

**MBA
USP
ESALQ**

CLOUD COMPUTING
Marcello Zillo Neto

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Law No. 9610/98

Marcello Zillo Neto [in](#)

Helping CISOs, C-Level executives and security teams rethink their security strategies for the present and future / Cybersecurity Professor / Writer / Member of Executive Sounding Board --> My opinions are my own.

São Paulo, São Paulo, Brazil · [500+ connections](#) · [Contact info](#)

[Open to](#) [Add profile section](#) [More...](#)

Microsoft

MIT Sloan School of Management

> 20 anos em Cyber Security

Engenheiro de Computação-USF; Pós em Segurança-IPEN; MBA Executivo – Insper; Transformação Digital e ML – MIT; Professor em vários cursos de Pós-Graduação.

[Marcello Zillo Neto | LinkedIn](#)

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

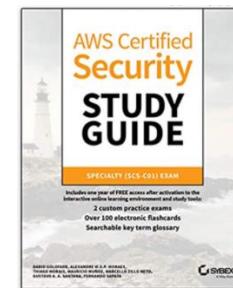


accenture

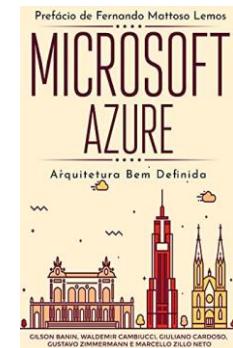
Santander

Banco Safra

aws



[Microsoft Azure: Well-Architected](#)



MBA USP ESALQ

Class Agenda

1

Introduction

2

SofA and migration plan

3

Security OF X IN Cloud

4

Creating your security journey

2

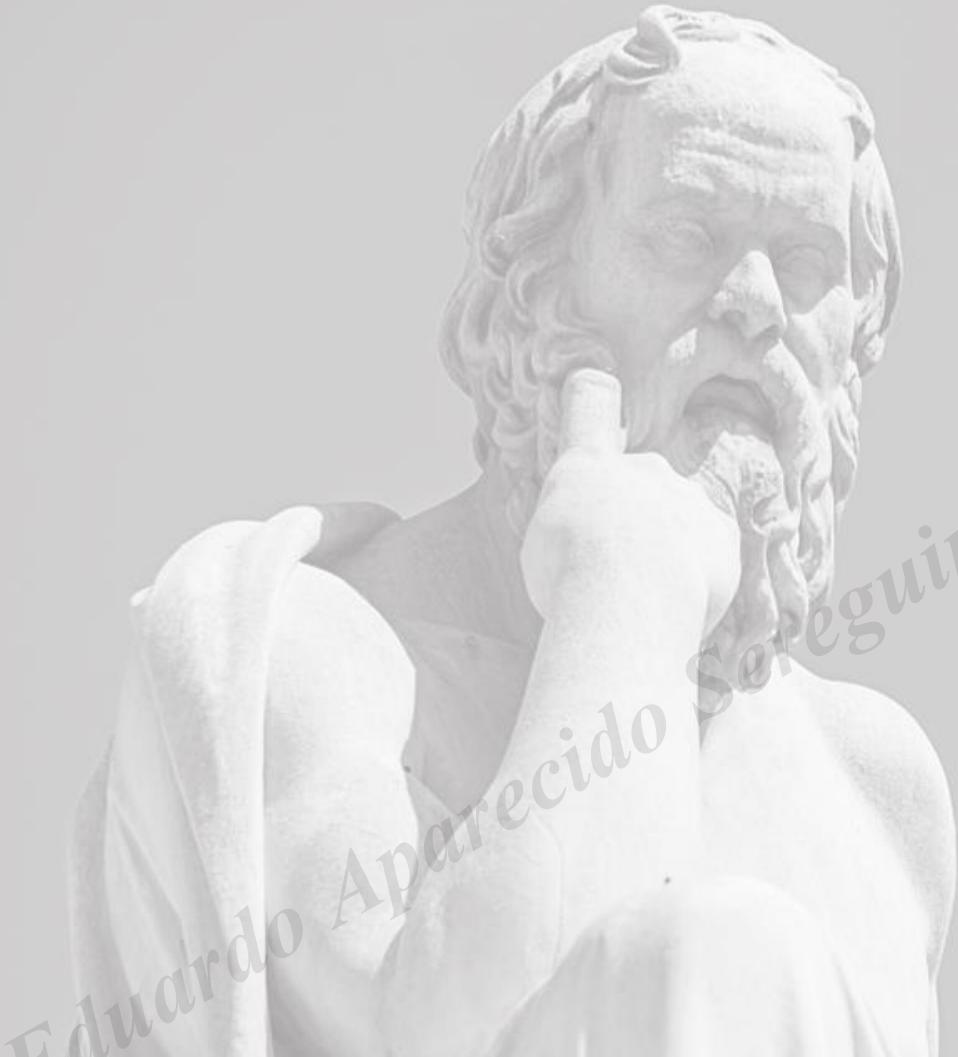
5

Data Security Architeture (examples)

Class Agenda

1

Introduction



1. What changes in management ?
2. Is the use of cloud safe?
3. How to migrate ?
4. What to migrate first?
5. What are the risks?
6. What are the myths ?
7. Is this only for startups?
8. What is the big challenge to implement?
9. What are the benefits?
10. What is the role of cloud in Digital Transformation?

Definition



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization **is prohibited**.



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization **is prohibited**.

Must Read

TECHNOLOGY

How Cloud Computing Is Changing Management

by Quentin Hardy

February 08, 2018

 Summary  Save  Share  Comment 7  Print  PDF \$8.95 Buy Copies



<https://hbr.org/2018/02/how-cloud-computing-is-changing-management>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

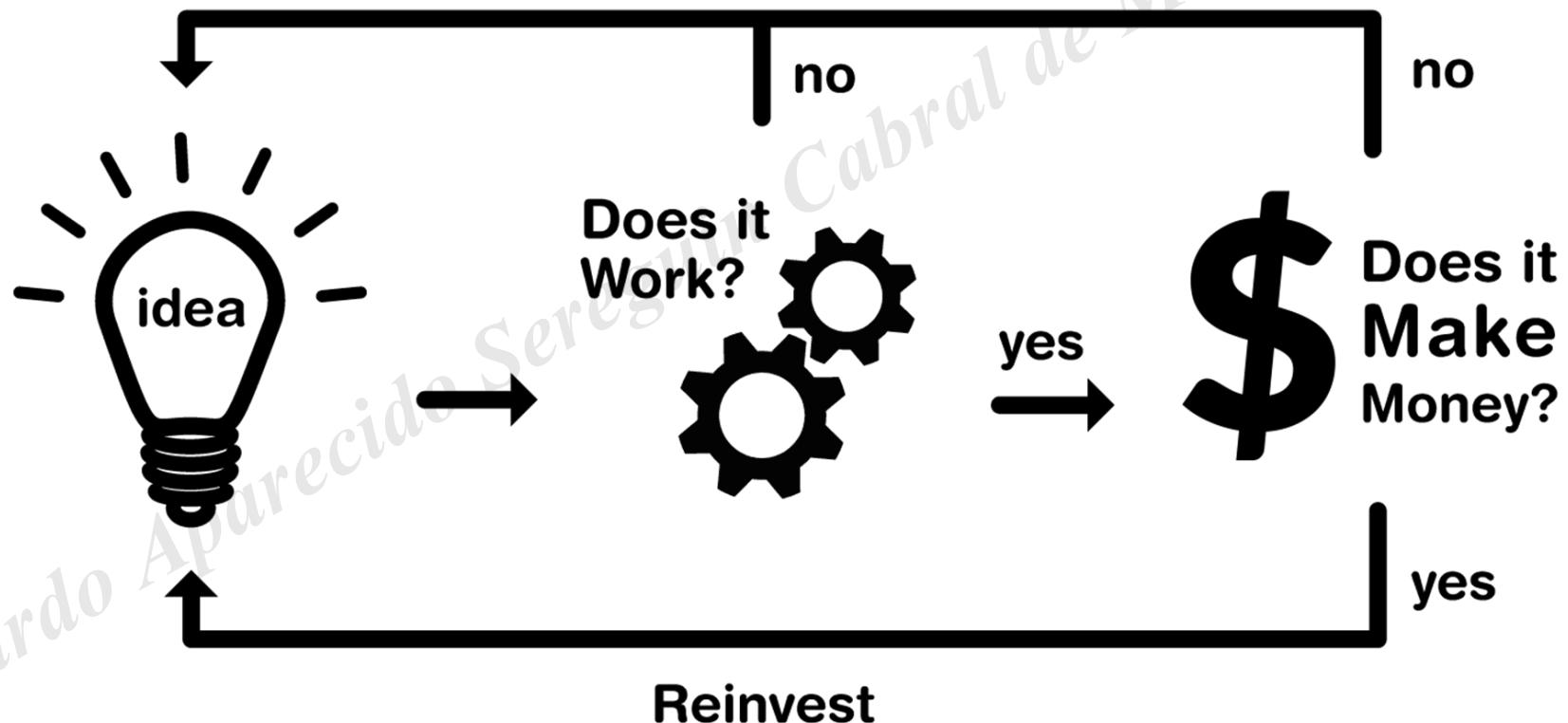
Cloud Computing and Change Management

“With the cloud, we can replicate processes more quickly. But you still need three things to be updated before you fully take advantage: **Organizational innovation, trained human capital, and social institutions, like infrastructure and regulation, that accommodate new technologies.**”

Erik Brynjolfsson – MIT Sloan School of Management

Fail Fast

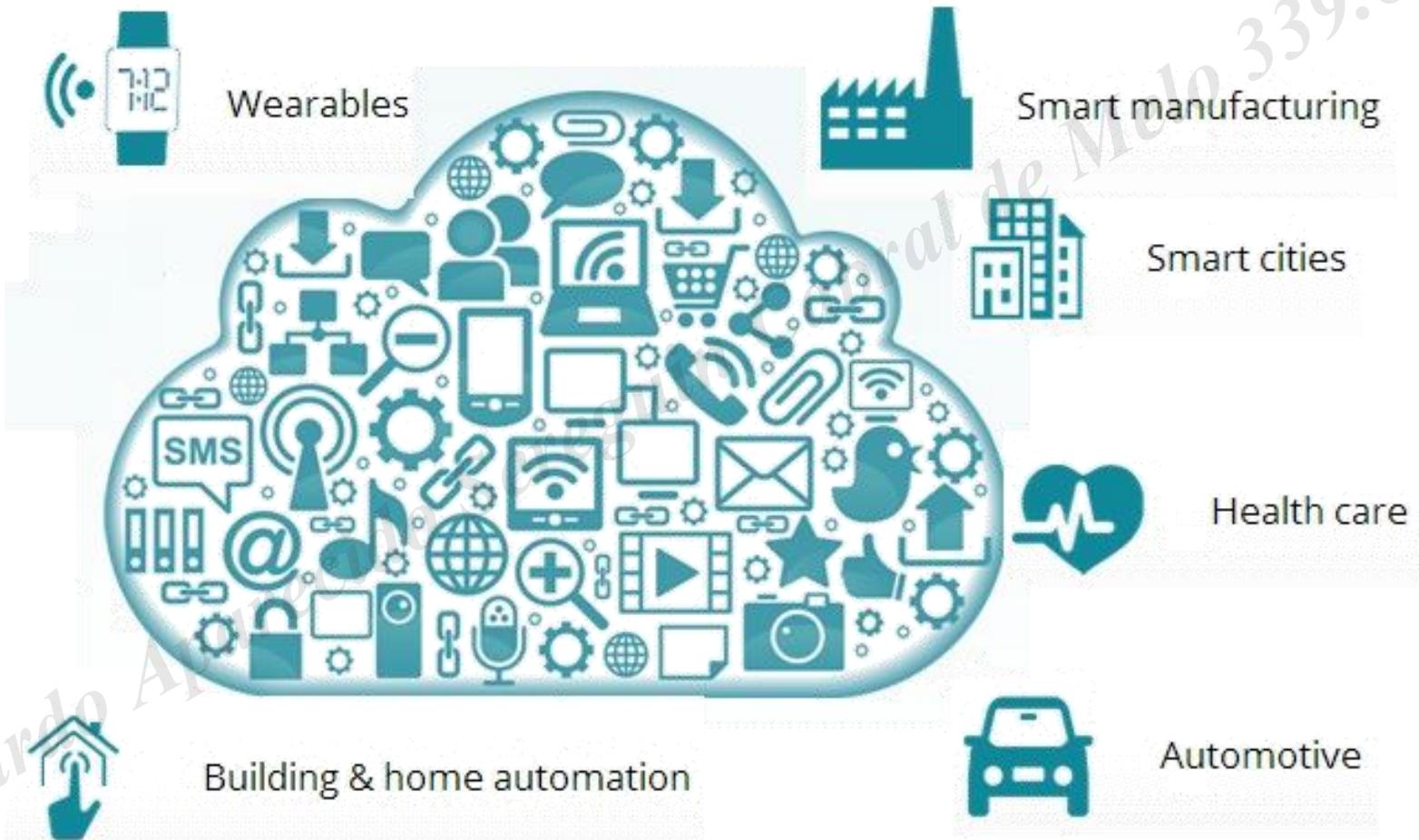
Fail Fast, Fail Often The Simplest Business Plan



