

FAi ONLINE

SEGURANÇA EM CLOUD-COMPUTING

Marcelo Zillo

Novas Tecnologias, Transformação Digital e Agilidade

SUMÁRIO

CONHEÇA SUA DISCIPLINA	4
<i>Entenda como funciona a disciplina do curso.</i>	
COM QUEM APRENDEREI?	5
<i>Conheça o professor que ministra a disciplina.</i>	
PRINCIPAIS PONTOS	6
<i>Entenda os principais pontos que podem ser percorridos ao longo da disciplina.</i>	
AULA 1, PARTE 1	7
<i>Introdução ao Cloud Computing.</i>	
AULA 1, PARTE 2	11
<i>Indústrias Transformadas; Tipos de Serviços de Nuvem; Modelos de Nuvem.</i>	
AULA 1, PARTE 3	14
<i>Quadrantes Mágicos do Gartner; Camadas de Cloud Computing; Benefícios e Barreiras dos Serviços de Nuvem.</i>	
AULA 1, PARTE 4	20
<i>Sofa e Plano de Migração; Stage of Adoption.</i>	
AULA 1, PARTE 5	24
<i>Segurança DA x NA Nuvem; Responsabilidade Compartilhada.</i>	

AULA 1, PARTE 6	27
<i>Jornada Segura; Pilares de Segurança.</i>	
CURADORIA	32
<i>Links dos materiais básicos e complementares da disciplina.</i>	
ESTUDO DE CASO	35
<i>Estudo de caso proposto pelo professor.</i>	
GLOSSÁRIO	36
<i>Informações sobre avaliação e canais de contato para dúvidas.</i>	

CONHEÇA SUA DISCIPLINA



O objetivo desta disciplina é o estudo dos sistemas de computação em nuvem de uma maneira ampla e sistêmica, permitindo a contextualização do tema e a identificação de interdependências das questões técnicas e em outros tópicos pertinentes como modelo de negócios e impacto socioeconômico. A disciplina discute ainda a adoção de nuvem do ponto de vista estratégico para a organização e os negócios, de modo a capacitar os gestores a conduzir projetos de migração para computação em nuvem, assim como gerir e implementar os ambientes da empresa nos provedores de computação em nuvem de forma segura e ordenada.



COM QUEM APRENDEREI?



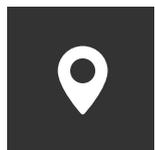
MARCELO ZILLO

CHIEF SECURITY ADVISOR - LATAM NA MICROSOFT. PROFESSOR DE CLOUD- ADOPTION E CLOUD-SECURITY NOS CURSOS MBA E PÓS-GRADUAÇÃO DA FIA

Marcello Zillo é National Security Officer em uma das maiores empresas de Tecnologia do Mundo. Engenheiro da Computação, com formação executiva em Estratégia de Negócios Digitais pelo MIT, MBA Executivo pelo Insper e Pós-graduação em Segurança da Informação pela USP. Atua com Segurança da informação e Segurança de Redes desde 1996, tendo atuado como Senior Manager e Solutions Architecture na maior empresa de serviços de nuvem do mundo, CSO e Head de Operações de Segurança de grandes bancos no Brasil, como Manager em consultoria e fornecedores de tecnologia para cibersegurança.



PRINCIPAIS PONTOS



CHECKPOINT DE APRENDIZAGEM

Assuntos totalmente conectados com a essência da disciplina que requerem a compreensão e atenção do aluno.



CITAÇÃO IMPORTANTE

Destaques acerca dos pontos altos da aula. Atuam como marcos de destaque sobre pontos importantes que, juntos, irão compor um importante mapa da disciplina.



REAL BUSINESS CASE

Case ou situação prática que irá exemplificar a aplicação de conceitos importantes da disciplina em vivência real. Situações problema, reações e impactos, e consequências e soluções.



GRÁFICOS

Gráficos mais relevantes da disciplina com um breve resumo do que foi tratado e que precisa ser destacado.



CONSULTORIA & MENTORIA

Importantes dicas sobre estratégias, aplicações práticas de conceitos apresentados e insights sobre profissões e mercado de trabalho.



VÍDEOS

Exibição de vídeos apresentados durante a aula.



ACESSO RÁPIDO

Links importantes que são apresentados na aula por meio de QR Codes, com uma breve descrição do que contém. Assim, o aluno terá o acesso direto aos sites recomendados.



GUIA DE PALAVRAS

Palavras-chave apresentadas ao longo da aula acompanhadas de sua tradução, significado ou origem.



SUGESTÃO DE LEITURA

Indicações de obras, autores, artigos e sites que irão contribuir para o processo de aprendizagem.

AULA 1, PARTE 1

MARCELO ZILLO



03:11 | CHECKPOINT DE APRENDIZAGEM

INTRODUÇÃO AO CLOUD COMPUTING

Ao falar sobre a adoção de uma nova tecnologia, em especial sobre serviço de nuvem, é muito importante fazer algumas reflexões:

1. O que muda na gestão?
2. Usar a nuvem é seguro?
3. Como migrar?
4. O que migrar?
5. Quais os riscos?
6. Quais os mitos?
7. Isso é somente para startups?
8. Qual o grande desafio para implementar?
9. Quais os benefícios?
10. Qual o papel da nuvem na Transformação Digital?

É cada vez mais comum a fala “subir os arquivos para a nuvem”. Trata-se da computação em nuvem ou cloud computing. Em um momento em que o trabalho e grande parte das atividades são realizados de maneira remota, o termo vem sendo popularizado, reconhecido e adotado por empresas que querem conhecer seus benefícios.

No entanto, a pergunta “é seguro?” ainda é constante entre os novos adeptos. É por isso que existe uma área de cloud computing totalmente dedicada aos requisitos, às práticas e às estruturas de segurança na nuvem: a cloud security. Proteção de dados, infraestrutura, programas envolvidos, principais preocupações com segurança de alto nível e muitos outros temas respondem as dúvidas sobre segurança nesse novo ambiente de computação.

A partir de agora, você vai se aprofundar nas bases que demonstram o quanto as aplicações em nuvem são fundamentais para a transformação digital. Também verá exemplos práticos, de empresas que adotaram esses sistemas com o objetivo de garantir um ambiente digital confiável e seguro.



NUVEM

A capacidade de provisionar recursos tecnológicos que envolvem armazenamento de dados, servidores, capacidade computacional, processamento, conectividade de rede e, principalmente, serviços como bancos de dados, inteligência artificial, conectividade de dispositivos, internet das coisas e muitas outras aplicações.

Existem três tipos de serviços de conexão de nuvem:



- **Nuvem híbrida** combina nuvens públicas e privadas ligadas por uma tecnologia que permite que dados e aplicativos sejam compartilhados entre elas.
- **Nuvem pública** pertence a um provedor de serviço de nuvem terceirizado e é administrada por ele. Fornece recursos de computação (ex.: servidores e armazenamento) pela internet.
- **Nuvem privada** é aquela em que os serviços e a infraestrutura são mantidos em uma rede privada.



21:03 | CONSULTORIA & MENTORIA

“À medida que você adota serviços de tecnologia, como serviços de nuvem, você tem o recurso tecnológico na pontas dos dedos.”



22:10 | GUIA DE PALAVRAS

FAIL FAST

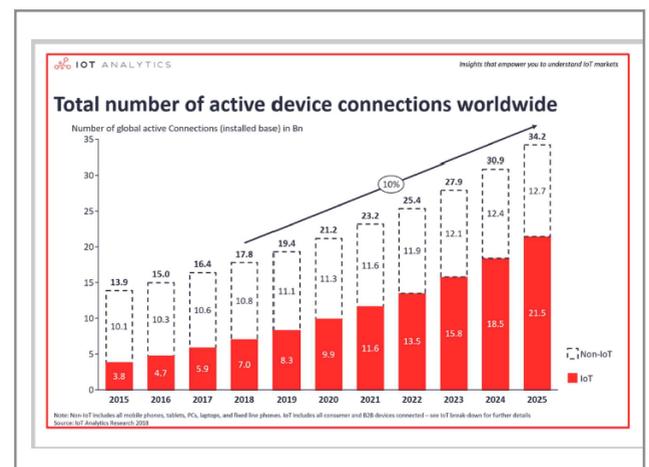
Filosofia que valoriza a constante experimentação dos projetos em busca de ideias que possuam valor real. O principal foco desse conceito é a diminuição da perda de investimento financeiro e de tempo, uma vez que se detecta rápido os pontos que podem levar ao fracasso e se inicia uma nova bateria de ideias.



25:15 | GRÁFICOS

IOT DEVICES

Este gráfico mostra que no ano de 2021 teremos a mesma quantidade de dispositivos móveis (tradicionais) e dispositivo IoT. Ao observar a previsão para 2025, é possível identificar que haverá muito mais dispositivos IoTs conectados do que dispositivos tradicionais.





