Manager, Cloud Trail
- CloudWatch
- Cost Explorer



- Advisor
- Billing API
- Portal
- Migrate
- Monitor
- Application Insights
- Cost Management



Mensagens e Eventos



- Simple Queue Service
- Amazon EventBridge



- Queue Storage, Service Bus
- EventGrid

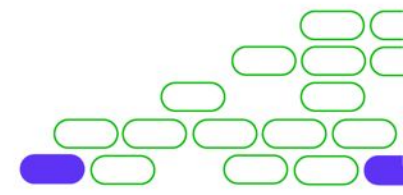
Networking



- Virtual Private Cloud
- VPN Gateway
- Route 53
- Direct Connect
- Network Load Balancer
- Application Load Balancer



- Virtual Network
- VPN Gateway
- DNS, Traffic Manager
- Express Route
- Load Balancer
- Application Gateway



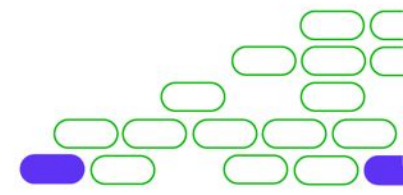
Autenticação e Autorização



- Identity and Access Management (IAM)
- Identity and Access Management (IAM)
- Organizations
- Directory Services
- Cognito
- Organizations



- Azure Active Directory
- Azure role-based access control
- Subscription Management
- Azure Active Directory Domain Services
- Azure Active Directory B2C
- Policy, Management Groups



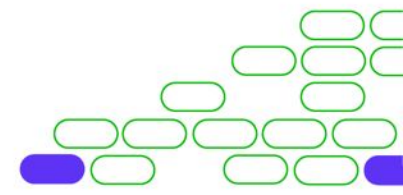
Criptografia



- Amazon S3 Key Management
- Key Management Service (KMS), CloudHSM



- Azure Storage Service Encryption
- Key Vault



Firewall



- Web Application Firewall
- Web Application Firewall



- Web Application Firewall
- Firewall

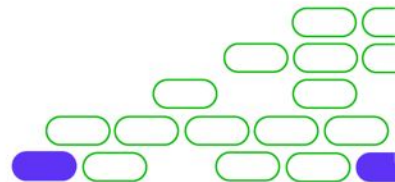
Security



- Inspector
- Certificate Manager
- GuardDuty
- Artifact
- Shield



- Security Center
- App Service Certificates
- Advanced Threat Protection
- Service Trust Portal
- DDoS Protection Service



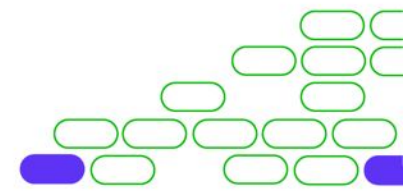
Storage



- Simple Storage Services (S3)
- Elastic Block Store (EBS)
- Elastic File System
- S3 Infrequent Access (IA)
- S3 Glacier
- Backup
- Storage Gateway



- Blob Storage
- Managed disks
- Files
- Storage cool tier
- Storage archive access tier
- Backup
- StorSimple



Web Applications



- Elastic Beanstalk
- API Gateway
- CloudFront
- Global Accelerator



- App Service
- API Management
- Content Delivery Network
- Front Door

Conclusão

- ✓ Visão geral dos principais serviços AWS e Azure.
- ✓ Tanto Azure quanto AWS possuem recursos com a mesma finalidade.





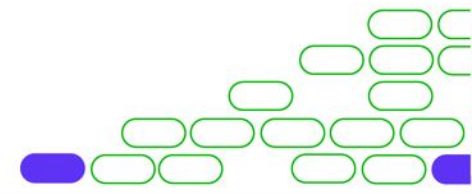
Faculdade



Segurança de Infraestrutura Cloud

CAPÍTULO 4. SEGURANÇA EM CLOUD

PROF. MACGAYVER MARQUES





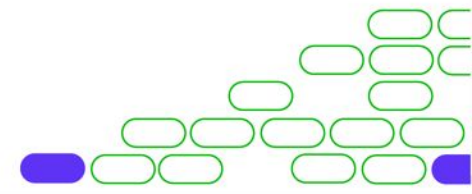
Faculdade



Segurança de Infraestrutura Cloud

AULA 4.1. MODELO DE PROCESSO E CONTROLES DE CLOUD SECURITY

PROF. MACGAYVER MARQUES



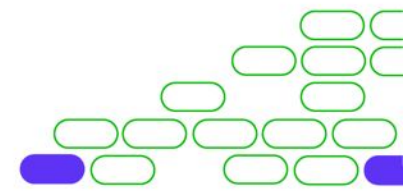
Nesta Aula

- ☐ Modelo de processo de Cloud Security.
- ☐ Gestão de acesso e identidade (IAM).
- ☐ Controles de Segurança de Infraestrutura.
- ☐ Controles de Segurança de Dados.
- ☐ Controles de Log e Monitoramento.
- ☐ Controles de Ameaças e Vulnerabilidades.



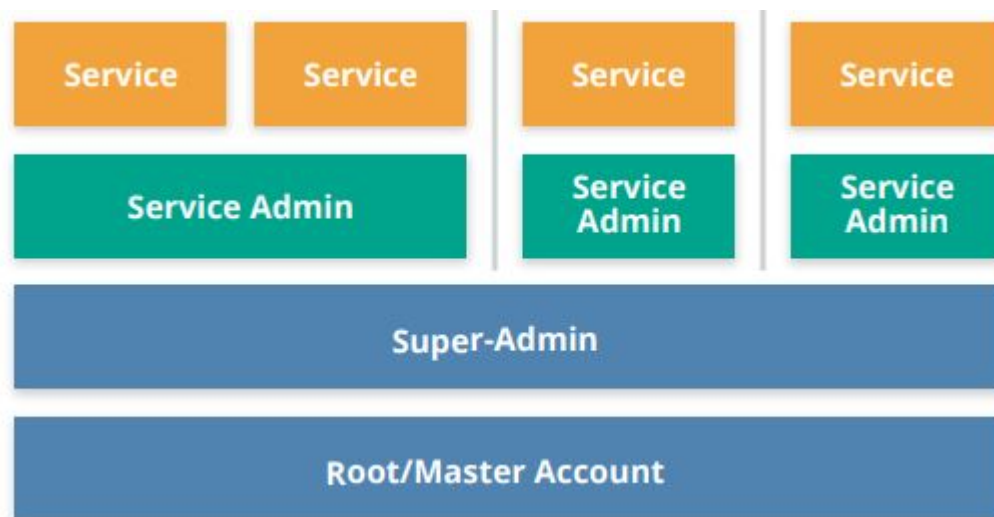
Modelo de Processo de Cloud Security

- Identificação de requisitos de segurança e conformidade e tipos de controle existentes.
- Selecionar seu provedor cloud, serviços e modelos de desenvolvimento.
- Definir a arquitetura.
- Avaliar os controles de segurança.
- Identificar os gaps de controle.
- Desenhar e implementar os controles para preencher os gaps.
- Gerenciar as mudanças ao longo do tempo.



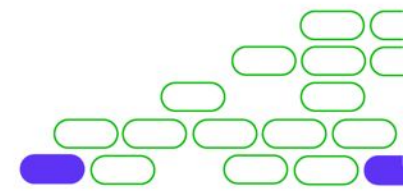
Gestão de Acesso e Identidade (IAM)

- Identificação, autenticação e autorização.
- Serve para determinar **quem** pode fazer **o que** na sua plataforma cloud.



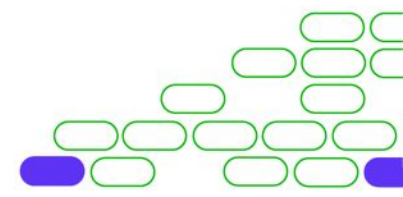
Controles IAM

- Política de senhas fortes.
- Inventário de identidades.
- Least Privilege.
- Provisionamento, mudança, revisão e revogação de acesso de usuário.
- Segregação e aprovação de roles com acessos privilegiados.
- Manter integridade dos logs.
- Autenticação forte.
- Gestão de senhas.
- Mecanismos de autorização.



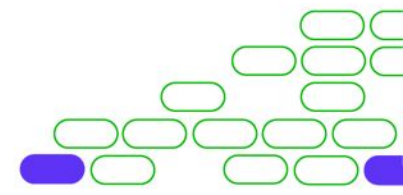
Controles de Segurança de Infraestrutura

- Planejamento de capacidade e recursos.
- Segurança de redes.
- Hardening de Sistema Operacional e security baseline.
- Separação de ambientes de Produção e Não-produção.
- Definir, implementar e avaliar processos, procedimentos e técnicas de defesa em profundidade para proteção, detecção e resposta oportuna a ataques baseados em rede.
- Segmentação e segregação de acesso ao Tenant.
- Utilização de protocolos seguros para migração para Cloud.
- Documentação de arquitetura de redes para ambientes de alto-risco.



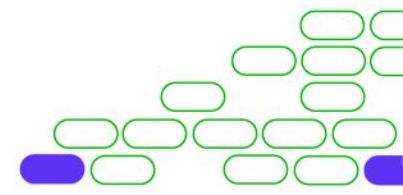
Controles de Segurança de Dados

- Classificação de dados.
- Inventário de Dados.
- Documentação de fluxo de dados.
- Propriedade e administração de dados (quem é o dono do dados e quem pode ter qual acesso naquele dado).
- Proteção de dados por design e padrão.
- Avaliação do impacto da proteção de dados.
- Proteger transferência da dados sensíveis.
- Acesso, reversão, retificação e exclusão de dados pessoais.