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

New technologies and Cloud - IoT

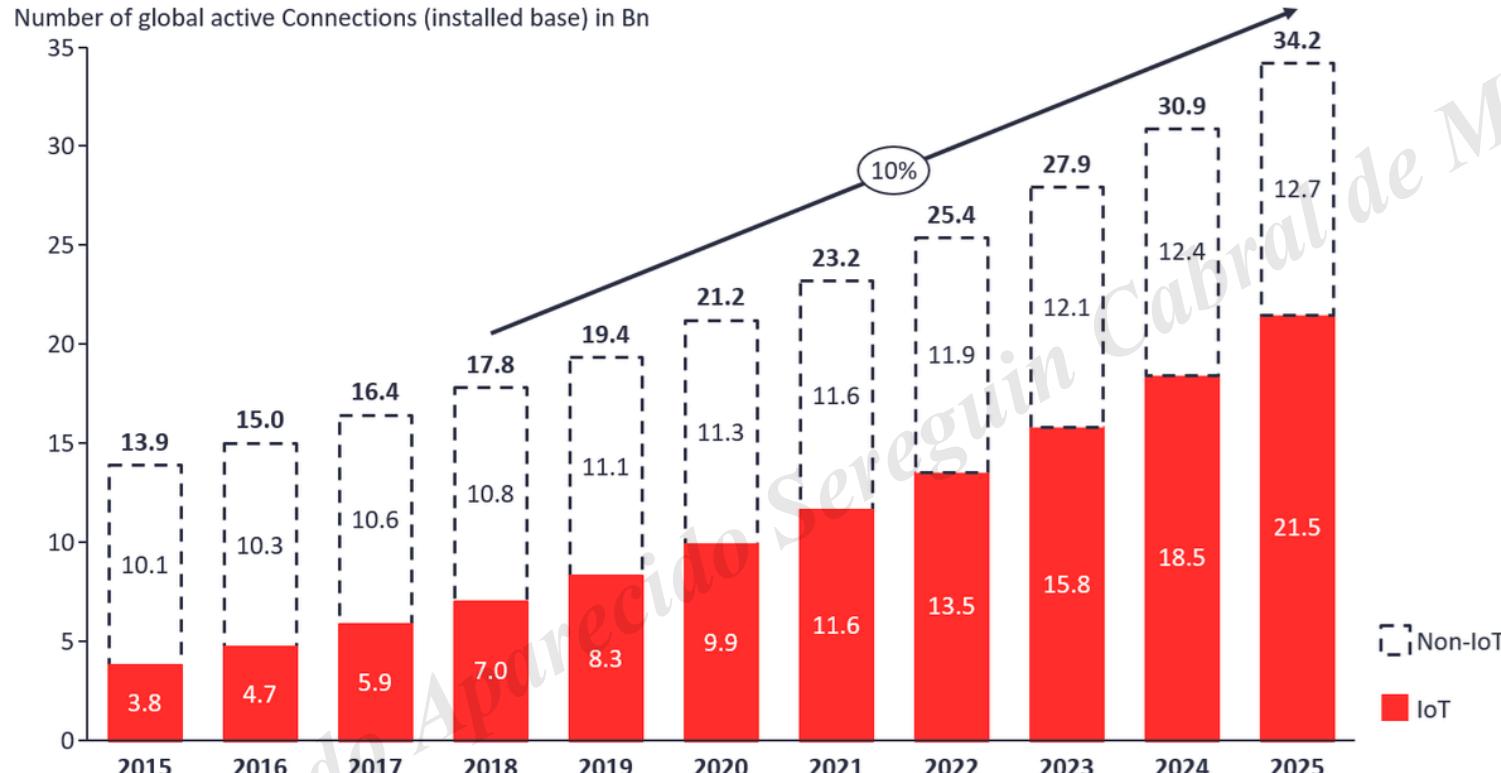


*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Total IoT Devices

Total number of active device connections worldwide

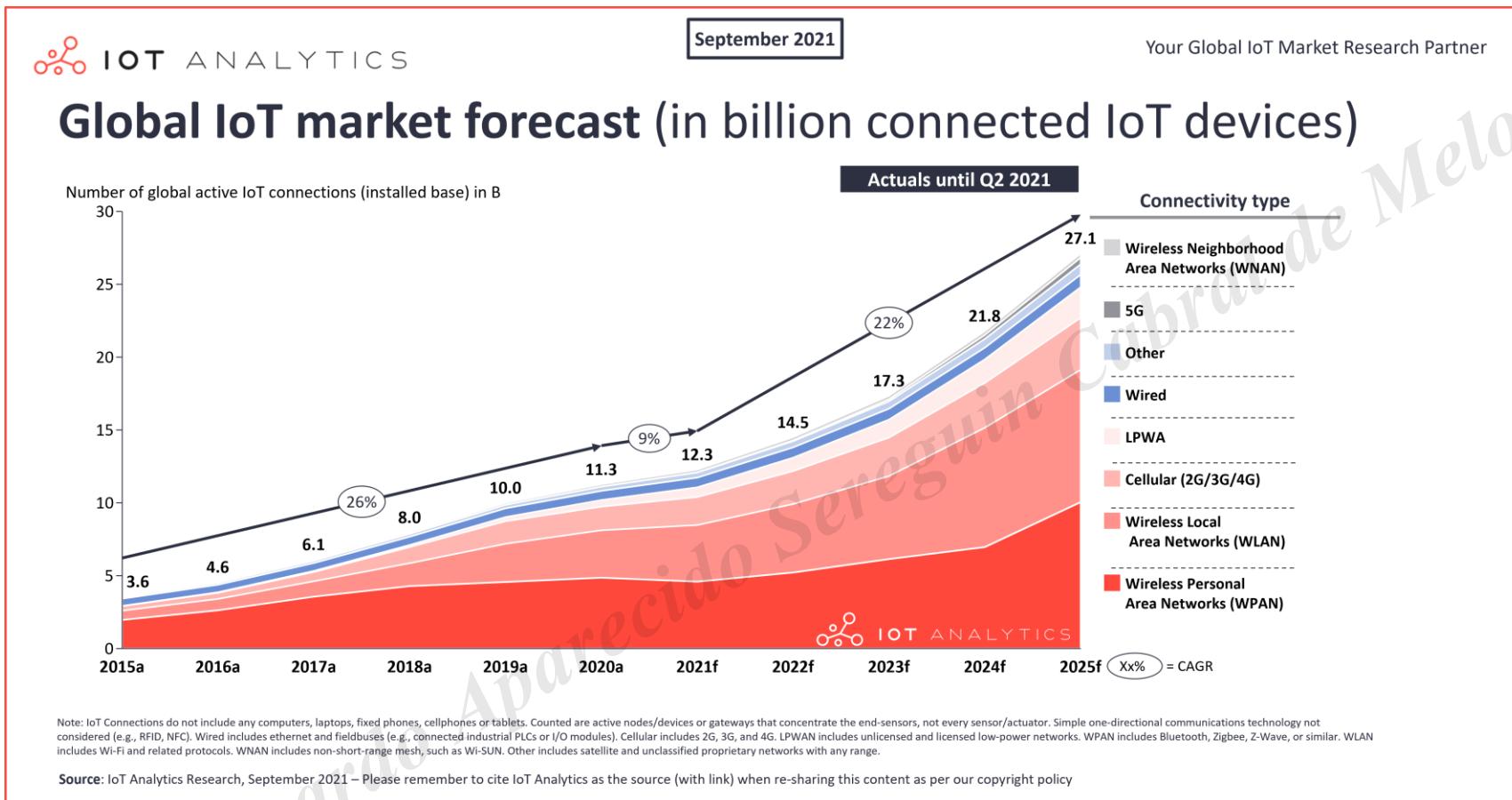


<https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

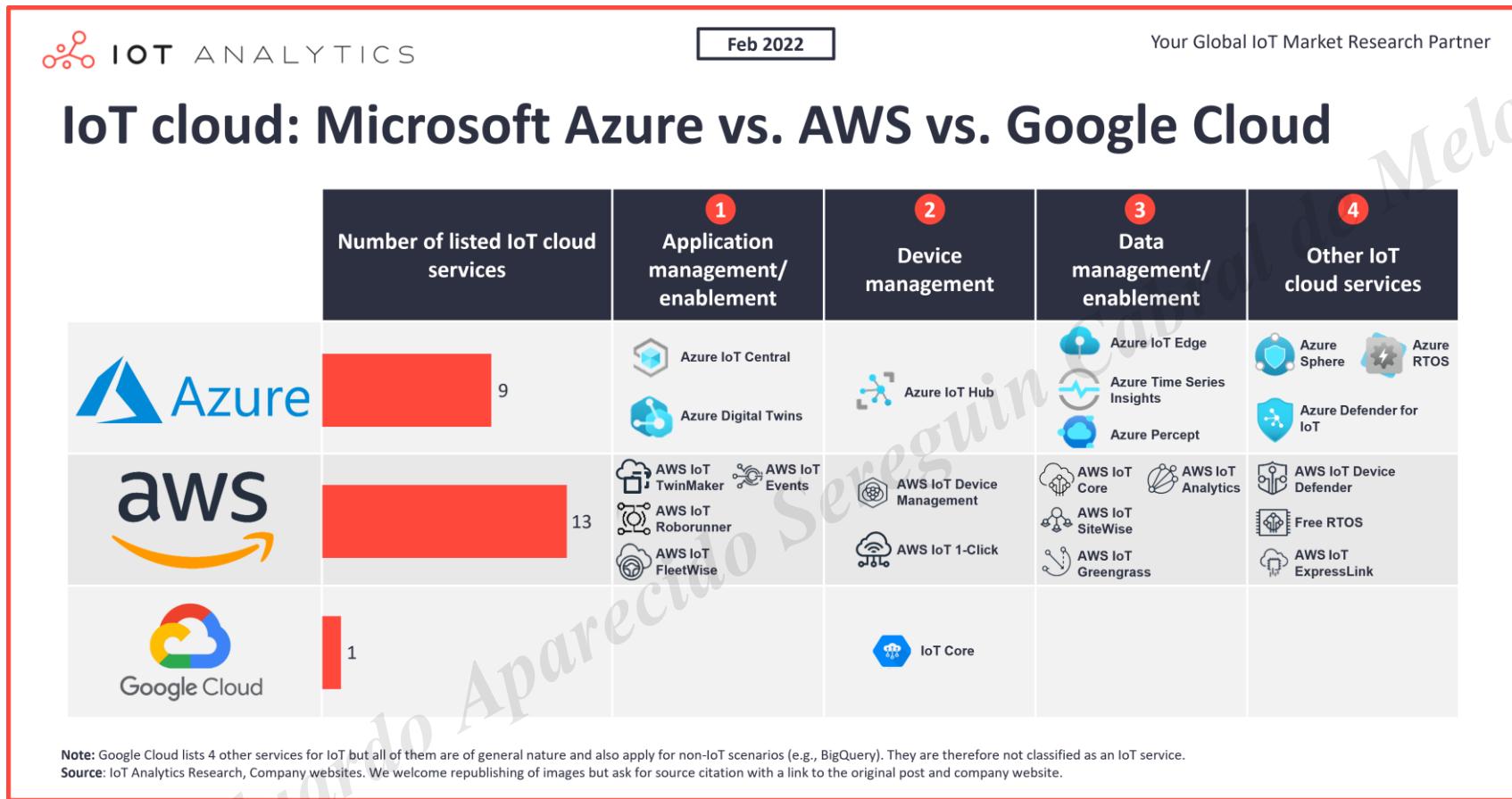
Total IoT Devices



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

IoT cloud