28:29 | CONSULTORIA & MENTORIA

“IoT é uma realidade que impulsiona, sem dúvida, o uso de nuvem para diversas verticais em empresas diferentes.”



AULA 1, PARTE 2

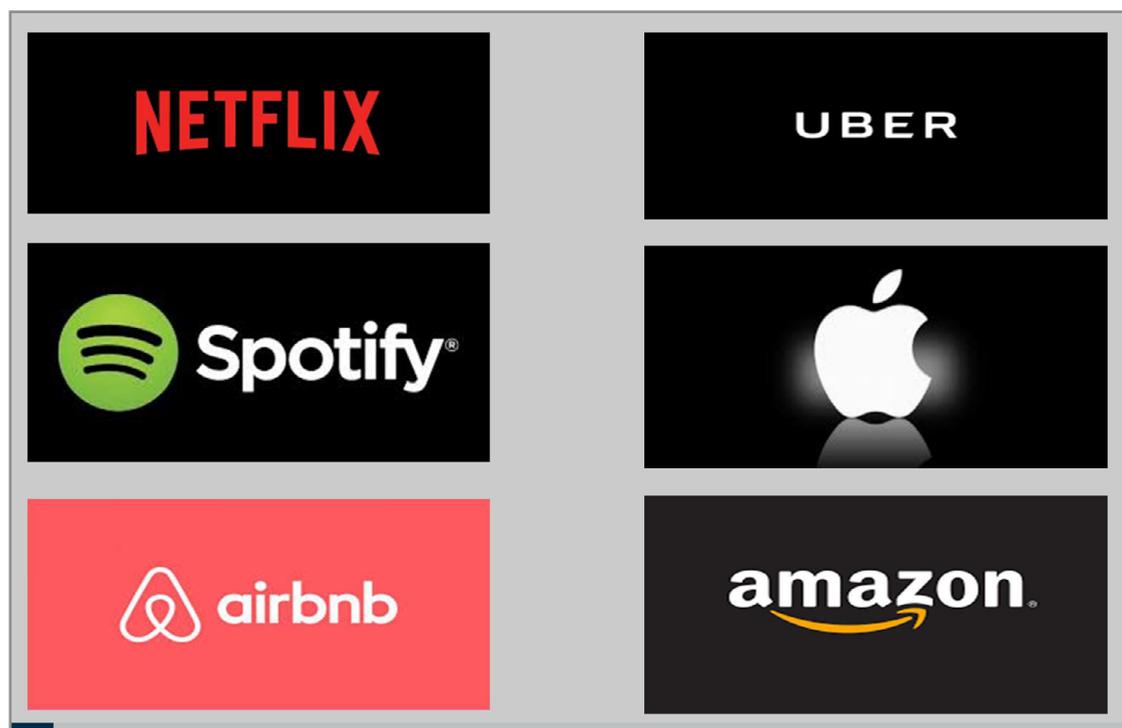
MARCELO ZILLO



00:01 | CHECKPOINT DE APRENDIZAGEM

INDÚSTRIAS TRANSFORMADAS

Conheça alguns exemplos de empresas que se transformaram com base nas inovações da computação em nuvem:



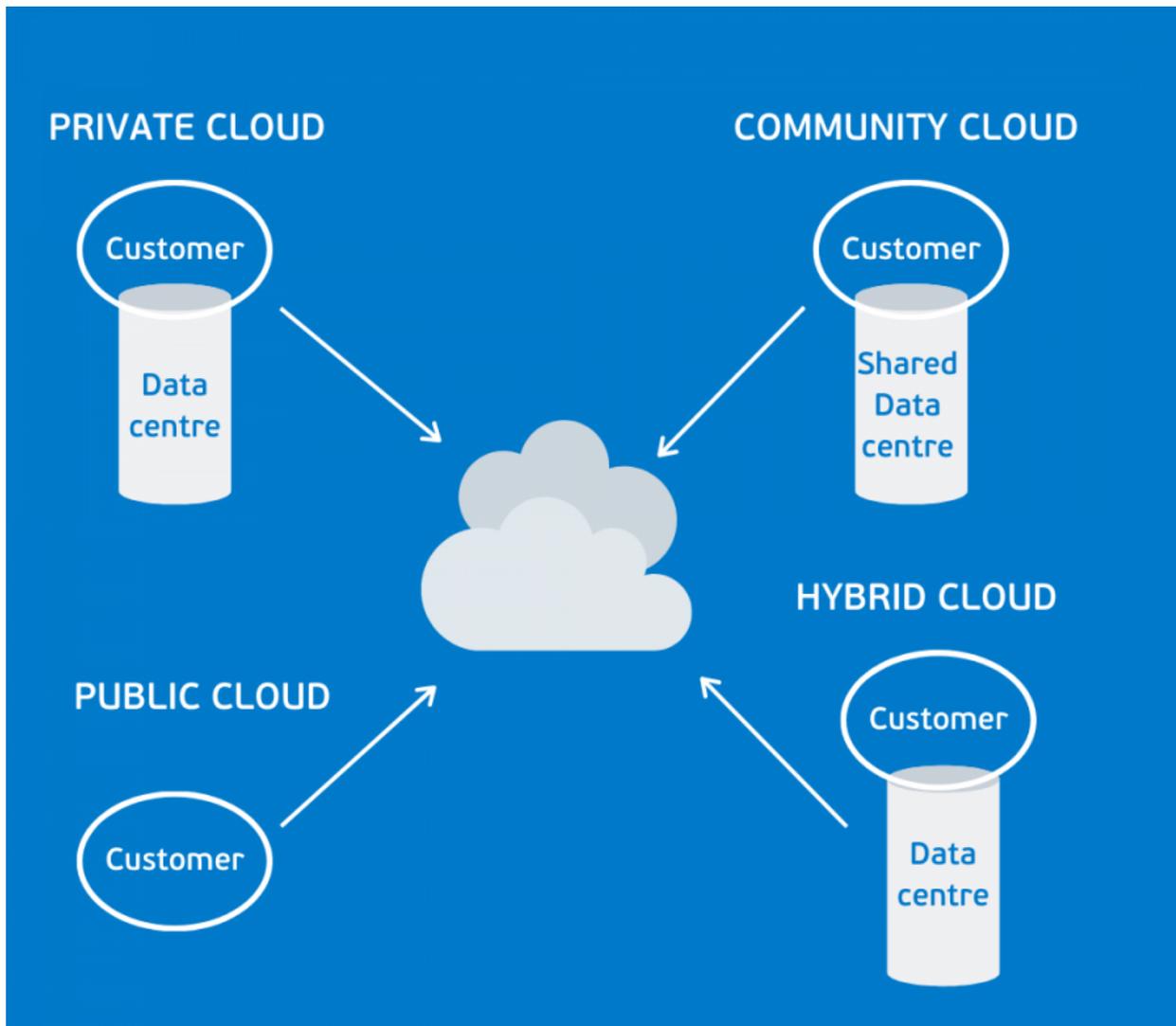
Essas empresas se beneficiaram da nuvem para criar um modelo pequeno, testar, falhar, gerar novas interações, disponibilizar o seu aplicativo, entender os seus usuários por meio dos acessos, gerar inteligência com o machine learning, replicar esse modelo, crescer globalmente e receber pelo uso.



TIPOS DE SERVIÇOS DE NUVEM

Empresas como Airbnb, Uber, Amazon, entre outras empresas nativas digitais, usam nuvem pública, que nada mais é do que recursos de hardware, facilities, software e pessoas que são de propriedade e gerenciados pelo *vendor*, cobrados no modelo de Pay as you Go.

Existem quatro tipos de serviços de conexão de nuvem:



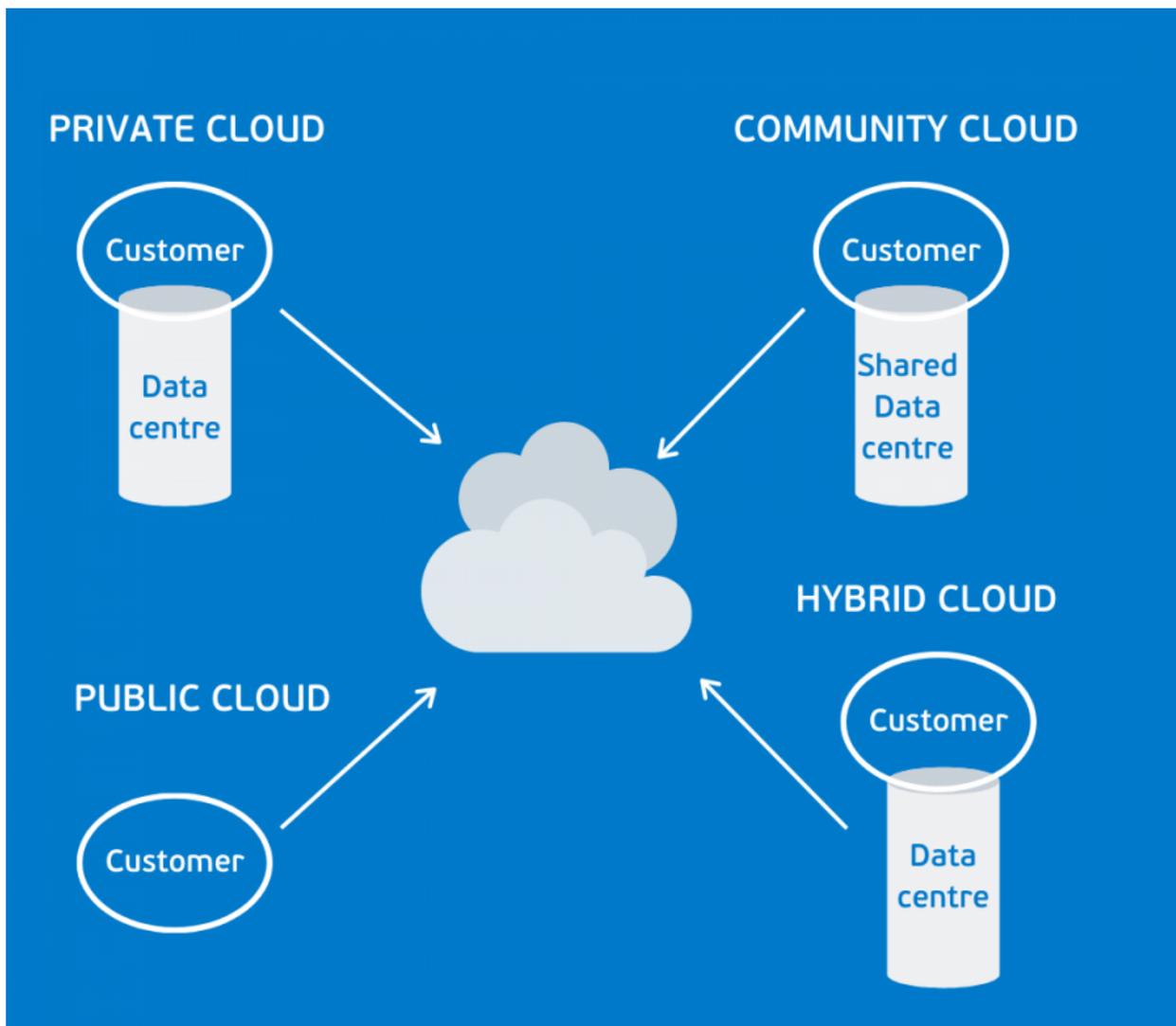
- **Nuvem híbrida** combina nuvens públicas e privadas ligadas por uma tecnologia que permite que dados e aplicativos sejam compartilhados entre elas.
- **Nuvem pública** pertence a um provedor de serviço de nuvem terceirizado e é administrada por ele. Fornece recursos de computação (ex.: servidores e armazenamento) pela internet.
- **Nuvem privada** é aquela em que os serviços e a infraestrutura são mantidos em uma rede privada.
- **Nuvem compartilhada** é destinada para as empresas que precisam compartilhar a infraestrutura entre um grupo específico de usuários com interesses em comum.



MODELOS DE NUVEM

Agora que você já conheceu os modelos de nuvem, entenda mais a respeito do mercado e dos modelos de serviços que podem ser adotados, principalmente, em nuvens públicas, que podem ser classificados da seguinte forma:

- **SaaS (Software como Serviço)** - Tudo é disponibilizado na nuvem, para ter acesso ao serviço pelo browser ou por um software.
- **PaaS (Plataforma como Serviço)** - Contrata-se um ambiente completo de desenvolvimento (porta, usuário, senha e plataforma) no qual é possível criar, modificar e otimizar softwares e aplicações.
- **IaaS (Infraestrutura como Serviço)** - Utiliza-se o provedor de serviços para ter acesso a uma capacidade de hardware que corresponde à memória, ao armazenamento, ao processamento etc.
- **FaaS (Função como Serviço)** - Permite que desenvolvedores criem e executem aplicativos e recursos sem a necessidade de construir ou manterem uma infraestrutura complexa.



AULA 1, PARTE 3

MARCELO ZILLO

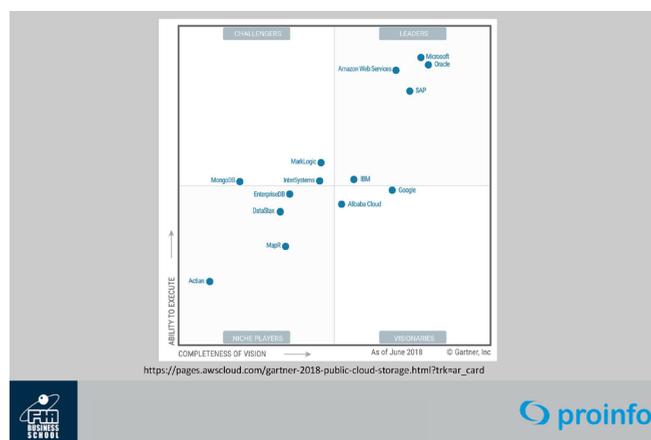


00:01 | CHECKPOINT DE APRENDIZAGEM

QUADRANTES MÁGICOS DO GARTNER

O empreendedor Gideon Gartner criou o Gartner Group, em 1970, focando em criação de conhecimento para auxiliar a tomada de decisão de seus mais de 10 mil clientes.

O Quadrante Mágico, criado por ele, é uma representação gráfica do mercado de TI, de acordo com a força de cada companhia em seu segmento na área tecnológica. Os gráficos de Gartner fornecem uma representação gráfica para ajudar a mensurar os pontos fortes e a melhorar nos principais players de mercado para auxiliar a decidir pelo melhor banco de dados. Veja alguns exemplos:





03:28 | CHECKPOINT DE APRENDIZAGEM

CAMADAS DE CLOUD COMPUTING

Para entender como os serviços estão sendo distribuídos dentro de cada um dos provedores de cloud, veja por exemplo, como a Microsoft Azure e Amazon Web Services (AWS) classificam os seus serviços:

Public Cloud Services – Microsoft Azure

32

The screenshot displays the Microsoft Azure service catalog, organized into several main sections:

- Platform Services:**
 - Security & Management:** Portal, Active Directory, Multi-Factor Authentication, Automation, Key Vault, Store / Marketplace, VM Image Gallery & VM Depot.
 - Compute:** Cloud Services, Service Fabric, Batch, Remote App.
 - Web and Mobile:** Web Apps, API Apps, API Management, Mobile Apps, Logic Apps, Notification Hubs.
 - Developer Services:** Visual Studio, Azure SDK, Team Project, Application Insights.
 - Hybrid Operations:** Azure AD Connect, Health, AD Privileged Identity Management, Backup, Operational Insights, Import/Export, Site Recovery, StorSimple.
 - Integration:** Storage Queues, Biztalk Services, Hybrid Connections, Service Bus.
 - Analytics & IoT:** HDInsight, Machine Learning, Data Factory, Event Hubs, Stream Analytics, Mobile Engagement.
 - Data:** SQL Database, SQL Data Warehouse, Redis Cache, Search, DocumentDB, Tables.
 - Media & CDN:** Media Services, Content Delivery Network (CDN).
- Infrastructure Services:**
 - Compute:** Virtual Machines, Containers.
 - Storage:** BLOB Storage, Azure Files, Premium Storage.
 - Networking:** Virtual Network, Load Balancer, DNS, Express Route, Traffic Manager, VPN Gateway, Application Gateway.
- Datacenter Infrastructure (24 Regions, 19 Online):** A row of server rack icons representing global availability.

Logos for FIA BUSINESS SCHOOL and proinfo are visible at the bottom.

Public Cloud Services - AWS

33

The screenshot displays the Amazon Web Services (AWS) service catalog, organized into several main sections:

- MARKETPLACE:** Business Apps, Business Intelligence, DevOps Tools, Security, Networking, Databases, Storage.
- ANALYTICS:** Data Warehouse, Hadoop/Spark, Real-time Streaming Data, Machine Learning, Elastic Search.
- APP SERVICES:** Queuing & Notifications, Workflow, Search, Email, Transcoding.
- MOBILE SERVICES:** API Gateway, Identity, Sync, Mobile Analytics, Push Notifications.
- DEVELOPMENT & OPERATIONS:** One-click App Deployment, DevOps Resource Management, Application Lifecycle Management, Containers, Triggers, Resource Templates.
- ENTERPRISE APPS:** Virtual Desktops, Sharing & Collaboration, Corporate Email, Backup.
- SECURITY & COMPLIANCE:** Identity Management, Access Control, Key Management & Storage, Monitoring & Logs, Configuration Compliance, Resource & Usage Auditing.
- CORE SERVICES:** Compute (VMs, Auto-scaling & Load Balancing), Storage (Object, Block, & Archive), CDN, Databases (Relational, NoSQL, Caching), Networking (VPC, DX, DNS).
- INFRASTRUCTURE:** Regions, Availability Zones, Points of Presence.