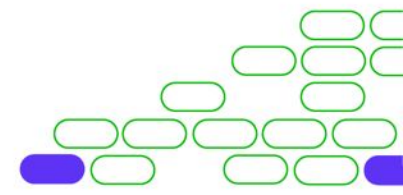
Controles de Log e Monitoramento

- Procedimento e políticas de Log e monitoramento.
- Proteção e monitoramento de Logs de auditoria.
- Monitoramento e alerta de segurança.
- Sincronização de relógio (NTS).
- Escopo, Registro e Proteção de Logs.
- Monitorar e gerar relatórios de Criptografia.
- Registro de transações/atividades.



Controles de Ameaças e Vulnerabilidades

- Política e procedimentos de ameaças e vulnerabilidades.
- Política e procedimentos de proteção contra Malwares.
- Agendar remediação de vulnerabilidades.
- Penetration Testing.
- Identificação, priorização e gerenciamento de vulnerabilidades.



Conclusão

- ✓ Existem frameworks e documentos para auxiliar na definição dos controles que devem ser realizados na cloud, como o [Cloud Controls Matrix version 4.0](#) da Cloud Security Alliance que foram a referência para a produção deste módulo.
- ✓ A responsabilidade pelos controles variam dependendo do tipo de serviço (IaaS, PaaS, SaaS).



Próxima aula

01.

Controles de Aplicação e Interface.

02.

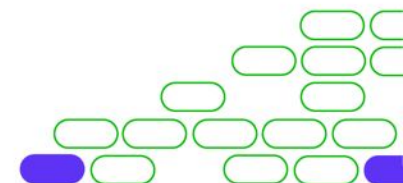
Controles de Criptografia e Key Management.

03.

Controles de Gestão de Incidentes, E-discovery e Cloud Forensis.

04.

Controles de Gerenciamento de Endpoints.





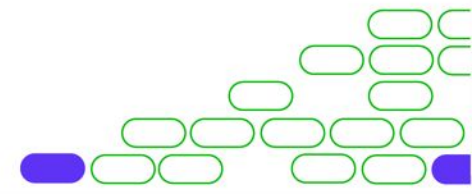
Faculdade



Segurança de Infraestrutura Cloud

AULA 4.2. CONTROLES DE CLOUD SECURITY

PROF. MACGAYVER MARQUES



Nesta Aula

- ☐ Controles de Aplicação e Interface.
- ☐ Controles de Criptografia e Key Management.
- ☐ Controles de Gestão de Incidentes, E-discovery e Cloud Forensis.
- ☐ Controles de Gerenciamento de Endpoints.



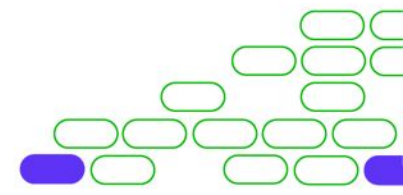
Controles de Aplicação e Interface

- Política e procedimentos de segurança de aplicativos e interfaces.
- Estabilizar, documentar e manter requisitos de baseline para segurança de aplicações.
- Desenvolvimento e desenho de aplicações seguras.
- Desenvolvimento automatizado de aplicações seguras.
- Testes de segurança de aplicação automatizados.
- Remediação de vulnerabilidades de aplicações.



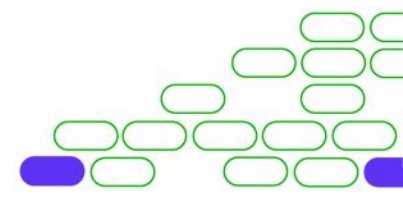
Controles de Criptografia e Key Management

- Política e procedimentos de criptografia e Key Management.
- Definição e implementação roles e responsabilidades de criptografia e key management.
- Criptografia de Dados.
- Gerenciamento de Mudanças de Criptografia.
- Auditoria de Criptografia e key management.
- Geração, rotação, revogação, suspensão, desativação, arquivamento, destruição e recuperação de Keys.
- Gerenciamento de Inventário de Chaves.



Controles de Gestão de Incidentes, E-discovery e Cloud Forensis

- Política e procedimentos de Gerenciamento de Incidentes de Segurança.
- Plano de resposta a incidentes.
- Testes de respostas a incidentes.
- Notificação de ameaça de segurança.
- Manter pontos de contato para autoridades regulatórias aplicáveis, autoridades locais e nacionais de aplicação da lei e outras autoridades jurisdicionais legais. (ANPD)



Controles de Gerenciamento de Endpoints

- Política e procedimentos de Gerenciamento de endpoints.
- Wipe Remoto.
- Aprovação de aplicações e serviços.
- Postura de segurança de endpoint de terceiros.
- Compatibilidade com sistemas e aplicações.
- Inventário de endpoints.
- Gerenciamento de endpoint.
- Bloqueio de tela automático.
- Criptografia de Storage.
- Prevenção e Detecção de Anti-malware.
- DLP.



Conclusão

- ✓ Existem frameworks e documentos para auxiliar na definição dos controles que devem ser realizados na cloud, como o [Cloud Controls Matrix version 4.0](#) da Cloud Security Alliance que foram a referência para a produção deste módulo.
- ✓ A responsabilidade pelos controles variam dependendo do tipo de serviço (IaaS, PaaS, SaaS).



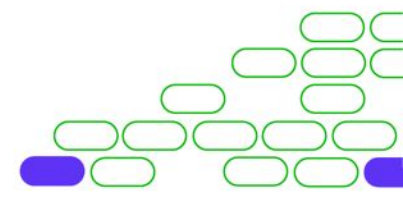
Próxima aula

01.

SIEM.

02.

Web Application Firewall.





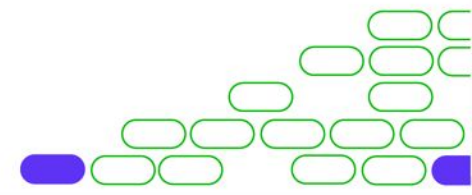
Faculdade



Segurança de Infraestrutura Cloud

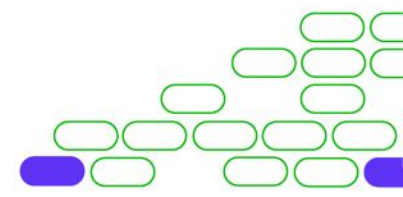
AULA 4.3. CLOUD SIEM E WEB APPLICATION FIREWALL

PROF. MACGAYVER MARQUES



Nesta Aula

- ❑ SIEM.
- ❑ Web Application Firewall.



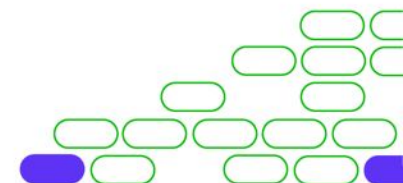
O que é um cloud-based SIEM?

- As soluções de gerenciamento de eventos e informações de segurança (SIEM) oferecem às empresas a capacidade de coletar, armazenar e analisar informações de segurança de toda a organização e alertar administradores de TI / equipes de segurança sobre possíveis ataques.
- O SIEM baseado em nuvem (também conhecido como SIEM-as-a-Service), leva o SIEM para o próximo nível, fornecendo às equipes de TI maior conveniência, flexibilidade e poder ao gerenciar ameaças em vários ambientes - tanto no local quanto no nuvem.