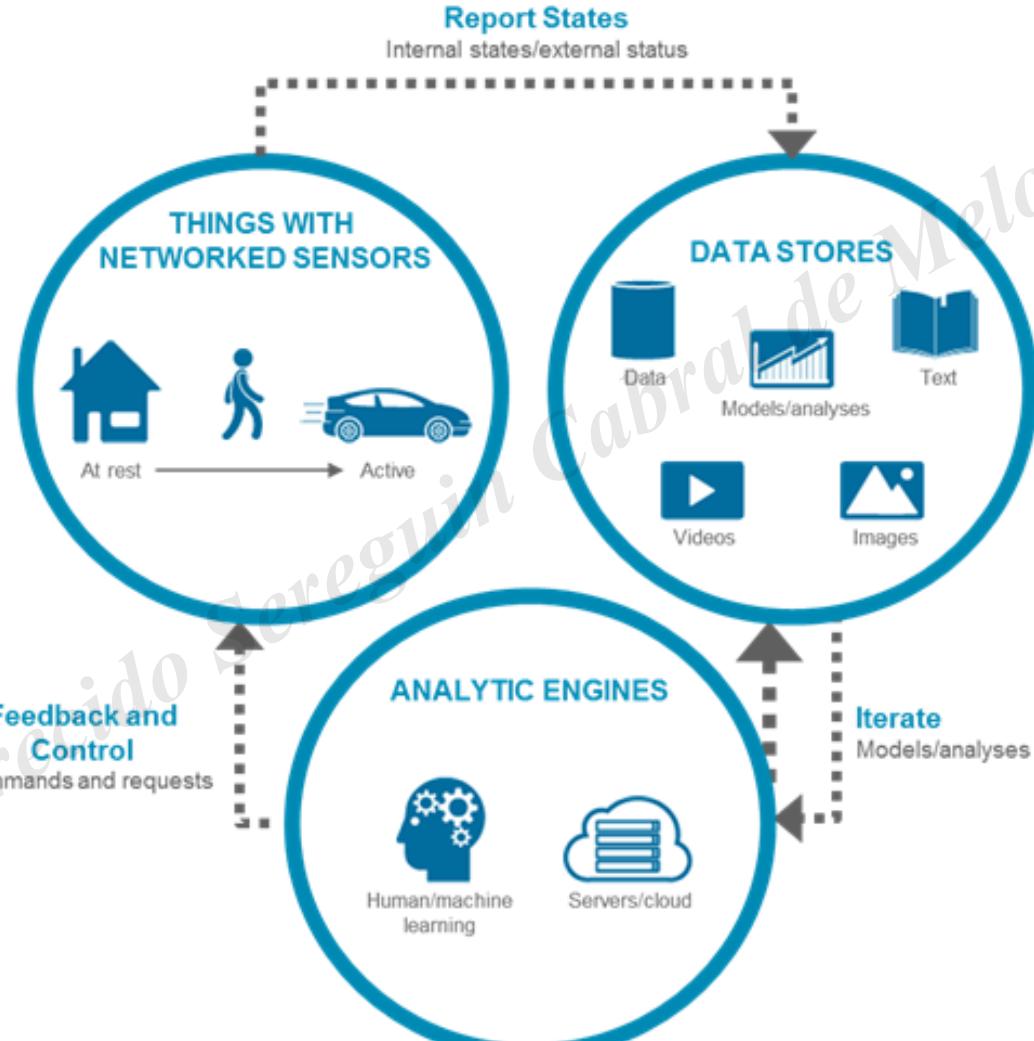
<https://iot-analytics.com/iot-cloud/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Analytics and Cloud

Interaction Between the Three Components of the Internet of Things



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

How many industries were transformed



Public Cloud

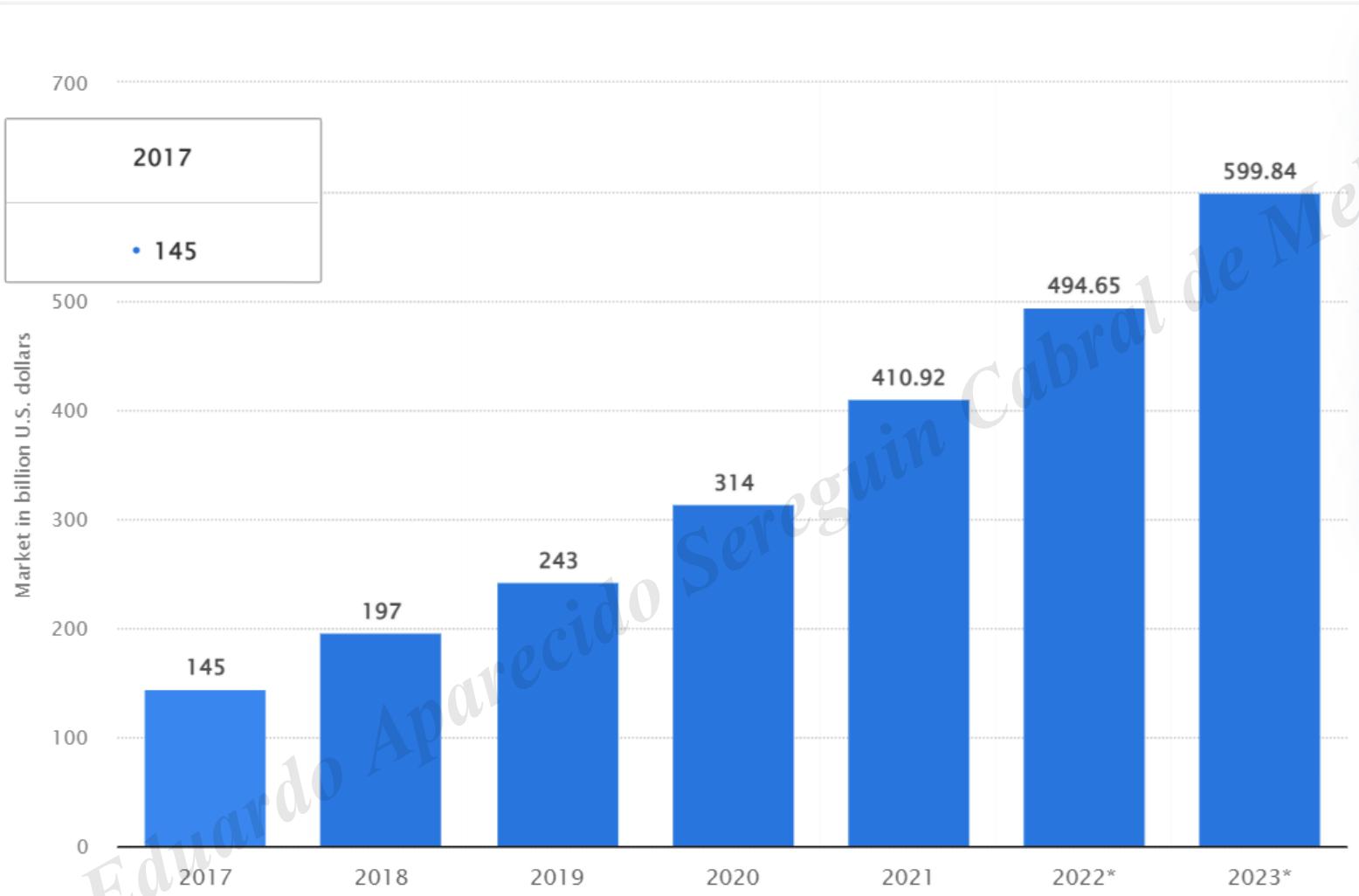
- Resources of hardware, facilities, software and people are property and managed by vendor, charged in the model of Pay as you Go.