Logos for FIA BUSINESS SCHOOL and proinfo are visible at the bottom.

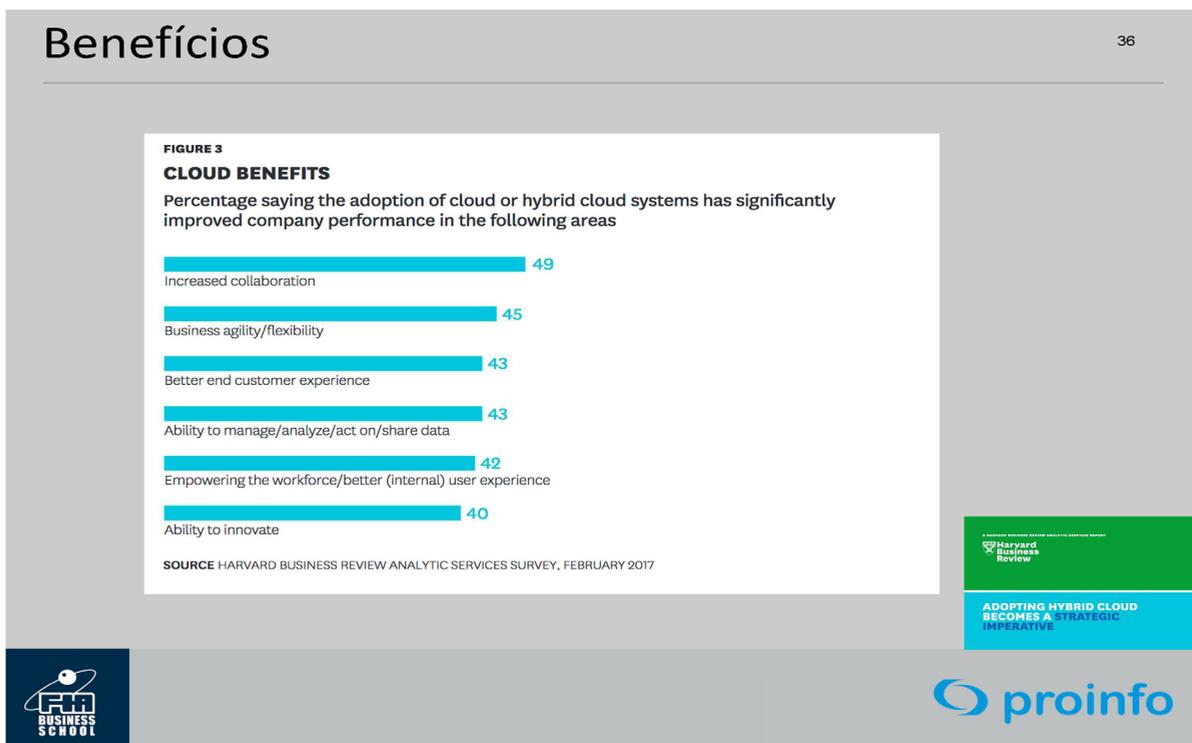
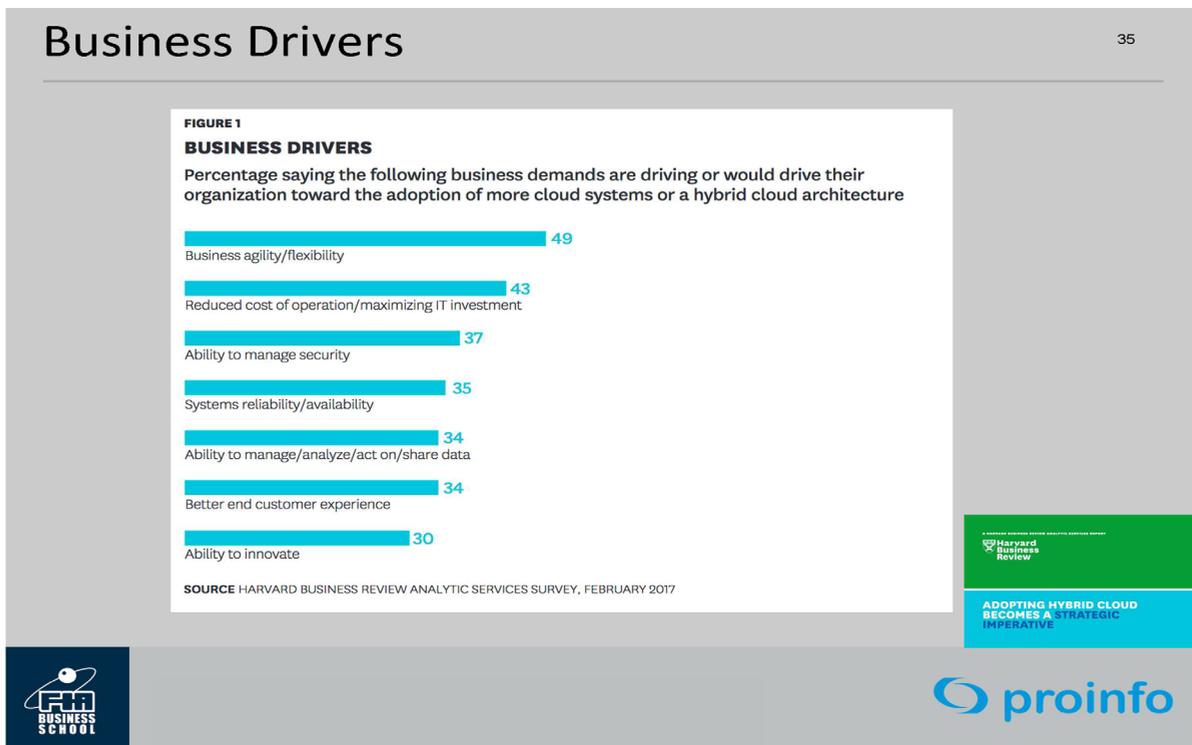


Artigo - Adopting Hybrid Cloud Becomes a Strategic Imperative



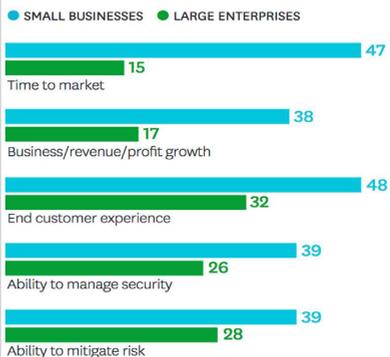
BENEFÍCIOS E BARREIRAS DOS SERVIÇOS DE NUVEM

O relatório de Harvard Business Review Analytic Service de 2017 aponta quais são os principais drivers de adoção de nuvens por parte das empresas, bem como os seus benefícios, barreiras e eficiência relacionada ao custo, sobretudo, quando se trata de nuvem pública:



INCREASED CLOUD BENEFITS FOR SMBs

Percentage of SMB and large-enterprise respondents who say the adoption of cloud/hybrid cloud systems has significantly improved company performance in the following areas



SOURCE HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, FEBRUARY 2017

Harvard Business Review

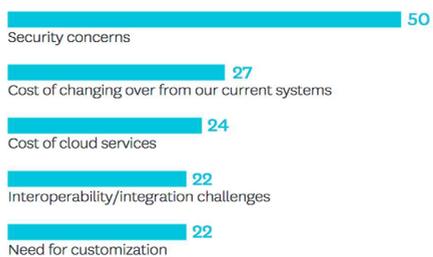
ADOPTING HYBRID CLOUD BECOMES A STRATEGIC IMPERATIVE



FIGURE 7

CLOUD BARRIERS

Percentage citing the following as barriers to fully embracing cloud systems

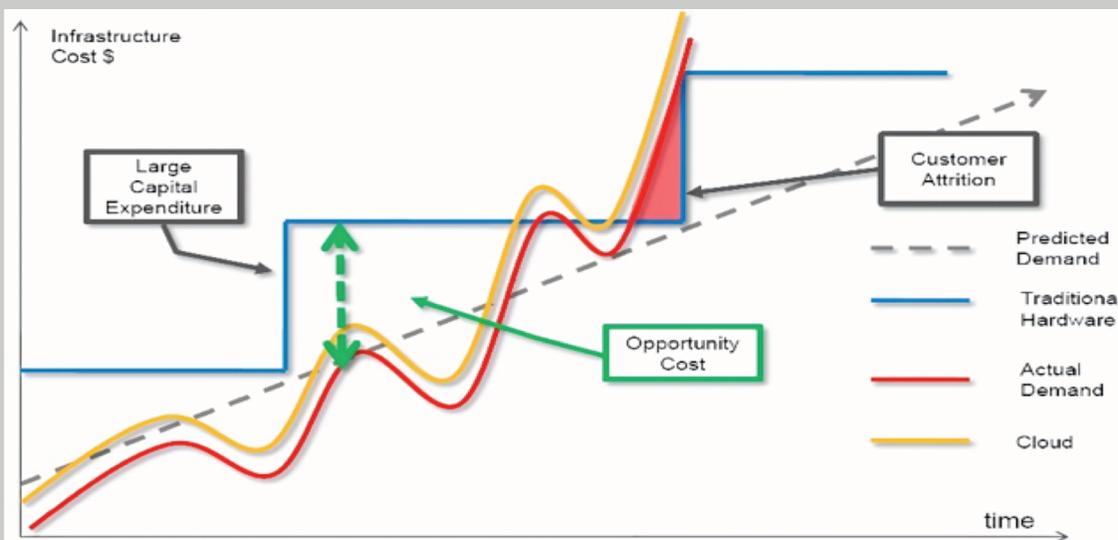


SOURCE HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, FEBRUARY 2017

Harvard Business Review

ADOPTING HYBRID CLOUD BECOMES A STRATEGIC IMPERATIVE





40:34 | ACESSO RÁPIDO

NUBANK

Airbnb, Spotify, Netflix e Nubank são alguns exemplos de empresas que transformaram o seu negócio através do uso de nuvem. Assista ao vídeo que apresenta o case do Nubank.