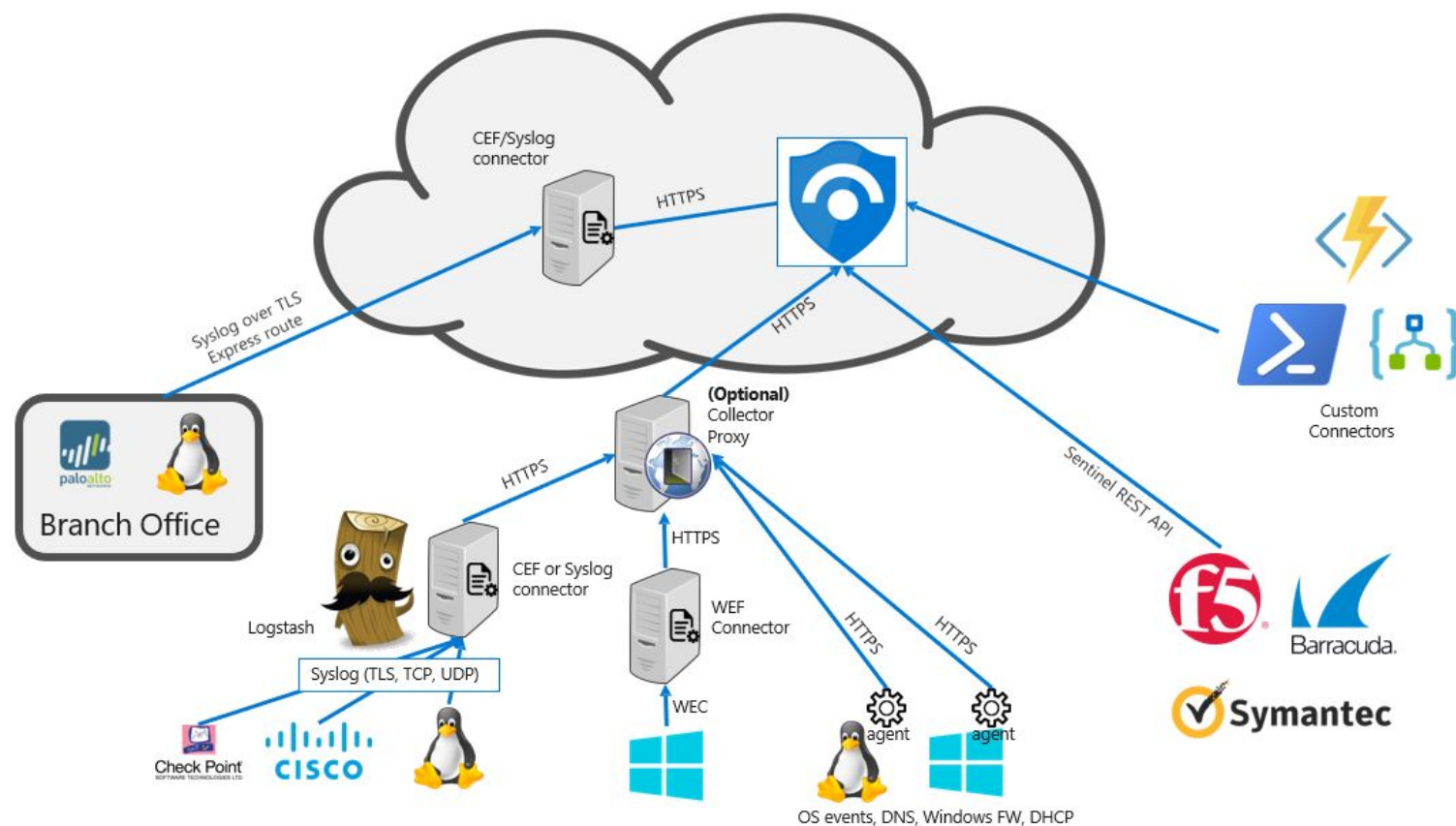


Vantagens de um cloud-based SIEM em relação a on-premises

- Não há a necessidade de compra de hardware
- Elástico
- Escalável
- Rápido
- Fácil de configurar
- Pay as you go
- Possibilidade de automação de respostas a incidentes
- Utilização de inteligência artificial

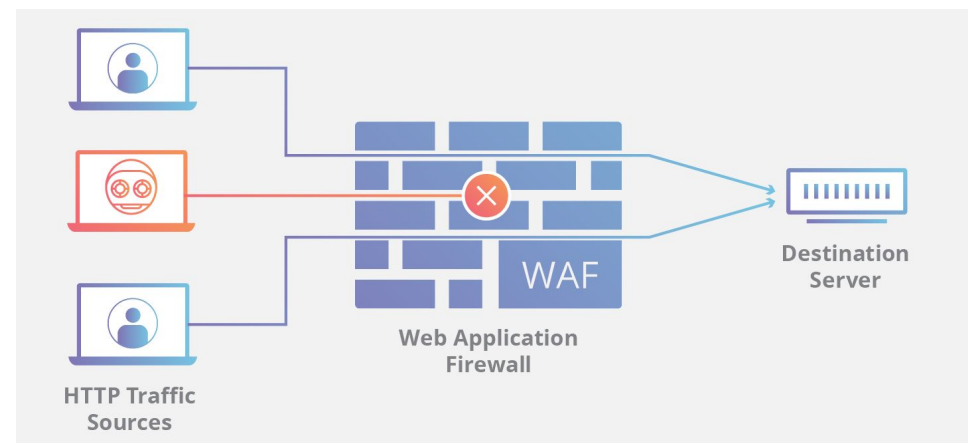


Exemplo de arquitetura SIEM



Web Application Firewall

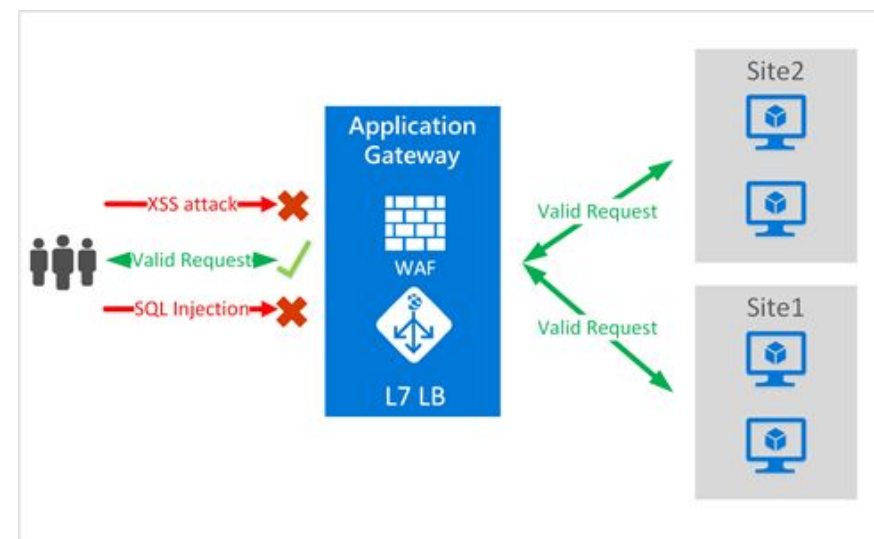
- Um Web Application Firewall (WAF) fornece segurança ao operar por meio de um **aplicativo ou serviço**, bloqueando chamadas de serviço, entradas e saídas que não atendem à política de um firewall, ou seja, conjunto de regras para uma conversa HTTP. WAFs não requerem modificação do código-fonte do aplicativo.
- Atua na camada 7 da OSI.



Proteções do Web Application

Firewall

- Roubo de identidades
- Acesso a informações confidenciais
- SQL Injection
- Cross site scripting (XSS)
- Ataques comuns, como injeção de comando, contrabando de solicitação HTTP, divisão de resposta HTTP e ataque de inclusão remota de arquivo
- Violações de protocolo HTTP
- Anomalias de protocolo HTTP
- Bots, crawlers e scanners
- Configurações incorretas de aplicativos comuns (por exemplo, Apache, IIS, etc.)
- Negação de serviço HTTP



Vantagens de um cloud-based Web Application Firewall

- Elástico
- Escalável
- Rápido
- Fácil de configurar
- Pay as you go



AWS WAF



Conclusão

- ✓ SIEM é um sistema que auxilia os times de segurança a centralizar os eventos de segurança, correlacionando-os e gerando incidentes.
- ✓ É de suma importância que as organizações utilizem um WAF para proteger suas aplicações de ataques comuns a aplicações.





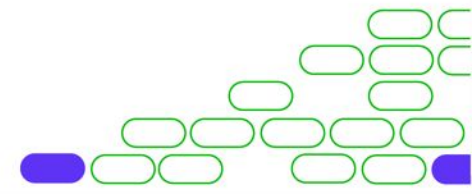
Faculdade



Segurança de Infraestrutura Cloud

CAPÍTULO 5. CONTINGÊNCIA E CONTINUIDADE CLOUD

PROF. MACGAYVER MARQUES





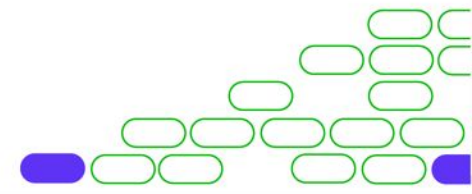
Faculdade



Segurança de Infraestrutura Cloud

AULA 5.1. PLANO DE CONTINGÊNCIA E DISASTER RECOVERY

PROF. MACGAYVER MARQUES



Nesta Aula

- ☐ Disaster Recovery (DR).
- ☐ Continuidade de Negócios (BC).