Google Cloud

Public Cloud Worldwide

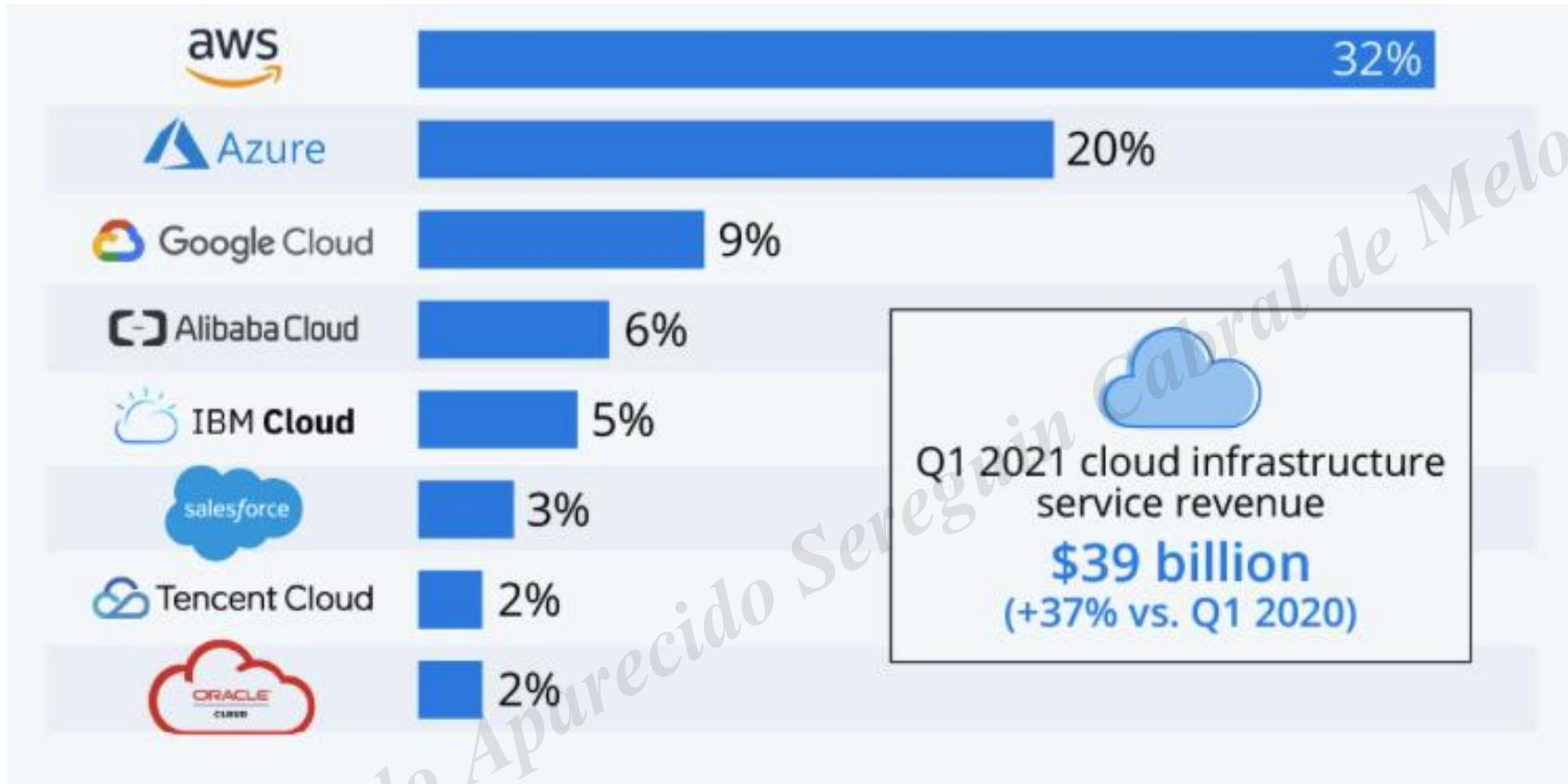
2017 - 2023



<https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Worldwide Market – Q1 2021



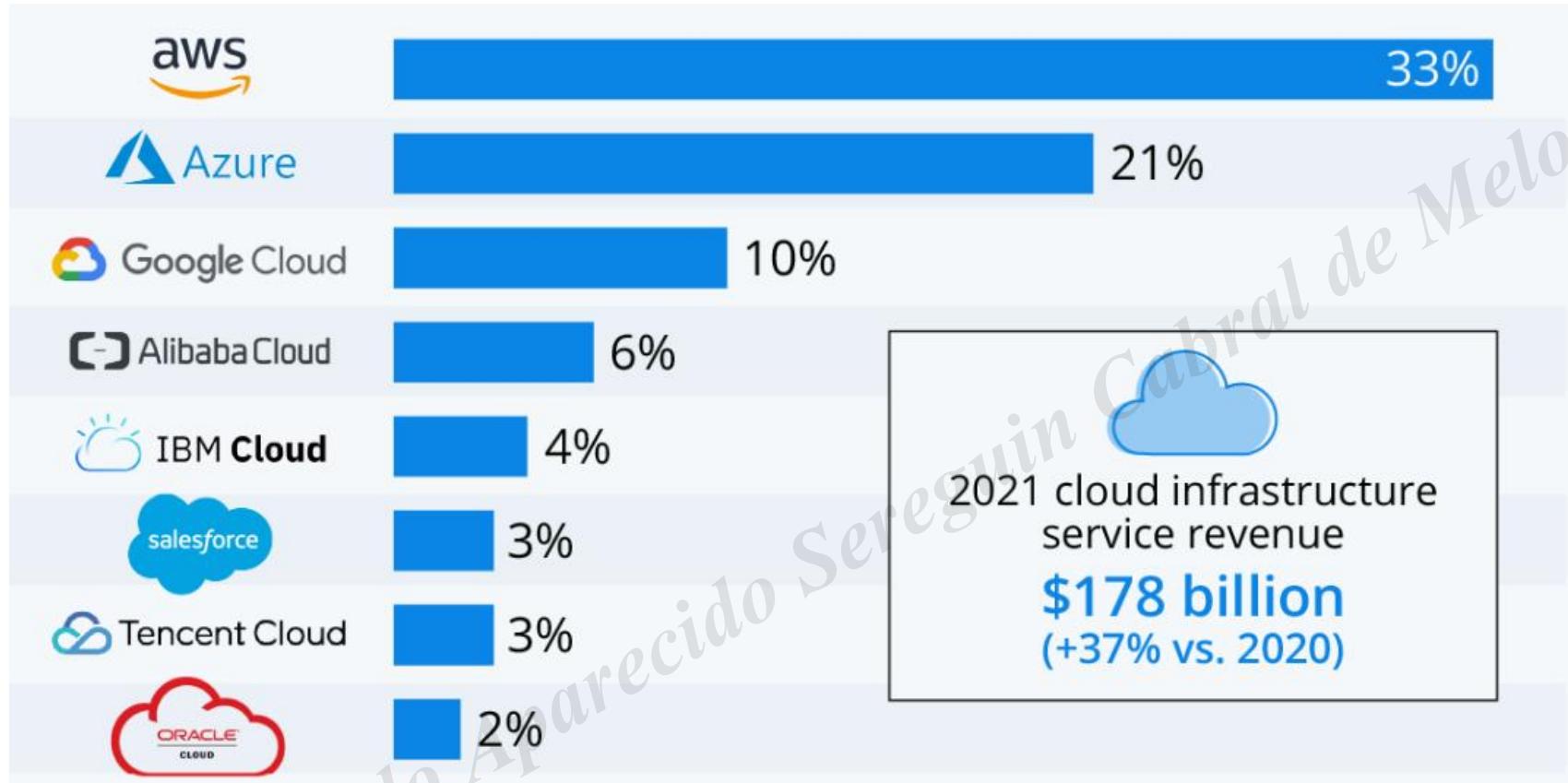
\$150 Billion
Cloud Market

<https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Worldwide Market – Q4 2021



\$180 Billion
Cloud Market

<https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

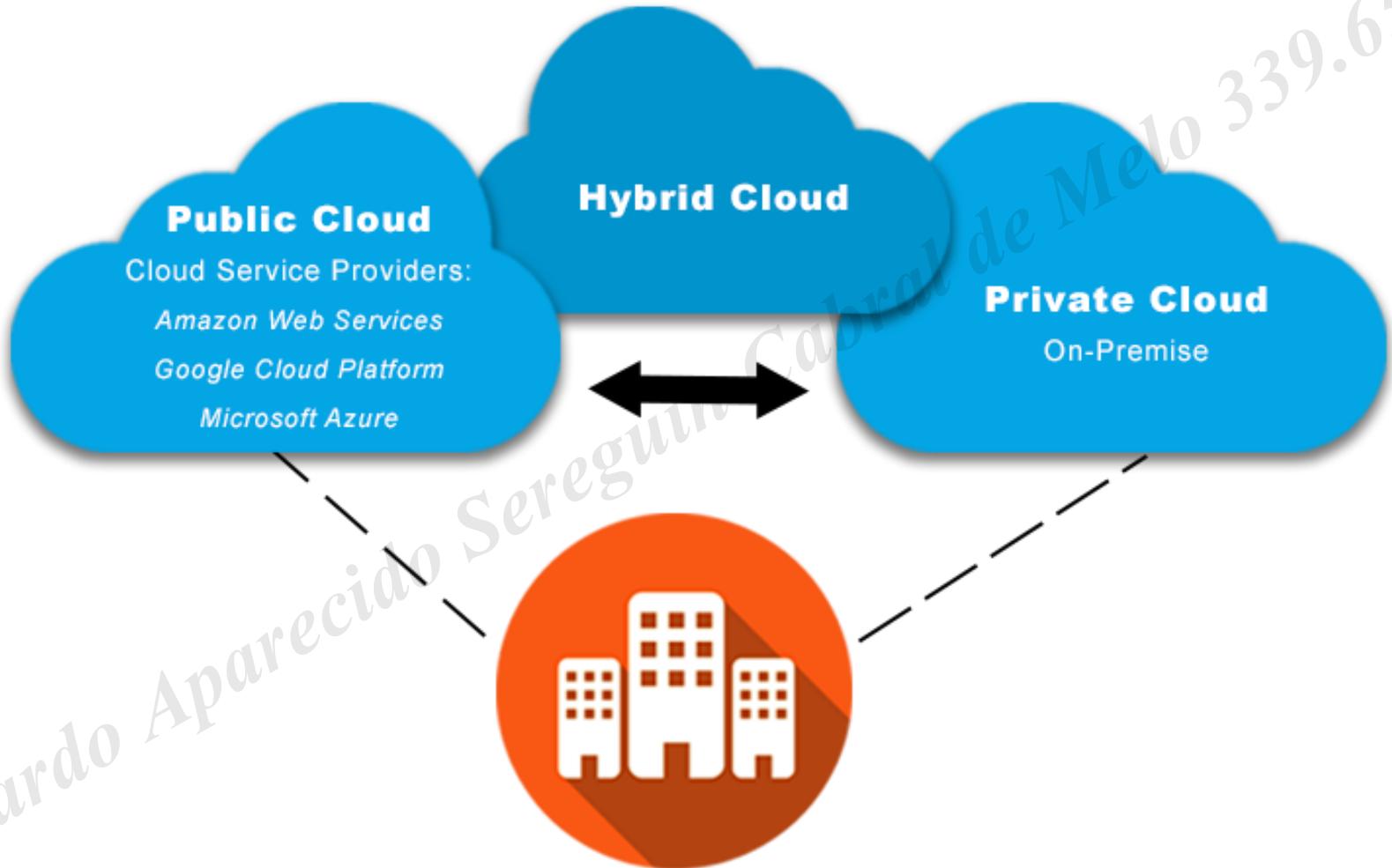
Democratization of technological resources



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization **is prohibited**.