44:07 | ACESSO RÁPIDO

EMBRAER

Veja mais um case de sucesso, que apresenta um sistema totalmente baseado na plataforma da AWS (Amazon Web Services) desenvolvido pela Embraer.





49:02 | ACESSO RÁPIDO

FÓRMULA 1

A Fórmula 1 também se beneficiou do uso da nuvem pública. Assista ao vídeo e conheça mais um case.



AULA 1, PARTE 4

MARCELO ZILLO



00:01 | CHECKPOINT DE APRENDIZAGEM

SOFA E PLANO DE MIGRAÇÃO

Nem todas as empresas nascem em um ambiente 100% Cloud Native, então, é necessário passar pelo processo de migração, que deve ser muito bem planejado, mas que pode ter caminhos distintos e metodologias diferentes. A maioria dos provedores de serviços de nuvem possuem um framework que auxilia a montar um plano para migrar as aplicações para um ambiente de nuvem pública, mantendo um ambiente de nuvem privada. Abaixo, veja um exemplo de Framework da Microsoft:

Cloud Adoption Framework – Microsoft 48

Microsoft | Docs Documentação Learn Q&A Exemplos de Código

Azure Documentação do produto Arquitetura Aprender sobre o Azure Desenvolver Recursos

Microsoft Cloud Adoption Framework for Azure

O Cloud Adoption Framework é uma coleção de documentação, diretrizes de implementação, melhores práticas e ferramentas comprovadas da Microsoft criadas para acelerar seu percurso de adoção na nuvem.

COMEÇAR AGORA Comece seu percurso na nuvem

BAIXAR Encontre ferramentas e modelos de adoção de nuvem

VISÃO GERAL O que é o Cloud Adoption Framework

NOVIDADES Novidades no Cloud Adoption Framework

Diretrizes do Cloud Adoption Framework

Essas diretrizes se alinham às fases do ciclo de vida de adoção de nuvem, garantindo fácil acesso às diretrizes certas na hora certa.

Introdução Documentar as decisões fundamentais Acelerar a migração Fornecer estabilidade operacional Alinhar sua organização

Estratégia Motivações Resultados dos negócios Alinhar sua estratégia de parceiros Escolha o primeiro projeto certo

Plano Racionalizar seu cenário digital Alinhamento da organização Plano de preparação de habilidades Plano de adoção de nuvem para DevOps

<https://bit.ly/2YoImdn>

FIA BUSINESS SCHOOL proinfo

A seguir, conheça os seis principais pilares para o processo de preparação de migração em nuvem:



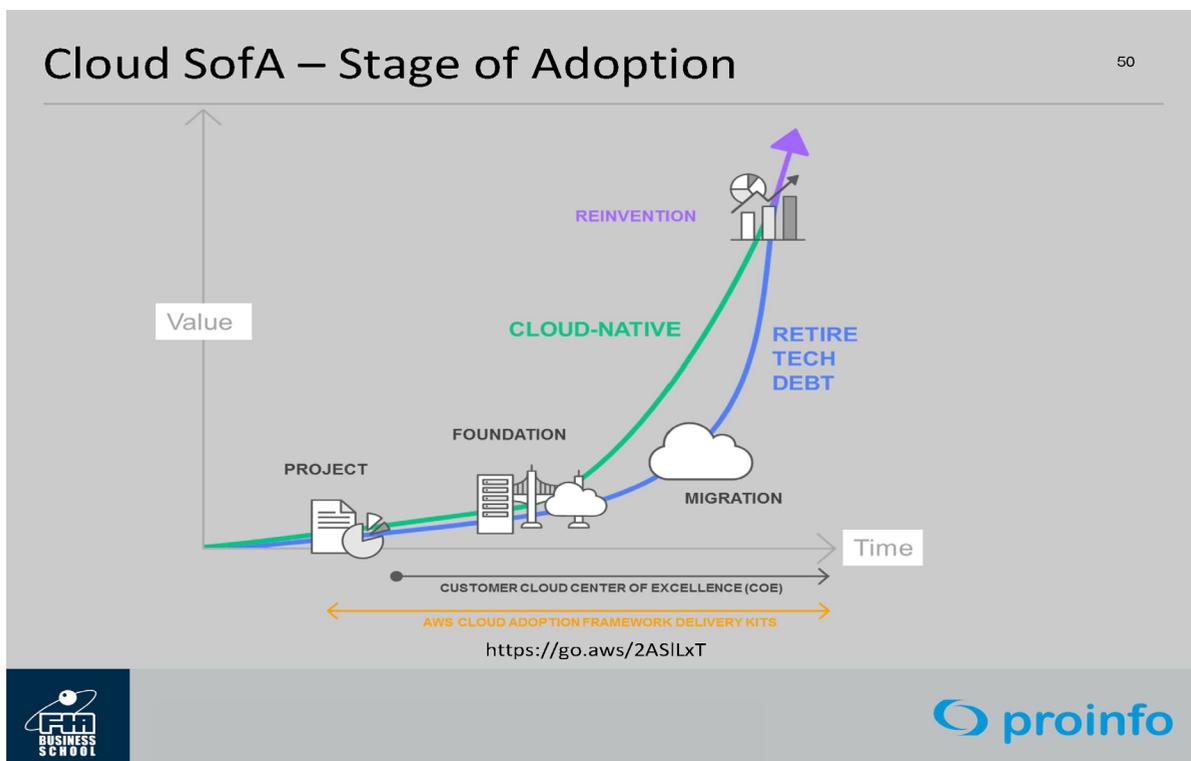
- 1 - **Negócios:** alinhar necessidades de TI com os negócios e mapear os investimentos;
- 2 - **Pessoas:** priorizar as competências;
- 3 - **Governança:** gerenciar investimentos;
- 4 - **Plataforma:** provisionar infraestrutura e aplicações;
- 5 - **Segurança:** gerenciar acessos e autorizações;
- 6 - **Operações:** observar as melhores práticas.



01:42 | GUIA DE PALAVRAS

STAGE OF ADOPTION

Caminho utilizado por empresas que estão começando a pensar em utilizar nuvem pública e que estão preparando o seu processo de migração.





23:29 | SUGESTÃO DE LEITURA

Artigo - The 8r's of cloud migration



33:50 | GUIA DE PALAVRAS

GRAVIDADE DOS DADOS

Situação vivenciada durante o processo de migração de dados para nuvem pública, devido a quantidade de dados que antes estavam armazenados dentro de um data center e passaram a estar fora de ambiente tradicional de armazenamento de dados.



37:49 | SUGESTÃO DE LEITURA

Livro - Ahead in the Cloud: Best Practices for Navigating the Future of Enterprise IT



41:27 | ACESSO RÁPIDO

AWS

Assista aos vídeos da AWS, Azure e VMWare e saiba como eles oferecem o serviço de extensão para migração de dados para nuvem.





45:25 | ACESSO RÁPIDO
AZURE STACK



47:11 | ACESSO RÁPIDO
VMWARE - AWS



AULA 1, PARTE 5

MARCELO ZILLO



00:01 | CHECKPOINT DE APRENDIZAGEM

SEGURANÇA DA X NA NUVEM

Agora que você conhece as bases sobre a computação em nuvem, é hora de compreender como a segurança dos dados funciona nesse ambiente.

A segurança da informação precisa acompanhar a constante evolução dos sistemas de nuvem. Novas ameaças surgem constantemente e o processo de compreender as fragilidades dos novos sistemas deve receber investimentos em pesquisa e desenvolvimento, a fim de impedir ameaças, vírus, invasões e roubo de dados.

Acompanhe algumas diferenças entre a segurança tradicional e na nuvem:

Ambiente tradicional	Nuvem
1. Grandes investimentos <i>upfront</i> .	1. Soluções nativas, sem custo adicional ou no modelo <i>pay as you go</i> .
2. Consome muito tempo para implementação.	2. Soluções de segurança nativas que podem ser implementadas com poucos cliques, sem prejudicar a usabilidade e <i>performance</i> .
3. Impacto em <i>performance</i> , prejudicando usabilidade e negócio.	3. Automação de processos complexos e soluções de segurança escaláveis.
4. Processos manuais, pouco automatizados, não escaláveis.	4. Uso de tecnologias da nuvem para proteger a própria nuvem.