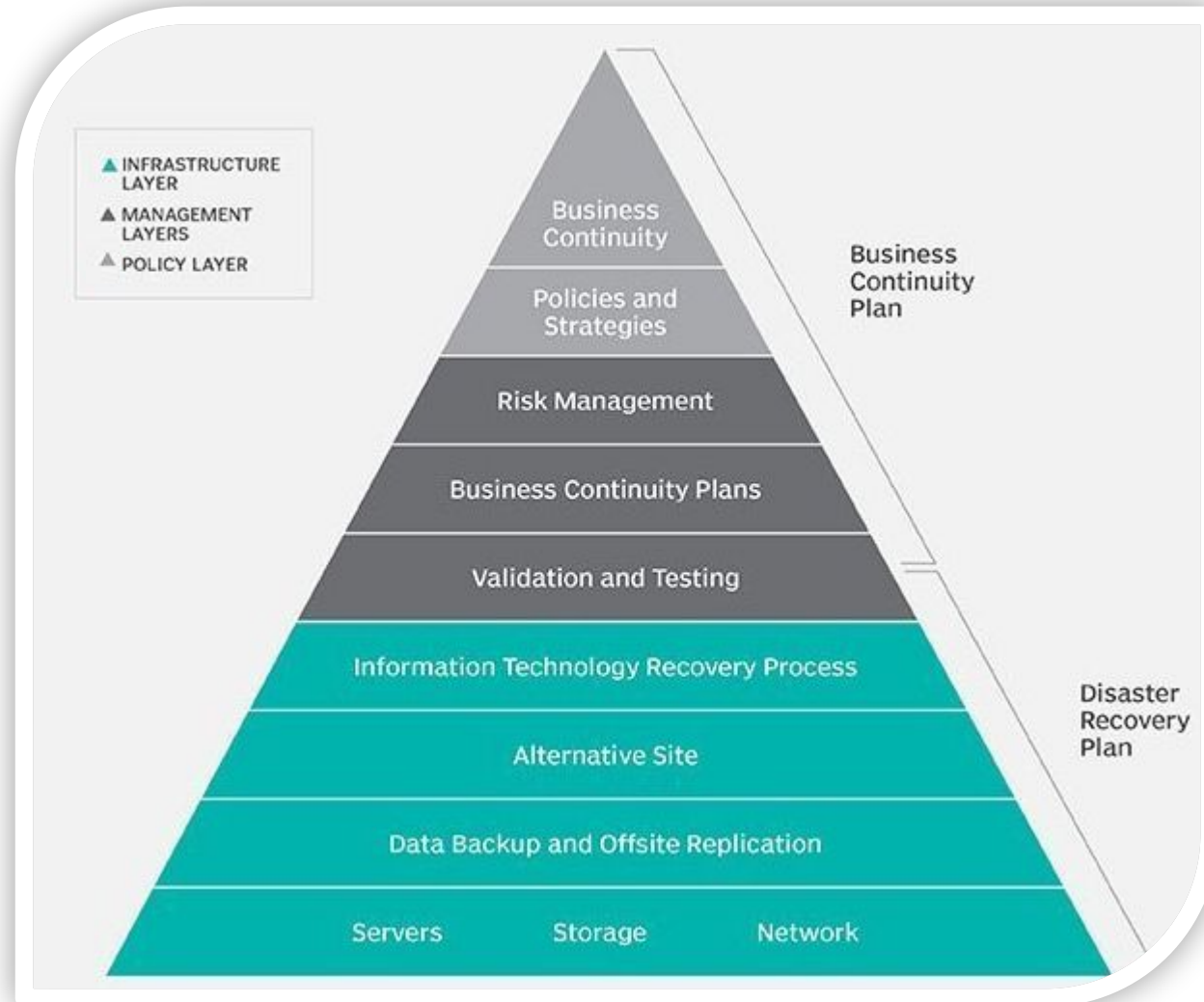


O que é Continuidade de Negócios e Disaster Recovery?

Continuidade de negócios e Disaster Recovery (BCDR ou BC / DR) é **um conjunto de processos e técnicas** usados para ajudar uma organização **a se recuperar de um desastre e continuar ou retomar** as operações de negócios de rotina. É um termo amplo que combina as funções e funções de TI e negócios após um desastre.



BC / DR



Principais aspectos de BC/DR na cloud

1

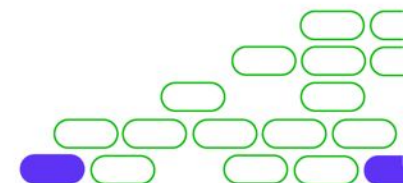
Garantir a continuidade e recuperação em um determinado provedor de cloud.

2

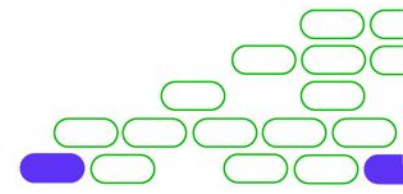
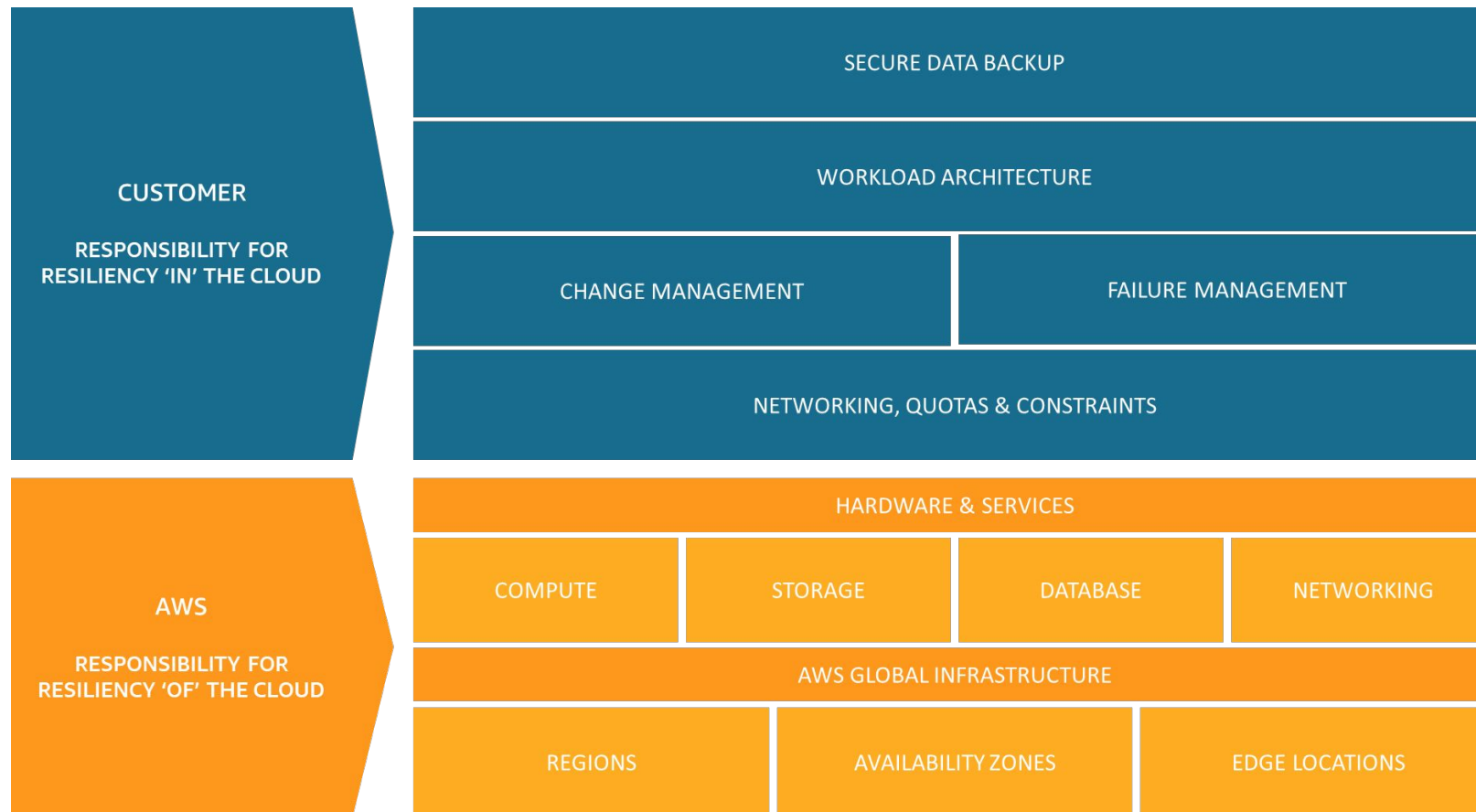
Preparação e gerenciamento de interrupções no provedor de cloud.

3

Considerar opções de portabilidade, caso precise migrar provedores ou plataformas.



Modelo de responsabilidade compartilhada para resiliência na cloud AWS



Por que eu preciso de planejar BC/DR na cloud?

1

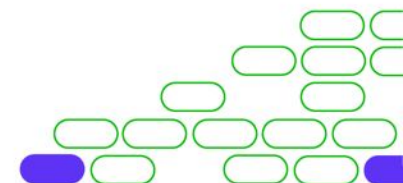
Proteger os dados do cliente.