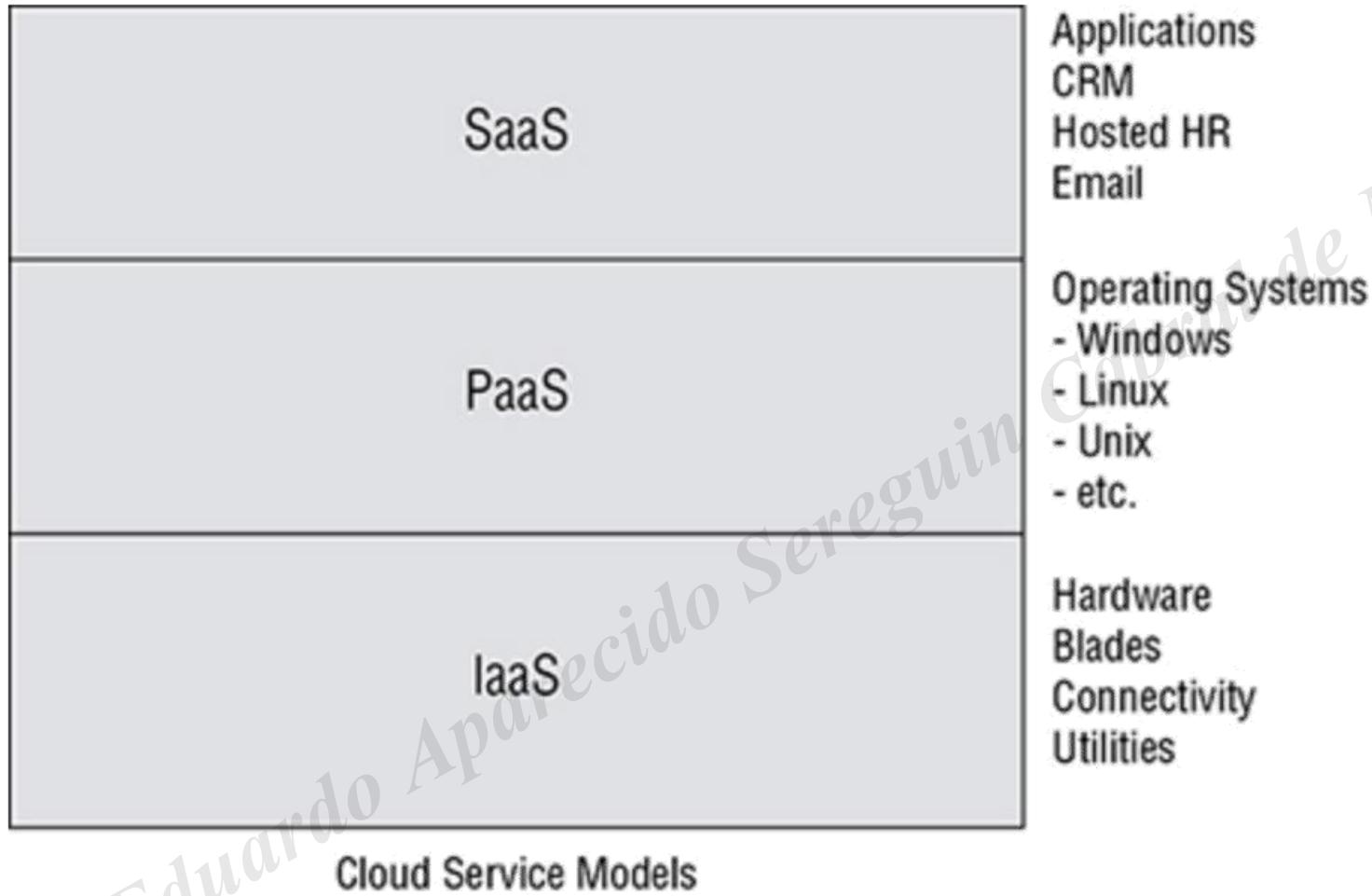
Hybrid Cloud



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

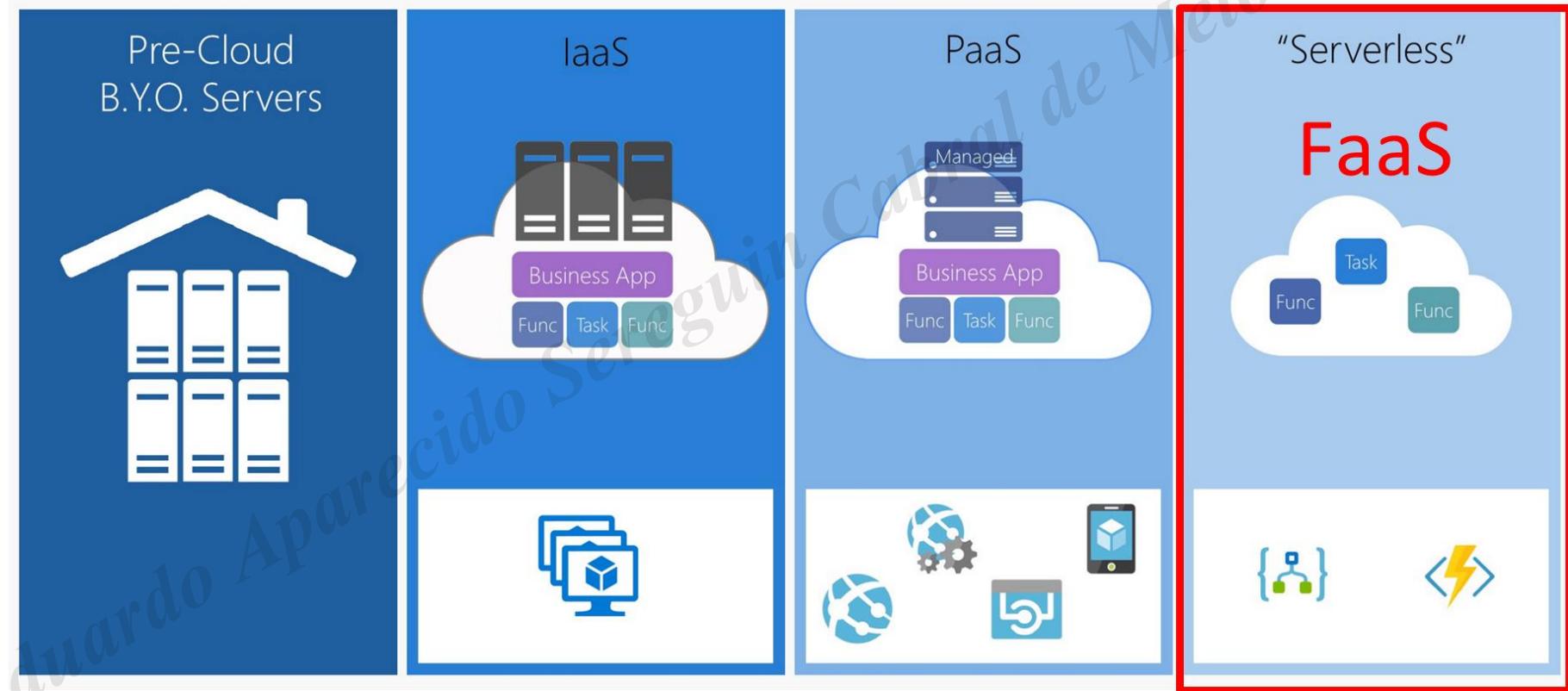
Cloud Service Models



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

FaaS – Function as a Service



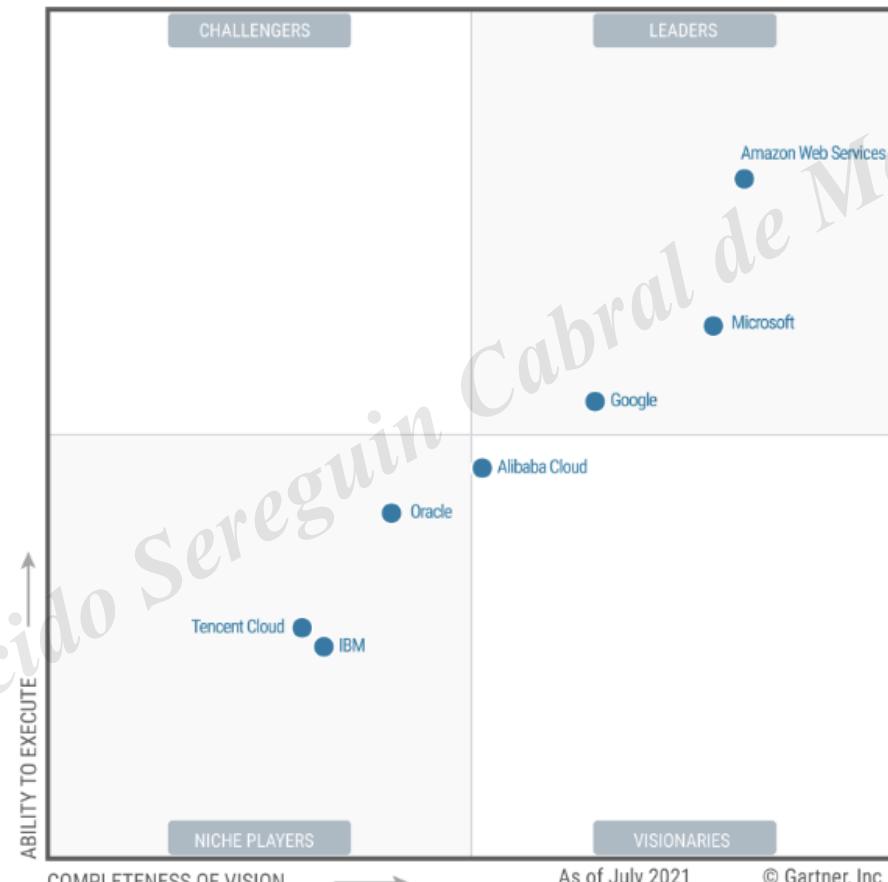
<https://medium.com/@oyetoketoby80/why-you-should-care-about-serverless-and-faas-6987c84eacb4>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Gartner Magic Quadrant IaaS

Figure 1: Magic Quadrant for Cloud Infrastructure and Platform Services



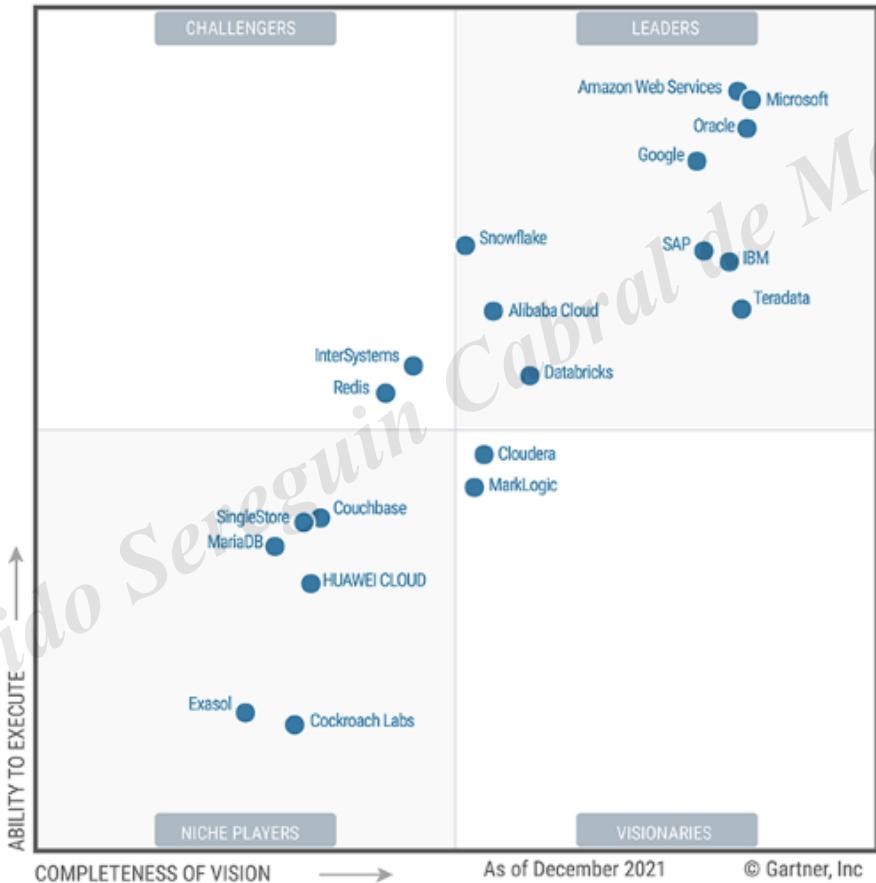
Source: Gartner (July 2021)

<https://aws.amazon.com/resources/analyst-reports/gartner-mq-cips-2021/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Gartner Magic DB MS

Figure 1: Magic Quadrant for Cloud Database Management Systems



<https://aws.amazon.com/blogs/database/aws-named-a-leader-in-2021-gartner-magic-quadrant-for-cloud-database-management-systems/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Gartner Magic CIPS

Figure 1: Magic Quadrant for Cloud Infrastructure and Platform Services



Source: Gartner (July 2021)