Sabemos que os dados armazenados na nuvem são valiosos para todas as organizações e pessoas, neste sentido, vale destacar alguns fatores importantes que dizem respeito à segurança em ambiente de nuvem:

- Provedores criados com premissa de segurança;
- Automação e previsibilidade;
- Criptografia em escala;
- Resiliência em escala global;
- Tecnologias disponíveis com um click;
- Segurança by design (segurança como código).



02:49 | CONSULTORIA & MENTORIA

"À medida que você busca criar novas aplicações, novos modelos de serviço, novos modelos de negócio para entregar isso rapidamente aos seus clientes, você tem que entregar isso com segurança."



23:43 | CITAÇÃO IMPORTANTE

"A nuvem traz a capacidade de democratizar a tecnologia."

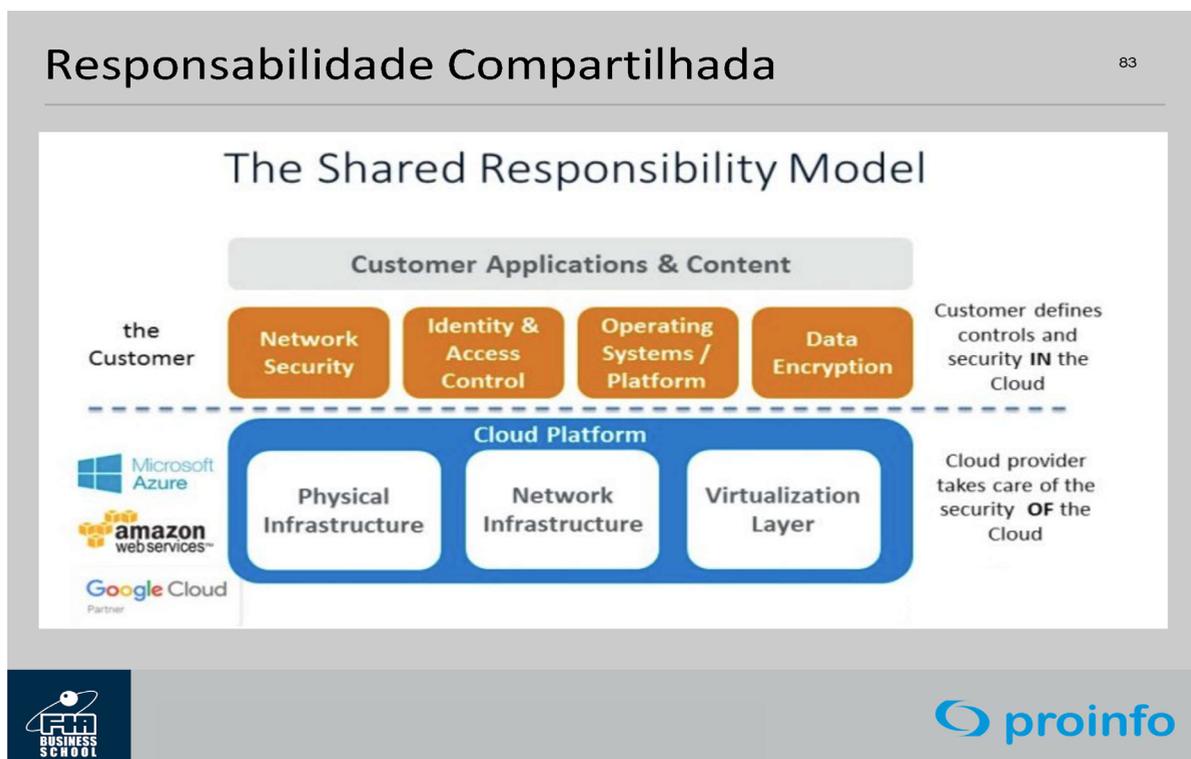
- Marcelo Zillo



25:35 | CHECKPOINT DE APRENDIZAGEM

RESPONSABILIDADE COMPARTILHADA

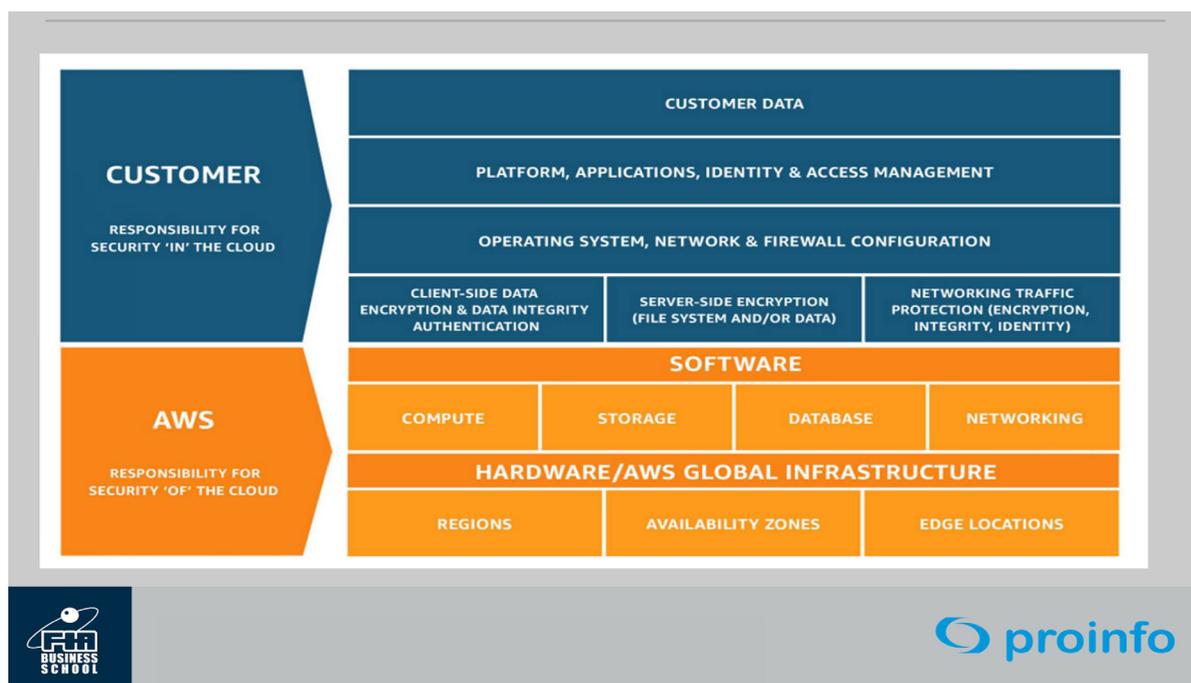
Se trata de um modelo criado pela indústria que determina qual é a responsabilidade do provedor e qual é a responsabilidade do usuário (cliente).



Apesar de ser uma tecnologia avançada e inovadora, a segurança dos dados da nuvem possui uma responsabilidade que não é unilateral. Depende não apenas da empresa provedora do serviço e da estrutura, mas o cliente precisa estar atento à responsabilidade que lhe é imputada nesses casos:

- **O provedor de serviços é responsável pela segurança DA nuvem:** regiões, datacenters, segurança do hardware, roteadores, etc.
- **O cliente é responsável pela proteção dos dados:** acionar os flags de proteção.

A seguir, conheça o modelo da AWS, que foi a primeira empresa a falar sobre o modelo de responsabilidade compartilhada:



AULA 1, PARTE 6

MARCELO ZILLO

00:01 | CHECKPOINT DE APRENDIZAGEM

JORNADA SEGURA

Saiba quais são os aspectos a se considerar ao pensar em um projeto de migração, efetivamente, usando boas práticas de segurança.

Uma das primeiras recomendações é definir quais serão os padrões de segurança que fazem sentido para a sua indústria. As certificações de segurança da informação são a melhor maneira de garantir o conhecimento e as habilidades corretas para se destacar nessa missão.

Conheça algumas:

Certificações relevantes para a indústria 91

Exemplos



The image displays six logos of security certifications arranged in two rows. The top row includes the CSA cloud security alliance logo, the ISO 27017 logo (International Organization for Standardization), and the ISO 27018 logo (International Organization for Standardization). The bottom row includes the PCI Security Standards Council logo, the ISO 27001 logo (International Organization for Standardization), and the HIPAA logo (featuring a caduceus symbol).



03:03 | ACESSO RÁPIDO

AWS - PROGRAMAS DE COMPLIANCE

Acesse o portal da AWS e baixe seus relatórios de auditoria.



03:17 | ACESSO RÁPIDO

MICROSOFT- PROGRAMAS DE COMPLIANCE

A Microsoft também possui um portal que mostra os seus relatórios de auditoria. Acesse o QR Code para saber mais.