2

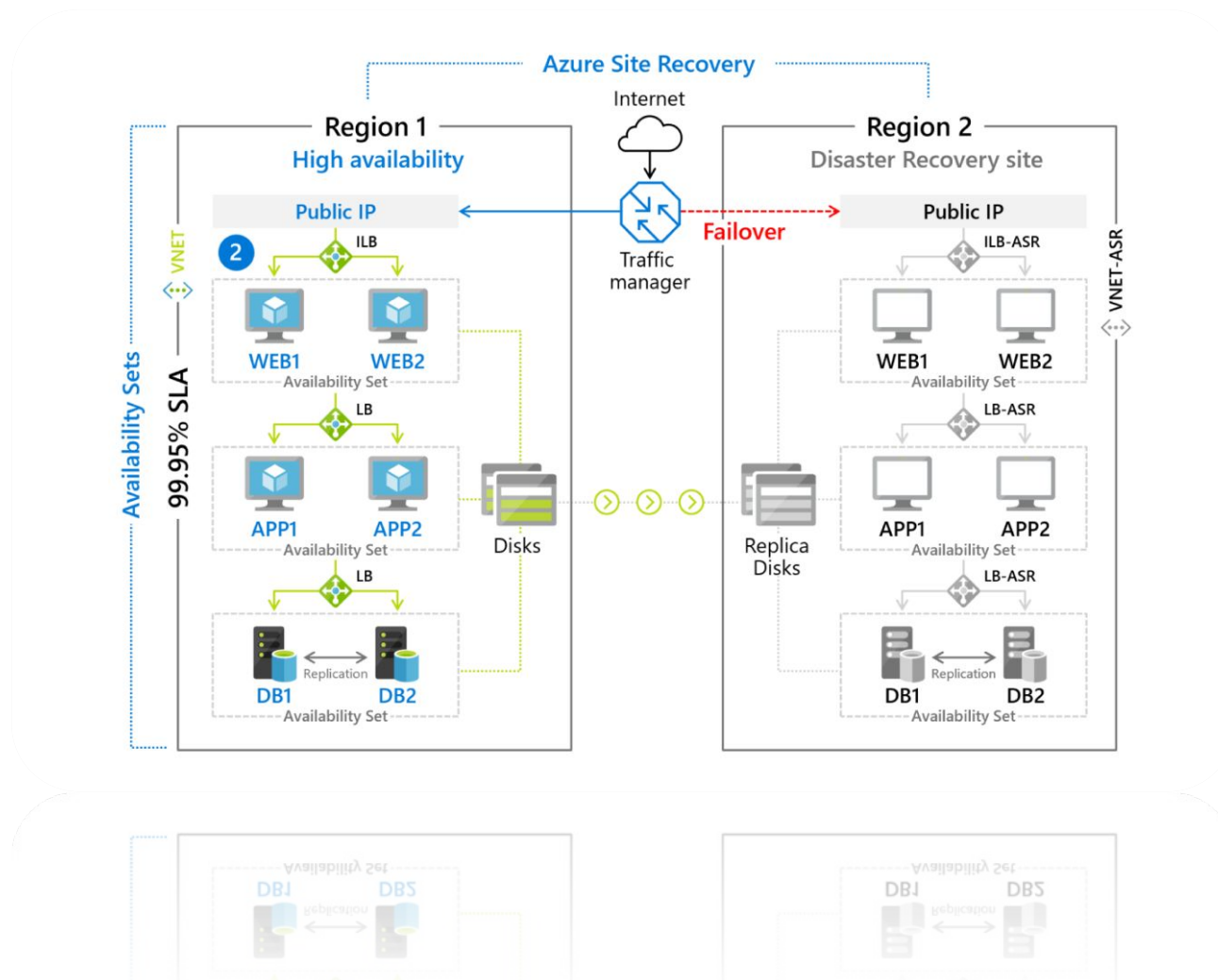
Limitar downtime e acelerar a recuperação e disponibilidade.

3

Proteger a reputação da organização.



Exemplo de arquitetura de DR



Conclusão

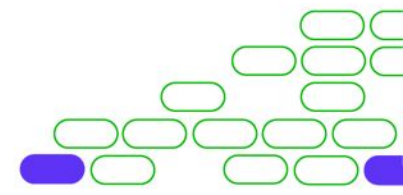
- ✓ Disaster recovery é uma parte do Plano de Continuidade de Negócios.
- ✓ **Ambientes críticos** que precisam de uma **disponibilidade alta** precisam de um ambiente de DR.
- ✓ A resiliência na cloud possui responsabilidade compartilhada entre o provedor e o cliente.



Próxima aula

01.

Backup na Cloud.





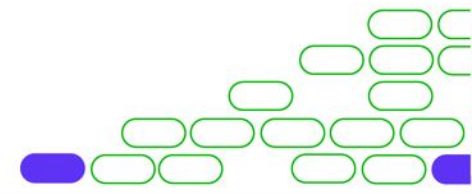
Faculdade



Segurança de Infraestrutura Cloud

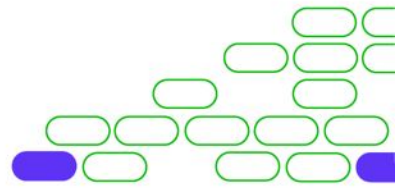
AULA 5.2. BACKUP NA NUVEM

PROF. MACGAYVER MARQUES



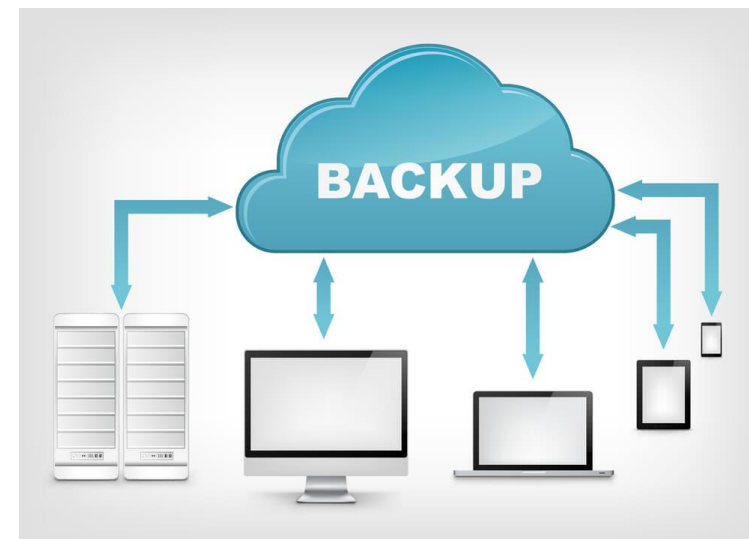
Nesta Aula

- ❑ Backup na Cloud.



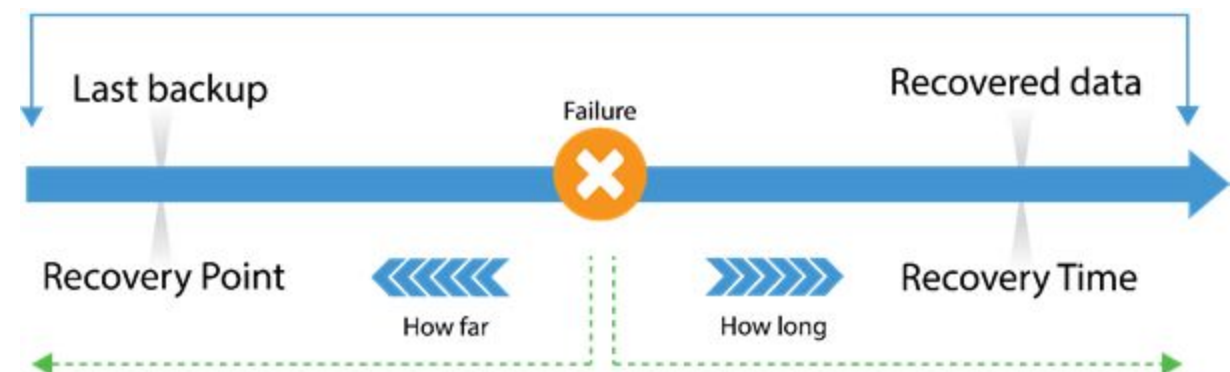
O que é Backup?

Backup é uma cópia de segurança dos seus dados (informações) de um dispositivo de armazenamento ou sistema para outro ambiente para que esses mesmos dados possam ser restaurados em caso de perda dos dados originais ou que ocorra um acidente.



RTO vs RPO

- O Recovery Point Objective (RPO) é a quantidade de dados que você poderia perder se um servidor falhasse. Por exemplo, se você fizer backup de seu servidor uma vez por noite, seu RPO poderá ser de 24 horas, enquanto se você replicar seu servidor em tempo real, seu RPO poderá ser de segundos.
- O Recovery Time Objective (RTO) está relacionado ao tempo de inatividade e representa quanto tempo leva para restaurar a partir do incidente até que as operações normais estejam disponíveis para os usuários.



O que eu posso fazer backup na cloud?

- Arquivos e máquinas virtuais on premises
- Máquinas virtuais do Azure e AWS
- Discos gerenciados
- File shares
- Bancos de dados SQL, Postgree, MySQL, etc.
- SAP HANA Databases
- Azure Blobs ou AWS Simple Storage Services (S3)



Vantagens do Backup na Cloud

- Economia de dinheiro e recursos
- Proteção de dados em caso de um evento de desastre
- Dados são acessíveis de qualquer lugar
- Melhor segurança de dados
- Proteção contra ciberataques
- Escalabilidade



Conclusão

- ✓ Backup na cloud pode ser mais vantajoso e mais seguro do que o backup on-premises por conta de localizações multi-geográficas e de não ter aporte financeiro em hardware.





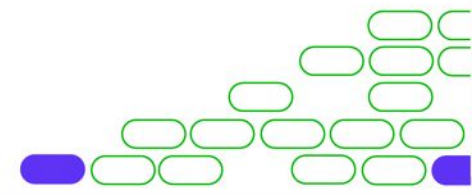
Faculdade



Segurança de Infraestrutura Cloud

CAPÍTULO 6. SEGURANÇA DE DADOS E APLICAÇÕES

PROF. MACGAYVER MARQUES





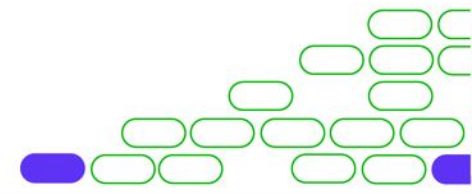
Faculdade



Segurança de Infraestrutura Cloud

AULA 6.1. GOVERNANÇA DA INFORMAÇÃO

PROF. MACGAYVER MARQUES



Nesta Aula

- ☐ O que são Dados?
- ☐ Ciclo de Vida da Segurança de Dados.
- ☐ Localização dos Dados.
- ☐ Acesso.
- ☐ Funções, Atores e Controles.



O que são dados?

Em geral, dados são qualquer conjunto de caracteres que é coletado e traduzido para algum propósito, geralmente análise. Se os dados não forem colocados em contexto, eles não farão nada para um ser humano ou computador.