<https://aws.amazon.com/resources/analyst-reports/gartner-mq-cips-2021/>

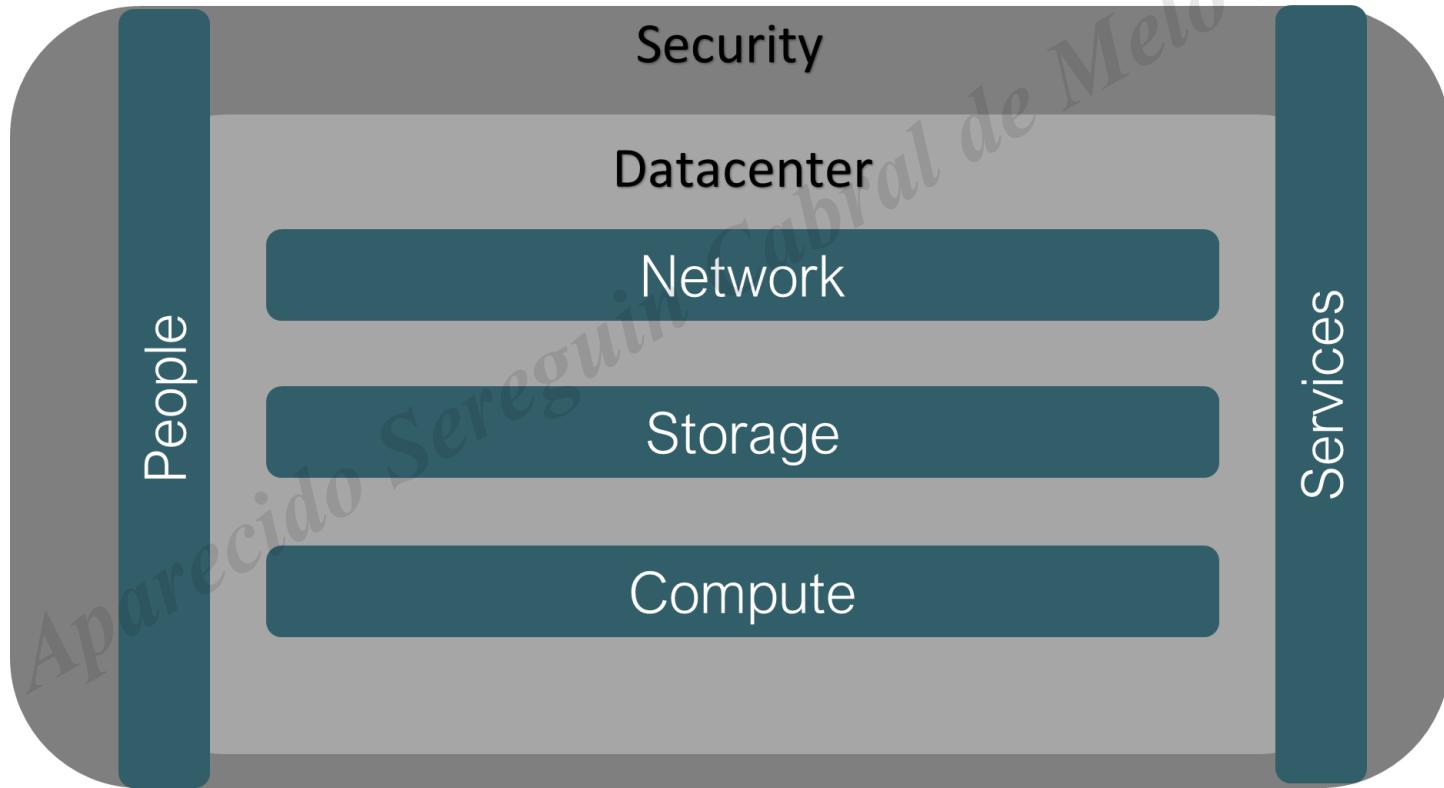
*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Forester Wave Cloud Data Warehouse



<https://aws.amazon.com/resources/analytical-report/the-fourth-wave-data-warehouse-2021/?profid=aa9f8d43cfbb11eca85b2cf38962fc07>

Cloud and its “lays”

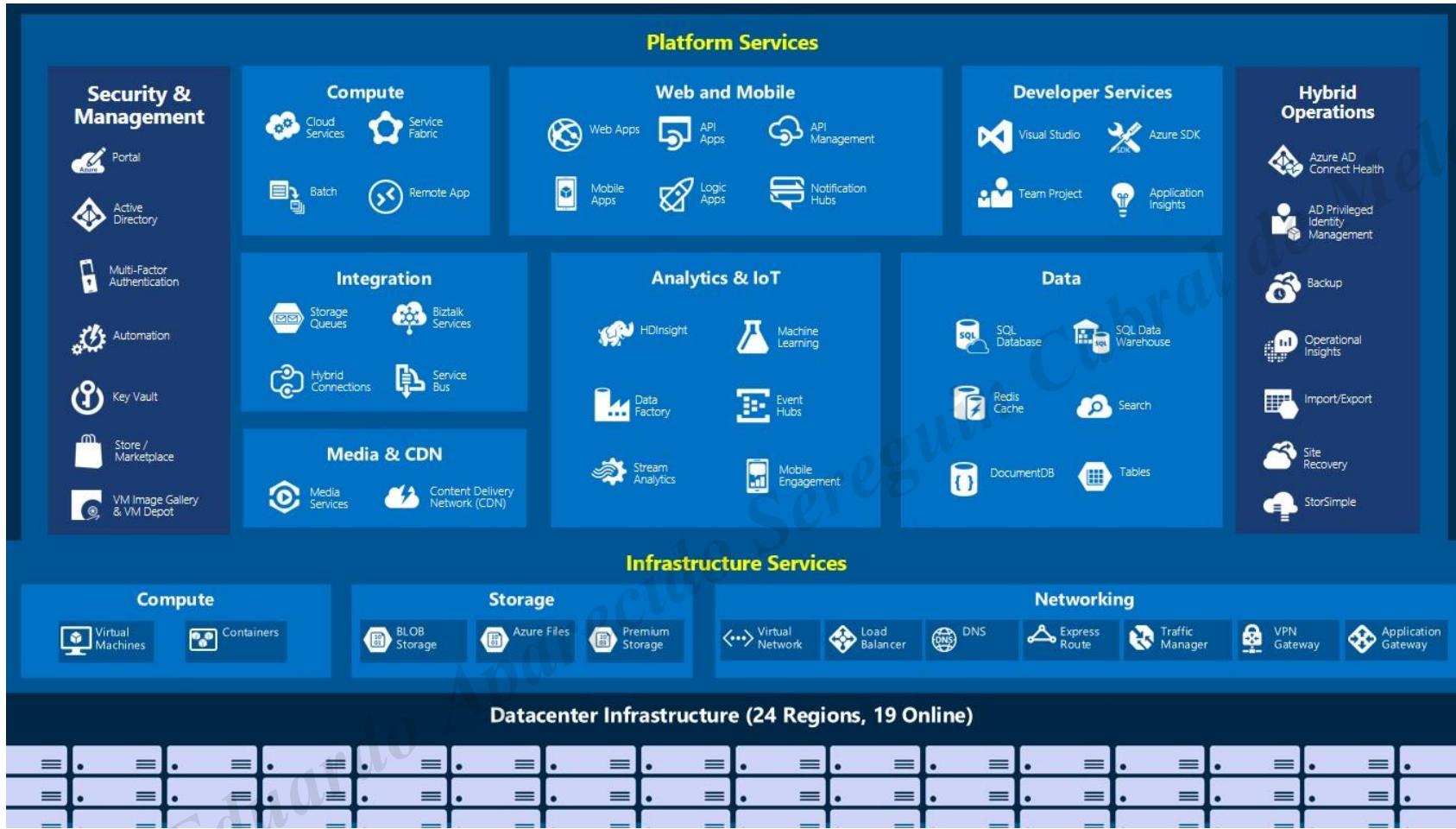


*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Public Cloud Services

Microsoft Azure

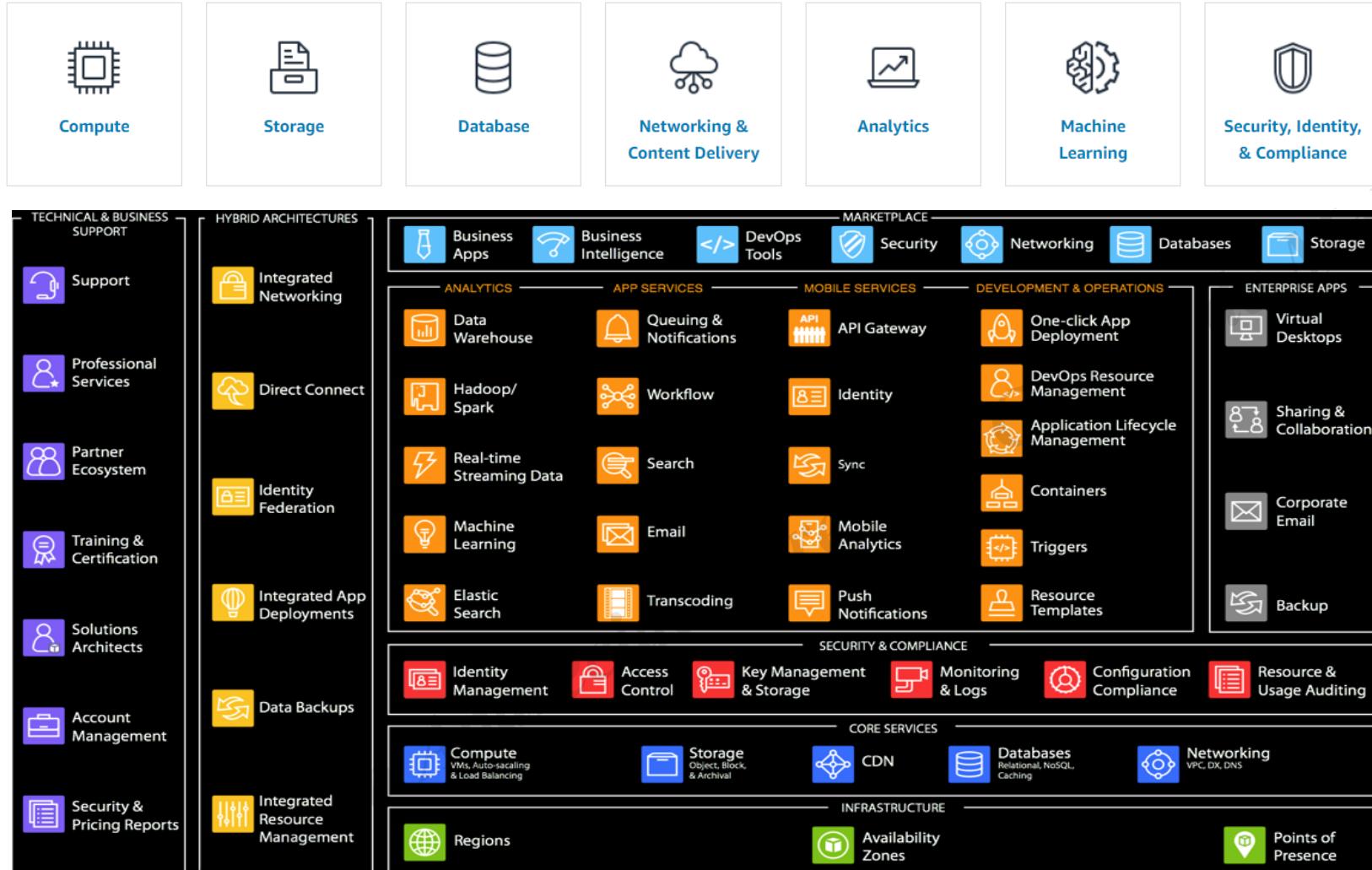


<https://azure.microsoft.com/en-us/services/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Public Cloud Services AWS