06:36 | ACESSO RÁPIDO

GOOGLE- PROGRAMAS DE COMPLIANCE

Conheça a central de recursos de conformidade da Google, onde são disponibilizadas as suas certificações e práticas de segurança adotadas. Vale a pena conferir!





15:25 | CITAÇÃO IMPORTANTE

"The time to repair the roofs when the sun is shining."

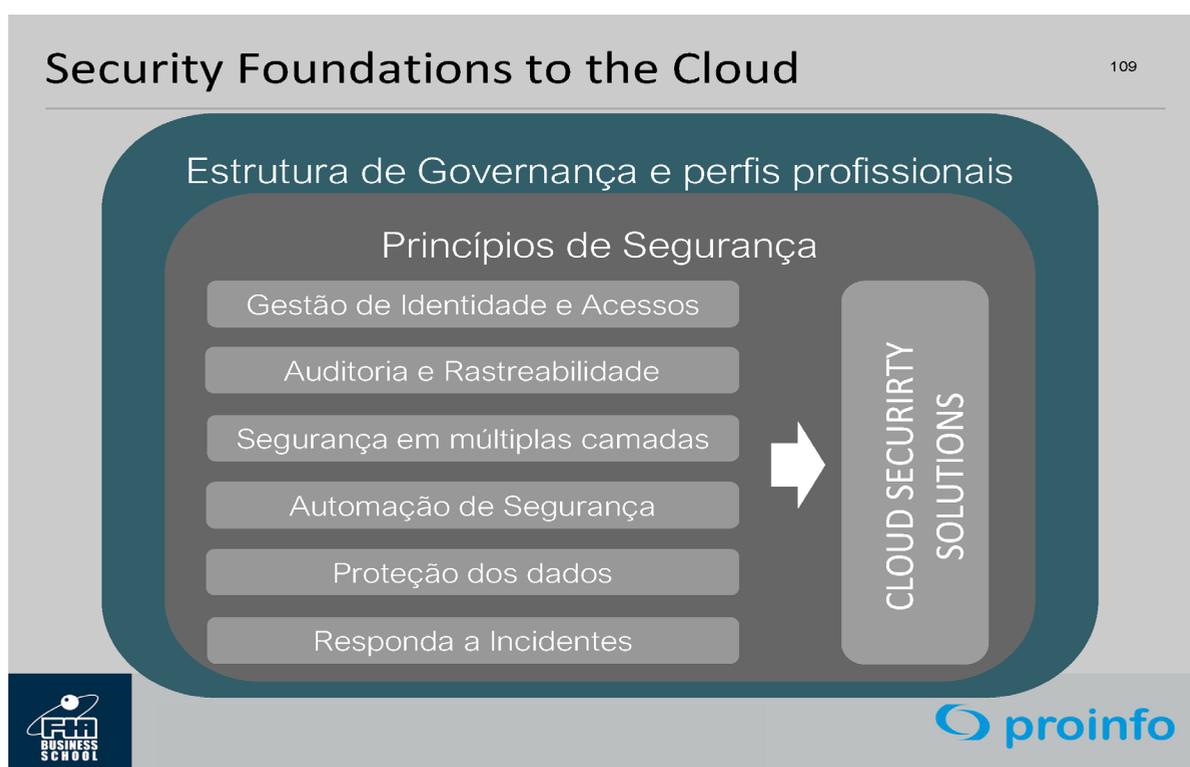
- John F. Kennedy



16:17 | CHECKPOINT DE APRENDIZAGEM

PILARES DE SEGURANÇA

Saiba quais são os princípios de segurança que você deve levar em conta ao adotar um serviço de nuvem:



Fatores relevantes sobre a Estrutura de Governança e Perfis Profissionais:

- 1 – Avalie questões relevantes de conformidade, contratuais e de controles do provedor;
- 2 – A equipe de segurança precisa ter novos perfis de profissionais;
- 3 – Revise seu BIA, PCN, DR;
- 4 – Teste e documente o plano (Continuidade/DR) considerando os recursos e funcionalidades da nuvem que podem, inclusive, melhorar o RTO e RPO.

7 Princípios de Segurança

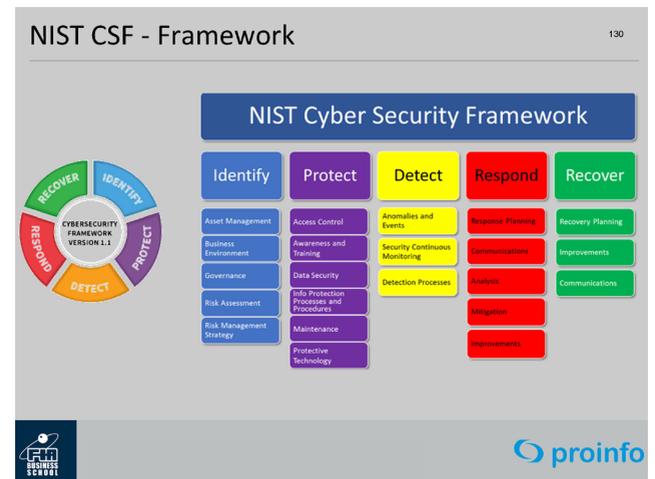
- 1- Gestão de identidade e acessos:** é a espinha dorsal para a criação de uma boa base de segurança na nuvem; essa etapa garante o mínimo de privilégio possível e perfis de acesso;
- 2- Auditoria e rastreabilidade:** centralize, monitore e gere alerta de ações e mudanças executadas em seus ambientes em tempo real;
- 3- Segurança em múltiplas camadas:** isole servidores e aplicações;
- 4- Automação de segurança:** avalie a segurança de aplicações de forma contínua;
- 5- Proteção dos dados:** efetue o mascaramento e o monitoramento de uso de dados;
- 6- Responda a incidentes:** segurança de nuvem em grande escala;
- 7- Cloud security solutions:** entenda o potencial das soluções Cloud Native.



43:57 | REAL BUSINESS CASE

NIST CYBERSECURITY FRAMEWORK

Trata-se de um framework criado para auxiliar empresas que estão diretamente relacionadas à infraestrutura crítica, e que tem por objetivo gerenciar e reduzir o risco de segurança cibernética.



45:37 | ACESSO RÁPIDO

NIST CYBERSECURITY FRAMEWORK IN THE AWS CLOUD

Saiba como implementar recursos de segurança, nativos do ambiente de nuvem, para se adequar ao NIST, acessando ao documento disponibilizado pela AWS.





53:48 | CONSULTORIA & MENTORIA

"Transformação digital, sem dúvida, pode ser acelerada com adoção de nuvem, com adoção de práticas ágeis, com uso de recursos nativos, com uso de tecnologia cloud native, mas se planeje, prepare o seu ambiente, pense na fundação e acelere a migração e a transformação digital."



CURADORIA

SITES E LIVROS RECOMENDADOS

1. Shared Responsibility Model (AWS)

Documento detalhando o modelo de responsabilidade compartilhada sugerido pela fornecedora de serviços em nuvem Amazon Web Services (AWS)

2. How Cloud Computing Is Changing Management

3. Shared Responsibility Model (Azure)

Documento elaborado pela Microsoft destacando modelo de responsabilidade compartilhada e quais tarefas de segurança devem ser tratadas pelo provedor de nuvem e quais tarefas devem ser tratadas pelo usuário.

4. Shared Responsibility Model (GCP)

Mais um documento, este elaborado pela Google detalhando o modelo de responsabilidade compartilhada de seu serviço de nuvem.

5. RESOLUÇÃO Nº 4.658, DE 26 DE ABRIL DE 2018

Resolução do Banco Central do Brasil (BACEN) sobre segurança cibernética e os requisitos para a contratação de serviços de computação em nuvem que devem ser observados pelas instituições financeiras e demais instituições autorizadas a funcionar no Brasil pelo BACEN.

6. (ISC)2 CCSP Certified Cloud Security Professional Official Study Guide 2nd Edition

Livro preparatório para o exame de certificação de profissionais para atuação em Segurança de Computação em Nuvem (Certified Cloud Security Professional) da (ISC).

(ISC)2 CCSP Certified Cloud Security Professional Official Study Guide, Editora: Sybex; Edição: 2nd (25 de dezembro de 2019), ISBN-10: 1119603374, ISBN-13: 978-1119603375

7. CSK Certificate of Cloud Security Knowledge All-in-One Exam Guide

O livro apresenta uma referência para os profissionais que estão se preparando para a prova de certificação 'Certificate of Cloud Security Knowledge', mas também é utilizado como fonte de consulta por profissionais de segurança na nuvem pois fornece ao leitor bases necessárias para a proteção dos dados em ambiente de nuvem.