- Caractere simples
- Boolean (verdadeiro ou falso)
- Texto
- Número
- Foto
- Som
- Vídeo



Descobrir e gerenciar dados é um Desafio



#1

Proteção e governança de dados confidenciais é a maior preocupação para estar em conformidade com regulamentações

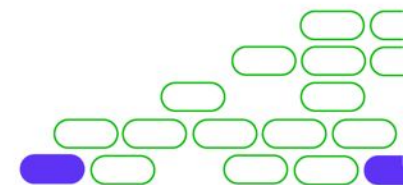
>80%

Dos dados corporativos são “dark” – Não são classificados, protegidos ou gerenciados

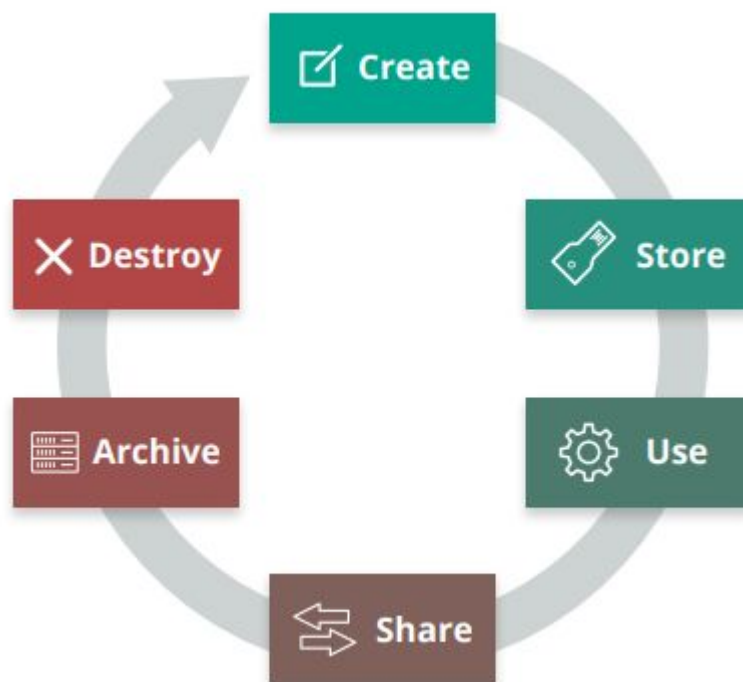
88%

Das organizações não tem maturidade para detectar e prevenir a perda de dados sensíveis

1. Forrester. Security Concerns, Approaches and Technology Adoption. December 2018
2. IBM. Future of Cognitive Computing. November 2015
3. Microsoft GDPR research, 2017



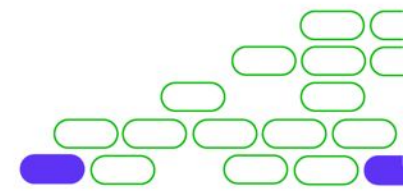
Ciclo de vida dos dados



Localização dos Dados

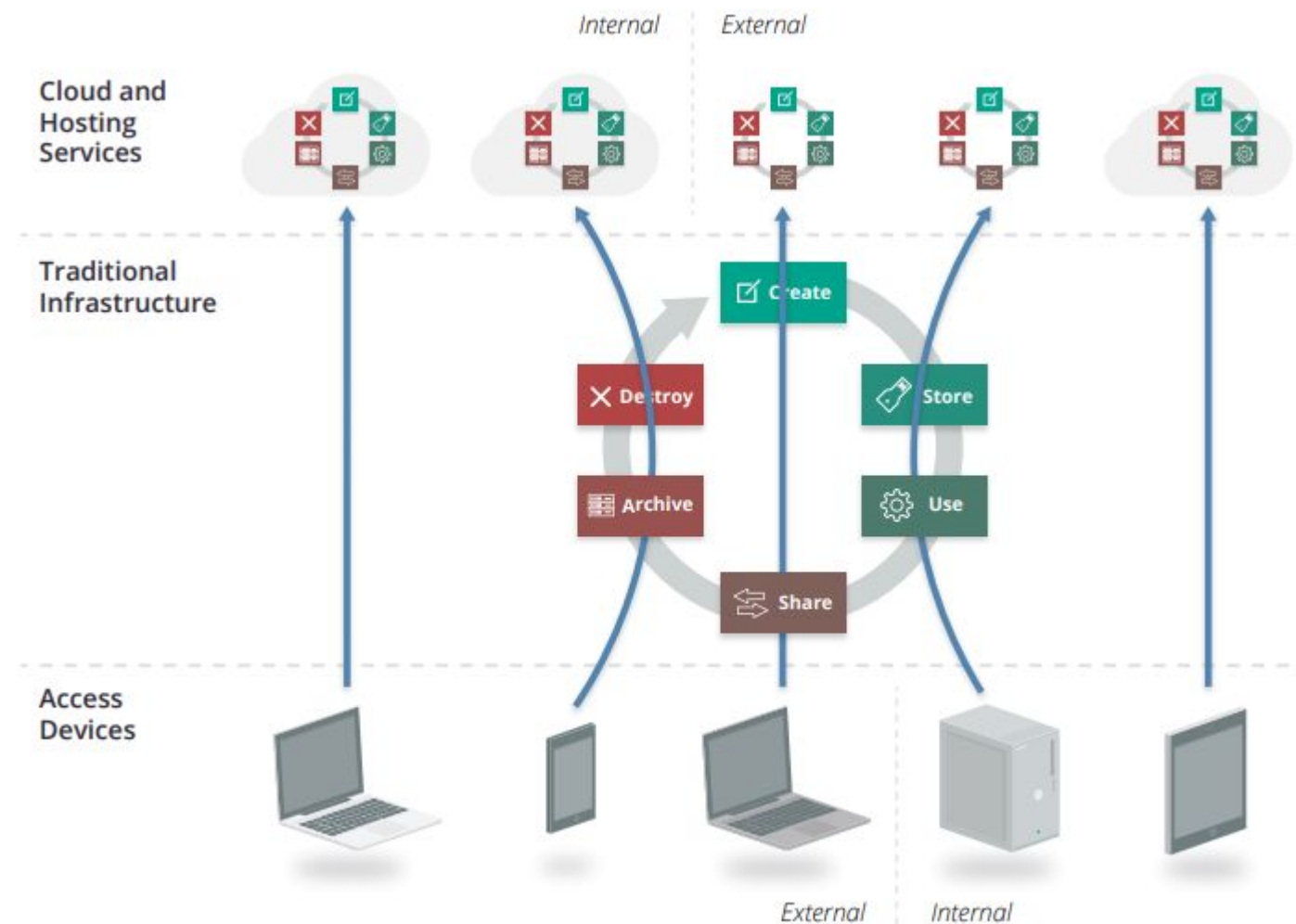
Para segurança de dados há 4 coisas que temos que entender:

1. Onde estão localizados meus dados?
2. Quais os ciclos de vidas e controles em cada uma dessas localizações?
3. Quando os dados podem ser movidos em cada ciclo de vida?
4. Como os dados movem entre as localizações (via quais canais)?

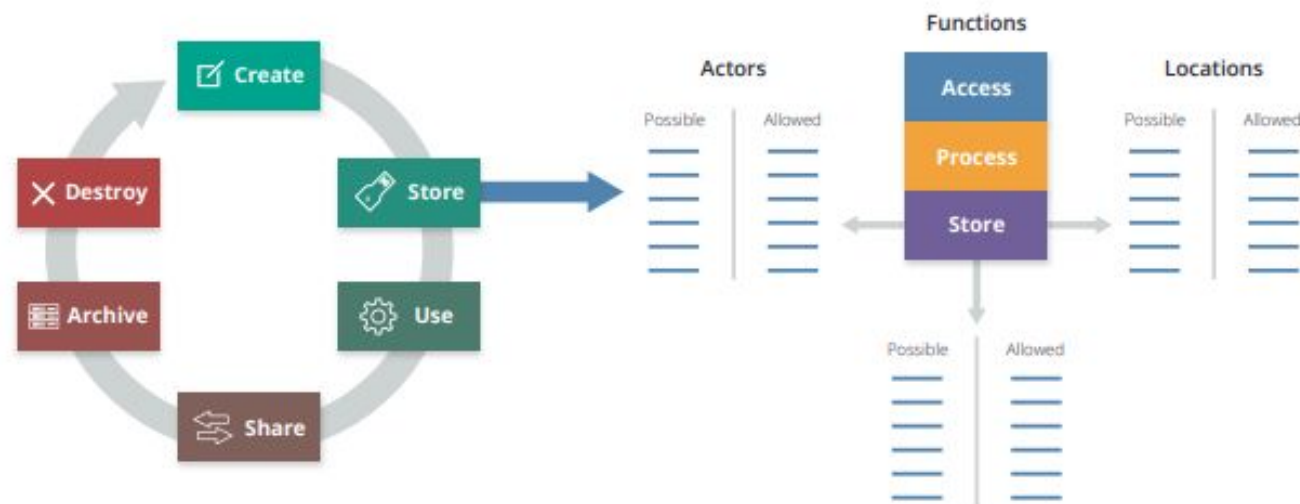


Acesso

- Quem tem acesso aos dados?
- Como eles são acessíveis?