<https://aws.amazon.com/products/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc&awsf.re%3AIinvert=%2Aall&awsf.Free%20Tier%20Type=%2Aall&awsf.tech-category=%2Aall>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Must Read



ADOPTING HYBRID CLOUD BECOMES A STRATEGIC IMPERATIVE

<https://hbr.org/resources/pdfs/comm/insight/HBRASHybridCloud.pdf>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

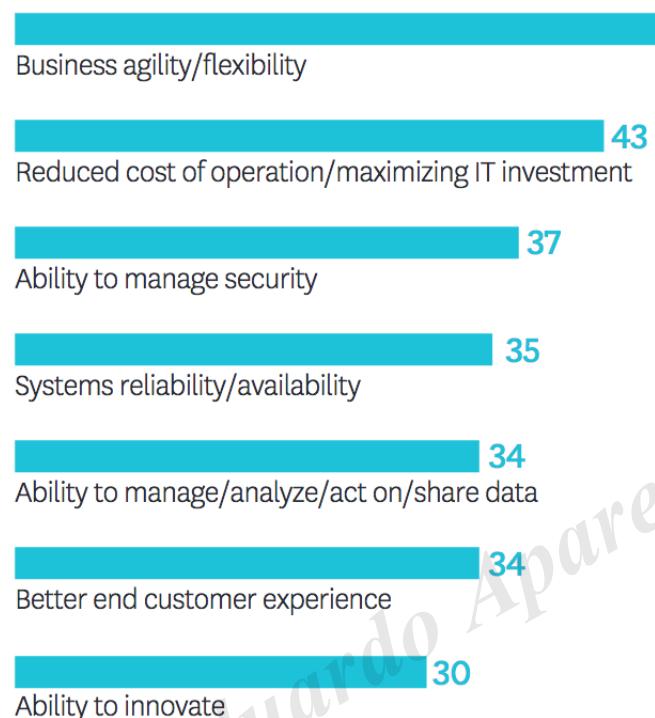
The total or partial reproduction of this material without authorization is prohibited.

Business Drivers

FIGURE 1

BUSINESS DRIVERS

Percentage saying the following business demands are driving or would drive their organization toward the adoption of more cloud systems or a hybrid cloud architecture



SOURCE HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, FEBRUARY 2017

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

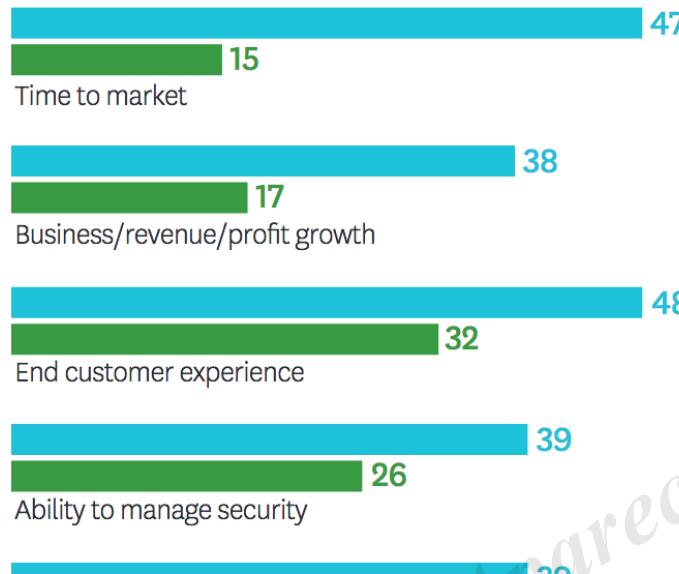


SMBs x Enterprises

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

● SMALL BUSINESSES ● LARGE ENTERPRISES



SOURCE HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, FEBRUARY 2017



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

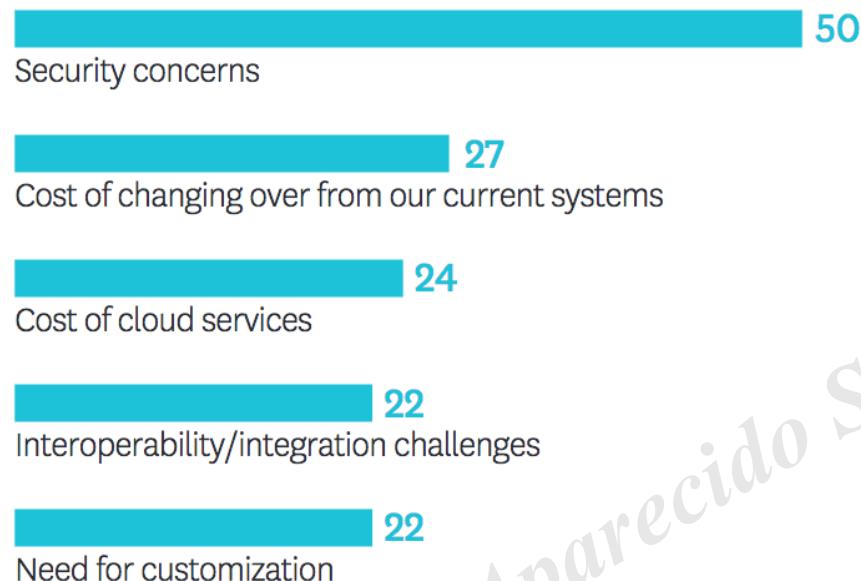
The total or partial reproduction of this material without authorization is prohibited.

Barriers

FIGURE 7

CLOUD BARRIERS

Percentage citing the following as barriers to fully embracing cloud systems



SOURCE HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, FEBRUARY 2017



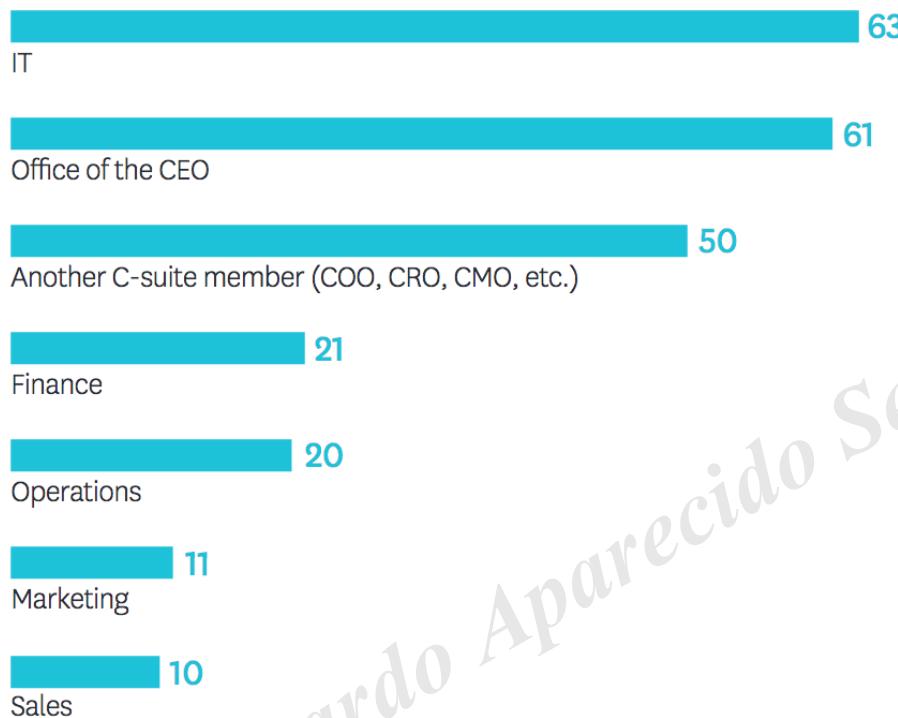
*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Who decides?

FIGURE 11

CLOUD DECISION MAKERS

Percentage saying the following have decision-making power regarding cloud computing investments



SOURCE HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, FEBRUARY 2017

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.



Drivers for cloud adoption

1. Greater agility.
2. Stop guessing capacity.
3. Change in the cost structure.
4. Fail Fast and innovate more.
5. Globalization in business.
6. Access innovative technology and services.

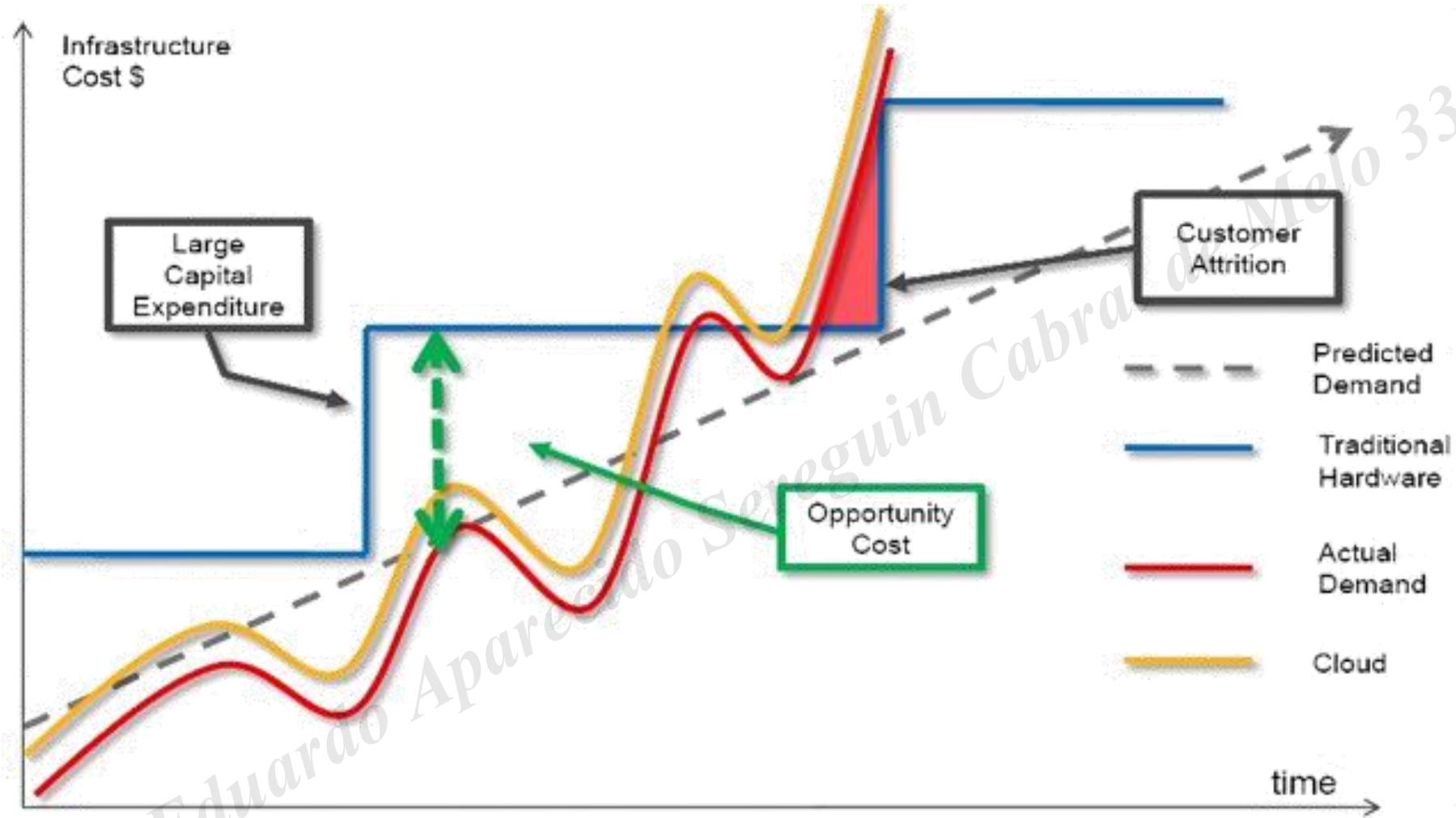


CapEx vs. OpEx



???