Autor: Graham Thompson, ISBN-13: 978-1260460087 , ISBN-10: 1260460088

8. A Case Study of the Capital One Data Breach

Estudo do Caso do incidente de violação de dados da Capital One, uma das maiores instituições financeiras dos EUA. Este estudo tem como objetivo entender o modus operandi técnico dos ataques, mapear as vulnerabilidades exploradas em um ataque e identificar os requisitos de conformidade e controle da

organização afetada com base versão 1.1 do National Institute of Standards and Technology (NIST) Cybersecurity Framework, uma estrutura agnóstica amplamente usada na indústria global para fornecer diretrizes de mitigação de ameaças cibernéticas.

9. CSA Releases New Research - Top Threats to Cloud Computing: Egregious Eleven

Relatório elaborado pela Cloud Security Alliance apresenta a pesquisa divulgada em 2019 identificando os problemas mais comuns de segurança e fornece um conjunto de recomendações de procedimentos e técnicas de controle que podem servir de referência para as equipes de compliance, riscos e tecnologia. O relatório classifica ainda onze principais tipos de riscos de segurança em nuvem, entre eles o os riscos de configuração incorreta, o sequestro de conta, interfaces e APIs inseguras, entre outros riscos.

10. Top Threats to Cloud Computing: Deep Dive

Estudo de caso que busca destacar variáveis de análise de segurança em computação de nuvem considerando as principais ameaças conhecidas. Através de nove casos de exemplos são apresentados uma narrativa detalhada e um gráfico de referência que fornece um resumo do estilo de ataque do ator, criando uma ponte entre as ameaças e vulnerabilidades e os controles e ações de prevenções necessárias.

11. Cloud Adoption Framework (AWS)

Documento elaborado pela AWS que propõe um Framework de referência para as organizações projetarem e executarem um conjunto de atividades para a adoção da computação em nuvem.

12. AWS Compliance Programs

Detalhamento do nível de aderência e conformidade dos serviços de nuvem da AWS em legislações e regulamentações existentes em diversos países.

13. Azure Compliance Programs

Detalhamento do nível de aderência e conformidade dos serviços de nuvem da Microsoft em legislações e regulamentações existentes em diversos países.

14. GCP Security Programs

Detalhamento do nível de aderência e conformidade dos serviços de nuvem da Google em legislações e regulamentações existentes em diversos países.

15. CSA – Cloud Security Alliance

A Cloud Security Alliance (CSA) é a organização líder mundial dedicada à definição e conscientização das melhores práticas para ajudar a garantir um ambiente seguro de computação em nuvem.

16. CSA – Cloud Security Alliance – Security Guidance v4.0

Guia de referência elaborado pela CSA com objetivo de fornecer orientação quanto ao uso dos serviços de nuvem para o atendimento das metas de negócios, com foco no gerenciamento e na mitigação dos riscos associados à adoção da tecnologia de computação em nuvem. O guia apresenta 14 domínios que vão desde “conceitos e arquitetura da cloud” até “segurança como serviço”.

17. NIST Cyber Security Framework (AWS)

Material elaborado pela AWS que avalia a Cloud Security Framework (CSF) do NIST e aderência dos serviços oferecidos pela AWS aos requisitos e recomendações do Framework da NIST.

18. NIST Cyber Security Framework (Azure)

Material elaborado pela Microsoft que avalia a Cloud Security Framework (CSF) do NIST e aderência dos serviços oferecidos pela AZURE aos requisitos e recomendações do Framework da NIST.

19. Serviços de Segurança AWS

Conjunto de serviços de segurança de nuvem, e casos de uso com a aplicação de cada serviço, oferecidos pela empresa AWS

20. Serviços de Segurança Microsoft

Conjunto de serviços de segurança de nuvem oferecidos pela empresa Microsoft na plataforma Azure.

21.State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating

22.AWS vs Azure vs Google Cloud Market Share 2020: What the Latest Data Shows

23. Private x Public Cloud

24. Gartner Magic Quadrants for Cloud Services

25.ADOPTING HYBRID CLOUD BECOMES A STRATEGIC IMPERATIVE - HARVARD BUSINESS REVIEW

26.Microsoft SofA

27. AWS SofA

28. Microsoft Zero Trust model

ESTUDO DE CASO

Caro aluno(a) FIA Online,

Neste estudo de caso você analisará uma situação vivenciada pela empresa Trade Bank que está pensando em migrar seus ambientes tecnológicos para a Cloud. Trata-se um banco tradicional com mais de 30 anos de presença no mercado da América Latina.

Atualmente, o ambiente tecnológico roda 100% on-premise (em ambiente de Datacenter tradicional) e o CIO está fortemente inclinado a migrar para serviços de nuvem pública.

No entanto, vários executivos têm preocupação em levar dados confidenciais para um serviço de nuvem pública.

Diante do exposto, você deverá se colocar no lugar do responsável pela área de segurança da informação e apresentar um plano para adoção segura e ágil de serviços de nuvem pública para a empresa Trade Bank.



CASO

Trade Bank - Plano para adoção de nuvem segura

GLOSSÁRIO

AWS: Amazon Web Services é uma plataforma de serviços de computação em nuvem oferecida pela Amazon.

CCoE: Cloud Center of Excellence - Centro de Excelência em Nuvem.

CDN: Content Delivery Network - Rede de fornecimento de conteúdo.

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. Em vez de comprar, ter e manter datacenters e servidores físicos, você pode acessar serviços de tecnologia, como capacidade computacional, armazenamento e bancos de dados, conforme a necessidade, usando um provedor de nuvem como a Amazon Web Services (AWS).

Cloud Native: Uma aplicação de computação nativa é criada especificamente para fornecer uma experiência de desenvolvimento consistente e gerenciamento automatizado em nuvem privada.

Community Cloud: Nuvem comunitária - Controlada e usada por um grupo de organizações com interesses comuns.

Content Delivery Network: Rede de fornecimento de conteúdo.

CSP: Cloud Server Providers - Provedores de Serviços de Nuvem.

DTO: Data Transfer Out - Transferência dos dados de saída.

FaaS: Function as a Service - A Função como Serviço - Permite que desenvolvedores criem e executem aplicativos e recursos sem a necessidade de construir ou manterem uma infraestrutura complexa.

Fail Fast: Fracasse Rápido - Filosofia que valoriza a constante experimentação dos projetos em busca de ideias que possuam valor real. O principal foco desse conceito é a diminuição da perda de investimento financeiro e de tempo, uma vez que se detecta rápido os pontos que podem levar ao fracasso e se inicia uma nova bateria de ideias.

Fail Often: Falhe Frequentemente - Quanto maior a quantidade de testes, maiores as oportunidades de aprendizado.

Gartner Magic Quadrant: O quadrante mágico do Gartner é uma representação gráfica das atividades do mercado tecnológico em um determinado período de tempo.

Hybrid Cloud: Nuvem Híbrida - Refere-se ao uso combinado de plataformas de nuvem privada e pública.

IaaS: Infraestrutura como Serviço - Utiliza-se o provedor de serviços para ter acesso a uma capacidade de hardware que corresponde à memória, ao armazenamento, ao processamento etc.

IoT: Internet of Things - Internet das Coisas.

LGPD: Lei Geral de Proteção de Dados - A Lei nº 13.709/2018 dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Machine Learning: Aprendizado de Máquina - É a capacidade que uma máquina adquire de aprender tal como fazem os humanos por meio da inteligência artificial.

NIST: Framework de segurança cibernética - Também chamado de NIST Cyber Security Framework, trata-se de um framework criado para auxiliar empresas que estão diretamente relacionadas à infraestrutura crítica, e que tem por objetivo gerenciar e reduzir o risco de segurança cibernética.

PaaS: Plataforma como Serviço - Contrata-se um ambiente completo de desenvolvimento (porta, usuário, senha e plataforma) no qual é possível criar, modificar e otimizar softwares e aplicações.

Private Cloud: Nuvem Privada - Operada e gerenciada pela própria organização com o objetivo de atender a suas próprias necessidades.

Public Cloud: Nuvem Pública - A nuvem pública é um modelo de implantação em nuvem no qual os recursos de computação pertencem a um provedor e são operados por ele, que os compartilha entre vários locatários via Internet.

Refactoring: Redesenhar uma aplicação.

Relocate: Realocar recurso do ambiente tradicional para o ambiente de nuvem pública.

RIPA: É uma Lei do Parlamento do Reino Unido, que regula os poderes dos órgãos públicos de realizar a vigilância e investigação, e controlar a interceptação de comunicações.

SaaS: Software como Serviço - Tudo é disponibilizado na nuvem, para ter acesso ao serviço pelo browser ou por um software.

Stage of Adoption - Caminho utilizado por empresas que estão começando a pensar em utilizar nuvem pública e que estão preparando o seu processo de migração.

SoC: Separation of Concerns - Um princípio de engenharia de software, que visa separar preocupações.

Streaming: Serviços de streaming são aqueles que possibilitam a transmissão de conteúdos pela internet, sem a necessidade do usuário fazer download para ter acesso ao filme, música ou livro.

WORM: Write Once Read Many ou "Escrita Uma Vez e Leitura Várias" numa tradução livre, é um conceito de sistema de armazenamento.

Fi ONLINE