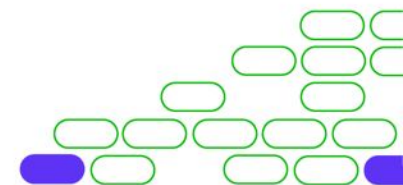


Funções, Atores e Controles





Recomendações



Conclusão

- ✓ A proteção dos dados é fundamental no mundo corporativo.
- ✓ Temos que ter uma estratégia para proteger os dados em todo seu ciclo de vida.
- ✓ O acesso aos dados confidenciais deve ser provisionado com diferentes tipos de perfil.



Próxima Aula

- ☐ Tipos de Storage na Cloud.
- ☐ Criptografia de Dados na Cloud.
- ☐ Cloud Access Security Broker (CASB).
- ☐ Data Loss Prevention (DLP).
- ☐ Fases de Desenvolvimento Seguro.





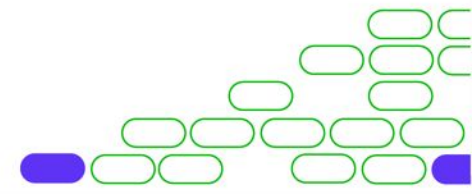
Faculdade



Segurança de Infraestrutura Cloud

AULA 6.2. ARMAZENAMENTO, CRIPTOGRAFIA E PROTEÇÃO DE DADOS NA CLOUD

PROF. MACGAYVER MARQUES



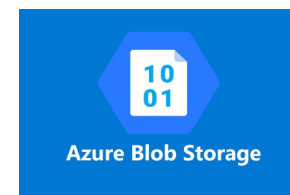
Nesta Aula

- ☐ Tipos de Storage na Cloud.
- ☐ Criptografia de Dados na Cloud.
- ☐ Cloud Access Security Broker (CASB).
- ☐ Data Loss Prevention (DLP).
- ☐ Fases de Desenvolvimento Seguro.



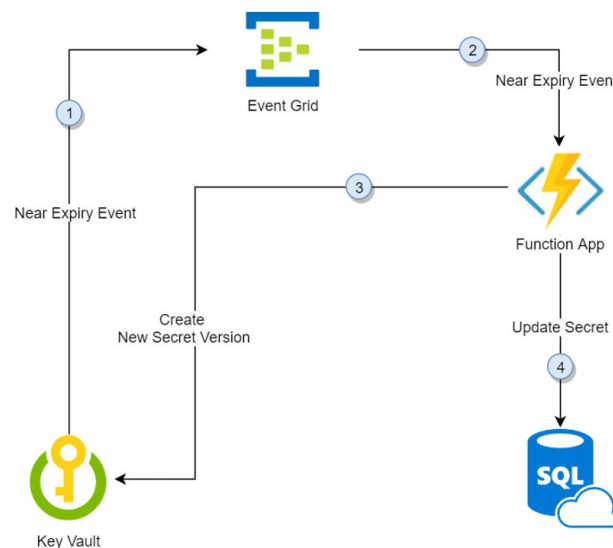
Tipos de Storage na Cloud

- Storage de Objetos: Armazenamento de arquivos
- Storage de Volumes: Discos de VMs
- Bancos de Dados
- Aplicação/Plataforma: CDN, arquivos de SaaS
- Redundância



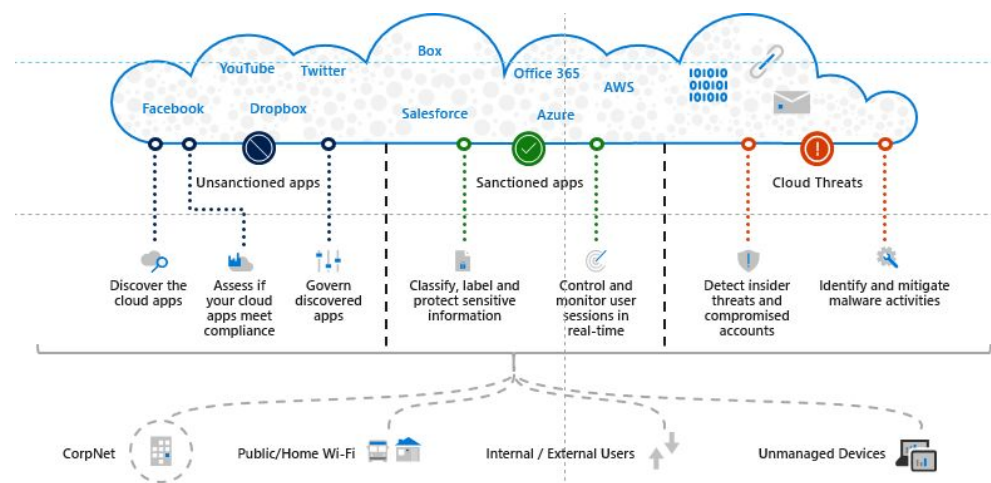
Criptografia de Dados na Cloud

- Criptografia de Storages
- Key Management
 - HSM
 - Appliance virtual
 - KSM, KeyVault
 - Híbrido



Cloud Access Security Broker (CASB)

- Fornece visibilidade avançada, controle sobre tráfego de dados e análises sofisticadas para identificar e combater ameaças cibernéticas em todos os seus serviços de cloud.
- Descubra e controle o uso de Shadow IT.
- Protege informações condidenciais em múltiplas clouds.
- Proteja contra ameaças cibernéticas e anomalias.
- Avalie a conformidade de seus aplicativos na cloud.



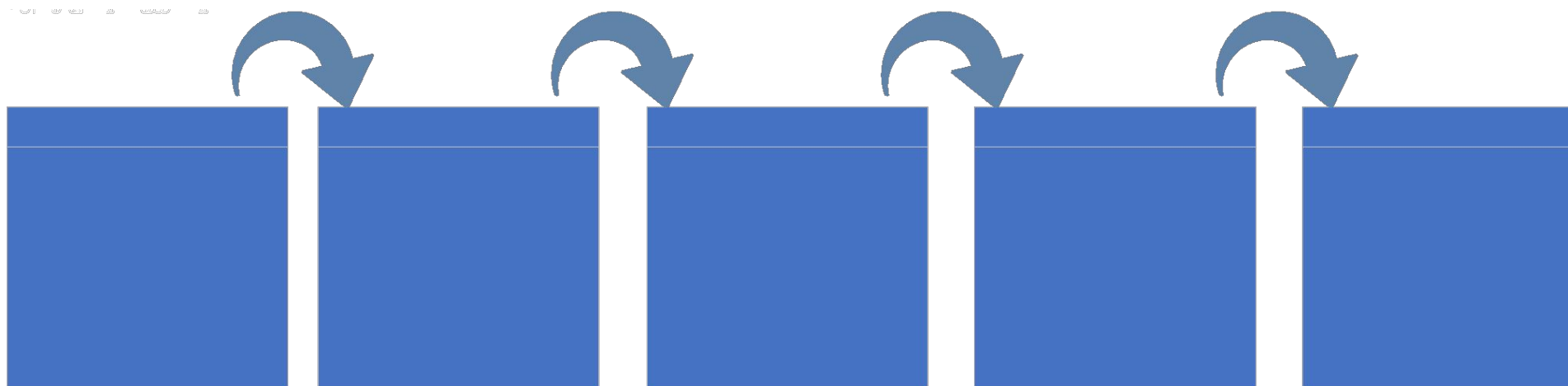
Data Loss Prevention (DLP)

- Identifica, rastreia e protege informações sensíveis em locais de armazenamento em clouds públicas (Dropbox, Office 365, G-Suite, etc.).
- Registra eventos para fins de auditoria.
- Exibir um aviso ou bloqueio para o usuário final que está enviando uma mensagem, um e-mail ou compartilhamento um arquivo.
- Funciona através de políticas/regras.
- Detecta tipos de informações sensíveis
 - Expressões regulares
 - Palavras ou dicionário de palavras
 - Checksum

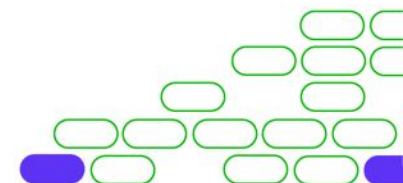
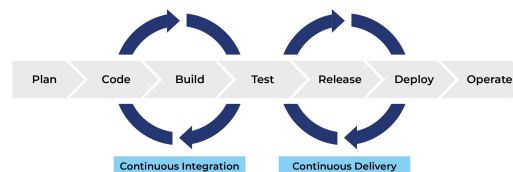


Fases de Desenvolvimento

Seguro



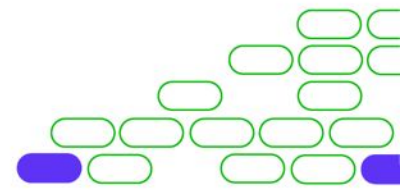
CI/CD



Como a Cloud Impacta no Desenvolvimento e Arquitetura de Aplicações



- Segregação por padrão
- Infraestrutura imutável
- Aumento no uso de microsserviços
- Arquiteturas PaaS e serverless
- Padronização
 - Templates
 - DevOps
- DevSecOps



Conclusão

- ✓ Criptografia de Storage é fundamental para garantir a segurança dos dados.
- ✓ CASB e DLP são tecnologias que auxiliam contra ameaças que buscam vazar informações confidenciais em clouds públicas.
- ✓ DevSecOps auxilia na padronização de desenvolvimento de aplicações seguras.





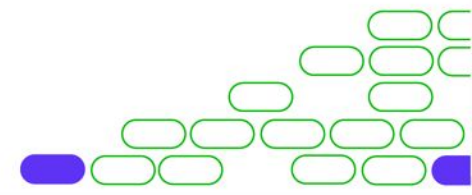
Faculdade



Segurança de Infraestrutura Cloud

CAPÍTULO 7. MELHORES PRÁTICAS DE SEGURANÇA EM CLOUD

PROF. MACGAYVER MARQUES





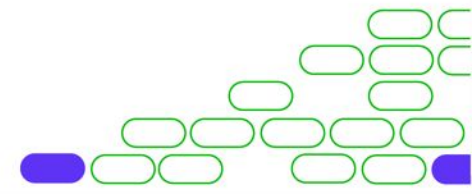
Faculdade



Segurança de Infraestrutura Cloud

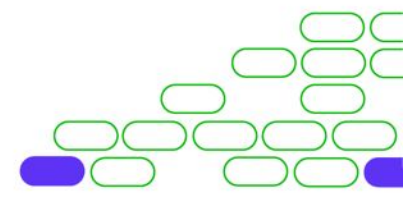
AULA 7.1. MELHORES PRÁTICAS DE SEGURANÇA EM CLOUD

PROF. MACGAYVER MARQUES



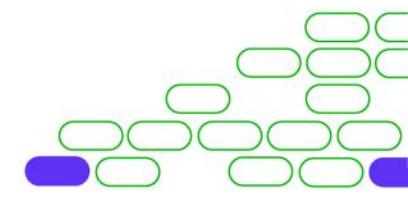
Nesta Aula

- ❑ Melhores práticas para segurança em Cloud.



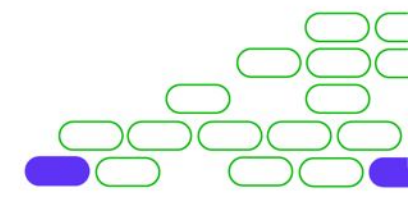
Melhores Práticas para Segurança de Redes

- Segmentar logicamente as sub-redes
 - Não atribuir regras de permissão com intervalos amplos (allow 0.0.0.0 – 255.255.255.255)
 - Segmentar o espaço de endereço maior em sub-redes
 - Criar controle de acesso à rede entre sub-redes
 - Evitar sub-redes virtuais pequenas para garantir simplicidade e flexibilidade
- Adotar uma abordagem de Zero Trust
 - Conceder acesso condicional a recursos com base em dispositivo, identidade, garantia, local de rede, etc.
 - Habilitação de acesso às portas somente após aprovação.
 - Conceder permissões temporárias para executar tarefas privilegiadas, para impedir que usuários mal-intencionados ou não autorizados obtenham acesso após a expiração das permissões.



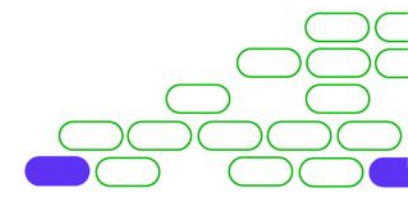
Melhores Práticas para Segurança de Redes

- Usar dispositivos de rede virtual
 - Firewall
 - Gerenciamento de vulnerabilidades
 - Controle de aplicativo
 - Filtragem web
 - Antivírus
 - Proteção contra botnet
- Evitar a exposição à Internet por meio de links WAN dedicados
 - VPN S2S
 - Link dedicado



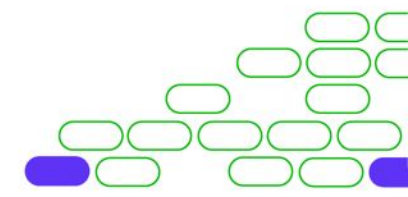
Melhores Práticas para Segurança de Bancos de Dados

- Gerenciamento central de identidades
 - Utilização de roles e grupos específicos para cada servidor ou instância de bancos de dados
- Utilização de acesso condicional com habilitação de MFA
- Minimizar o uso de autenticação com senha para usuários
 - Utilização de SSO
- Proteger senhas com segredos
 - HSM, KeyVault
- Gerenciamento de acesso
 - Aplicar o princípio de privilégios mínimos
 - Utilização de contas distintas em ambientes de testes e prod



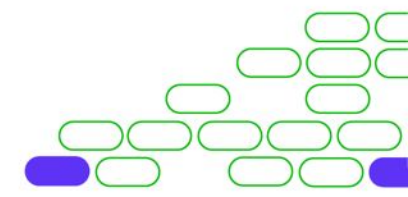
Melhores Práticas para Segurança de Bancos de Dados

- Realizações de revisão de códigos constantes
 - Padronização
 - Vulnerability Assessment
 - Testes
- Proteção de dados
 - Criptografar dados em trânsito
 - Criptografar dados em repouso
 - Habilitar a função Always Encrypted para dados confidenciais
 - Sempre armazenar as chaves de criptografia em um gerenciador de chaves



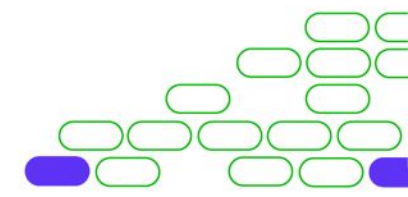
Melhores Práticas para Segurança de Bancos de Dados

- Minimizar a superfície de ataque
 - Link dedicado, VPN
 - Regras de firewall para garantir acesso para IPs autorizados
 - Restrição de acesso à porta 3342
- Proteção contra ataques DDoS
- Monitoramento, registro em log e auditoria
- Auditar eventos de segurança críticos
- Identificar e marcar dados confidenciais
- Acompanhar o acesso aos dados confidenciais
- Utilização de alta-disponibilidade



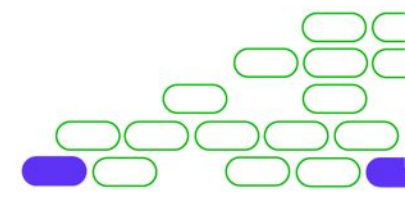
Melhores Práticas para Segurança e Criptografia de Dados

- Proteger dados
 - Em repouso
 - Criptografia de discos e BD
 - Em trânsito
 - VPN S2S e VPN P2S
 - HTTPS
- Definir uma solução de gerenciamento de chaves criptográficas
 - Conceder acesso a usuários, grupos e aplicativos em um escopo específico.
 - Controle o que os usuários têm acesso. (RBAC)
 - Armazenar certificados no cofre de chaves
- Garantir segurança de endpoints que acessarem dados sensíveis
- Proteger e-mails, documentos e dados confidenciais



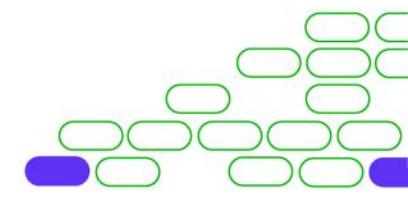
Melhores Práticas Controle de Acesso e IAM

- Tratar identidade como perímetro de segurança primário
- Centralizar o gerenciamento de identidade
- SSO
- Ativar acesso condicional
- Habilitar o gerenciamento de senhas
- MFA
- RBAC
- PIM
- Monitoramento de identidades



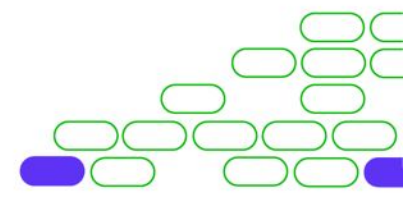
Melhores Práticas Segurança Operacional

- Gerenciar e monitorar senhas de usuários
- Blueprints para automatizar a governança de recursos
- Monitoramento de serviços
- EDR e SIEM
- Monitoramento de rede ponta a ponta
- Proteção contra DDoS
 - Aplicações escaláveis
 - Alta disponibilidade
 - NSG
 - Anti DDoS
- Habilitar Policy



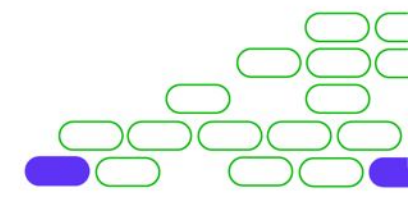
Melhores Práticas Segurança PaaS

- Identidade como perímetro de segurança primário
 - Proteger suas chaves e credenciais para proteger a implantação de PaaS.
 - Não colocar as credenciais e outros segredos no código-fonte nem no GitHub.
 - MFA
 - Utilizar protocolos de segurança padrão OAuth2 e Kerberos
- Instalar um WAF
- Monitorar o desempenho dos aplicativos
- Executar Pentest



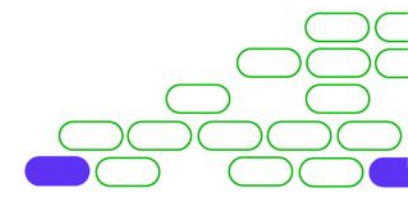
Melhores Práticas para Segurança de Bancos de Dados PaaS

- Utilizar repositório de identidades centralizado
- Restringir o acesso com base no IP
- Criptografar dados em repouso e em trânsito
 - Always Encrypted
- Realização de backups



Melhores Práticas Segurança IaaS

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



Conclusão

- ✓ Existem documentações oficiais de melhores práticas de segurança tanto da AWS quanto do Azure disponíveis publicamente, que seguem diversos frameworks e diretrizes de mercado que devem ser seguidas para que possamos ter um nível elevado de segurança no nosso ambiente cloud.