Cost Efficiency



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Only foreigners ???

Highly regulated environment



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

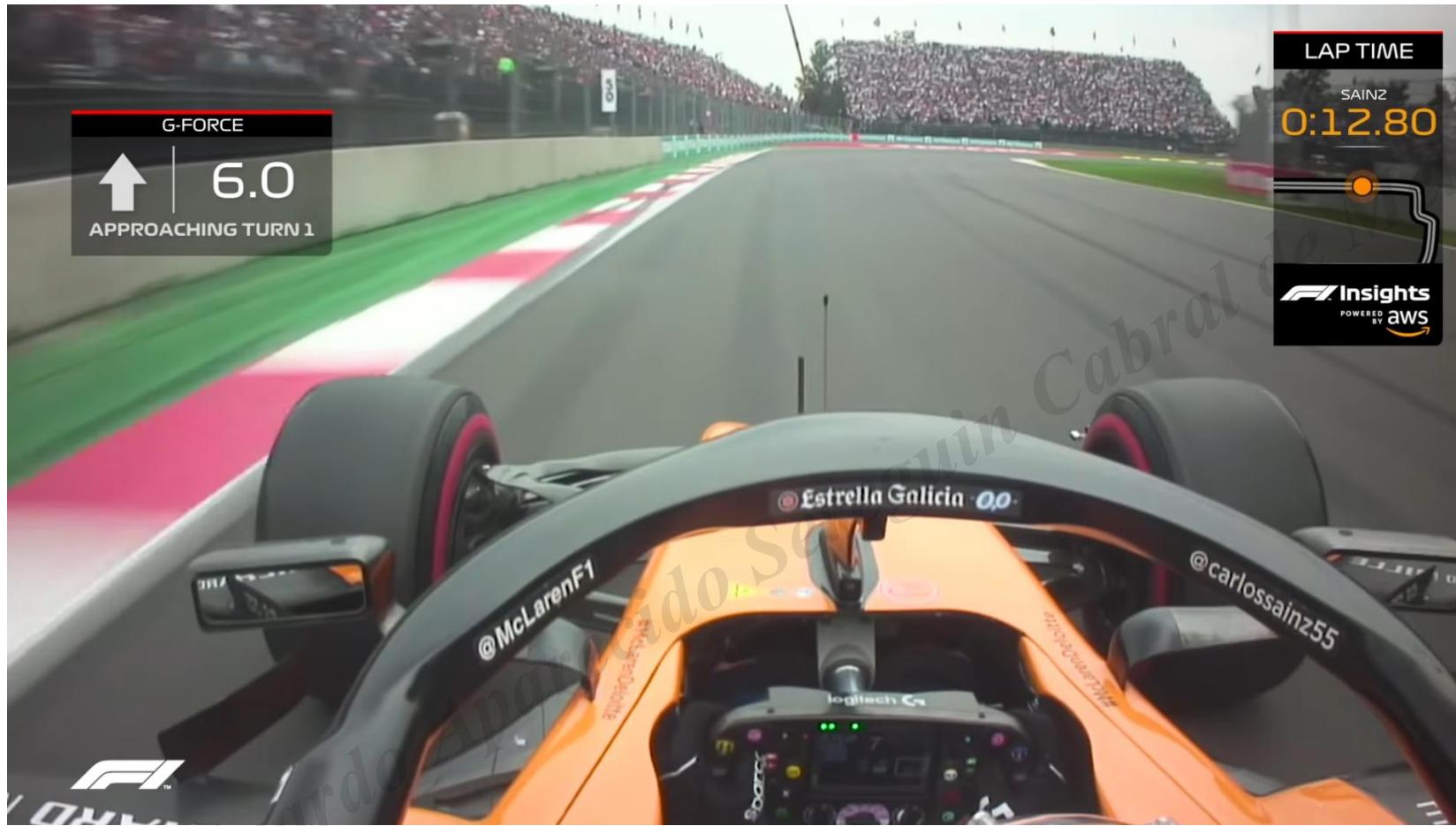
Any industry?

96% of productivity



ICON is our software that pairs up
with every single airplane around the world.

Entertainment?



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Entertainment?



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Several segments

Microsoft Microsoft 365 Azure Office 365 Dynamics 365 Power Platform Windows 10 Toda a Microsoft Pesquisar Carrinho Entrar

Histórias de clientes Pesquisar

Pesquisar histórias de clientes

Pesquisar histórias de clientes Classificar por

Limpar filtros

Idioma

Setor

Produto

Tamanho da organização

Região

GrupoFleury
Provedor da saúde
Com Dynamics 365, Grupo Fleury leva sua cultura de excelência no atendimento para a esfera digital

natura
Varejo
Com Dynamics 365, Natura dá robustez ao seu atendimento e mantém relação com os clientes

ame
Setor bancário e Mercados de capitais
Ame Digital aprimora coleta de dados e agiliza o desenvolvimento de aplicativos com Data Lake corporativo

TIGRE
Outros
Grupo Tigre implementa novas técnicas de Analytics com suporte da Nuvem Microsoft

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Class Agenda

2

SofA and migration plan

Cloud Adoption Framework

Microsoft

The screenshot shows the Microsoft Cloud Adoption Framework for Azure landing page. At the top, there's a navigation bar with links for Microsoft, Docs, Documentação (underlined), Learn, Q&A, Exemplos de Código, Pesquisar, Portal, Conta gratuita, Indicador, and Compartilhar. Below the navigation is a search bar with placeholder text "Pesquisar". The main title "Microsoft Cloud Adoption Framework for Azure" is displayed in a large white font on a dark blue background. A sub-headline in smaller white text reads: "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." Below this, there are four cards: "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), and "NOVIDADES" (Novidades no Cloud Adoption Framework). Further down, a section titled "Diretrizes do Cloud Adoption Framework" is shown, with three cards: "Introdução" (Documentar as decisões fundamentais, Acelerar a migração, Fornecer excelência operacional, Alinhar sua organização), "Estratégia" (Motivações, Resultados dos negócios, Alinhar sua estratégia de parceiros, Escolha o primeiro projeto certo), and "Plano" (Racionalizar seu acervo digital, Alinhamento da organização, Plano de preparação de habilidades, Plano de adoção de nuvem para DevOps).

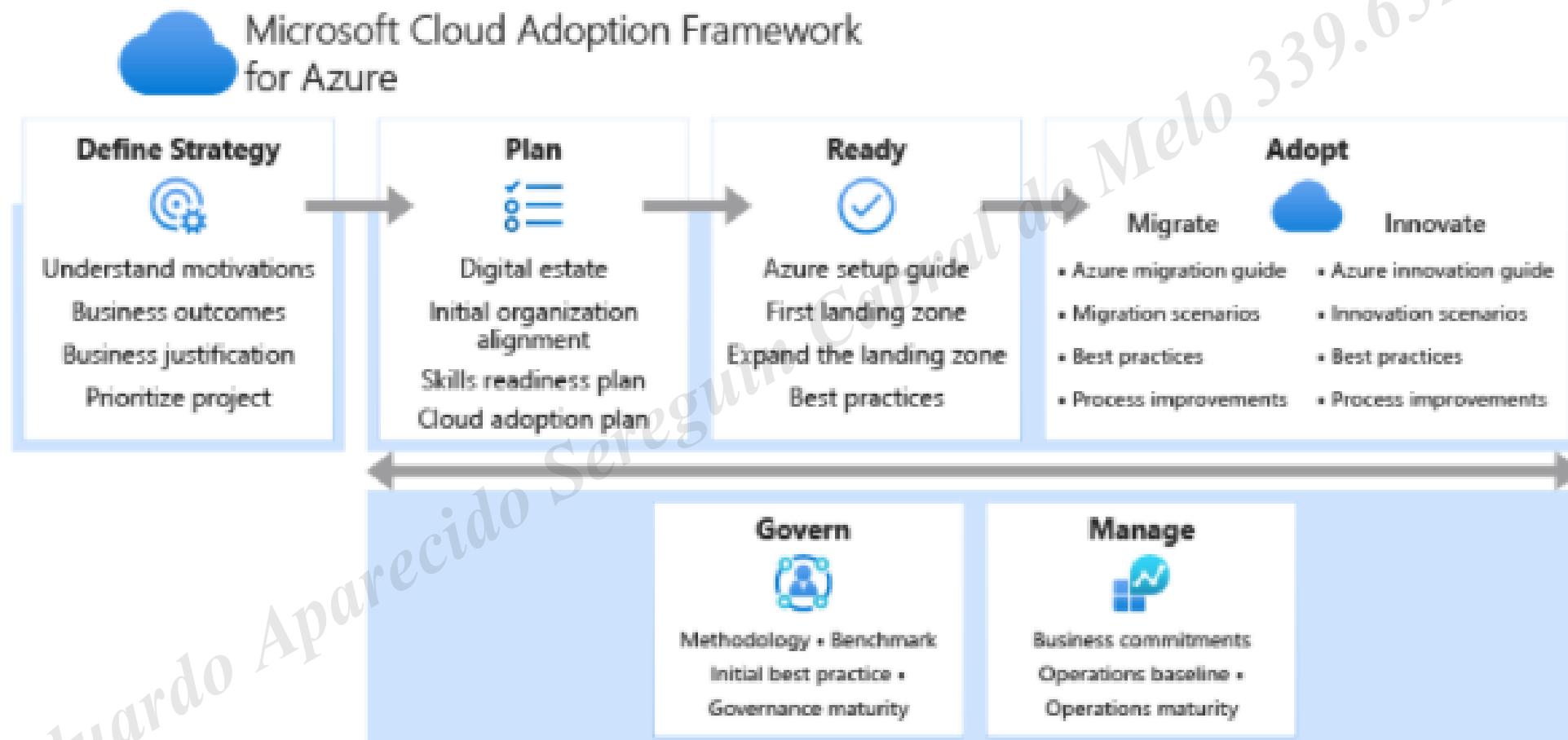
<https://bit.ly/2Yolmdn>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Cloud Adoption Framework

Microsoft



[Microsoft Cloud Adoption Framework for Azure documentation - Cloud Adoption Framework | Microsoft Docs](#)

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Well Architecture Framework

Cost Optimization



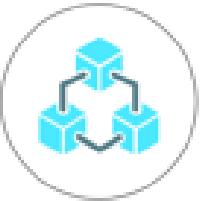
Operational Excellence



Efficiency of Performance



Reliability



Security



- ✓ Azure Hybrid Benefit
- ✓ Reserved Instances
- ✓ Separation
- ✓ Resize
- ✓ Move to PaaS

- ✓ Devops
- ✓ Implementation
- ✓ Monitor
- ✓ Processes and Chaining

- ✓ Design for sizing
- ✓ Monitor the performance

- ✓ Define requirements
- ✓ Test with simulations and forced failovers
- ✓ Implement consciously
- ✓ Monitor health
- ✓ Respond to the failure and disaster

- ✓ Management of identity and access
- ✓ Protection against attacks
- ✓ App security
- ✓ Cryptography of data and sovereignty
- ✓ Security operations

<https://aka.ms/architecture/framework>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Well-Architected Review



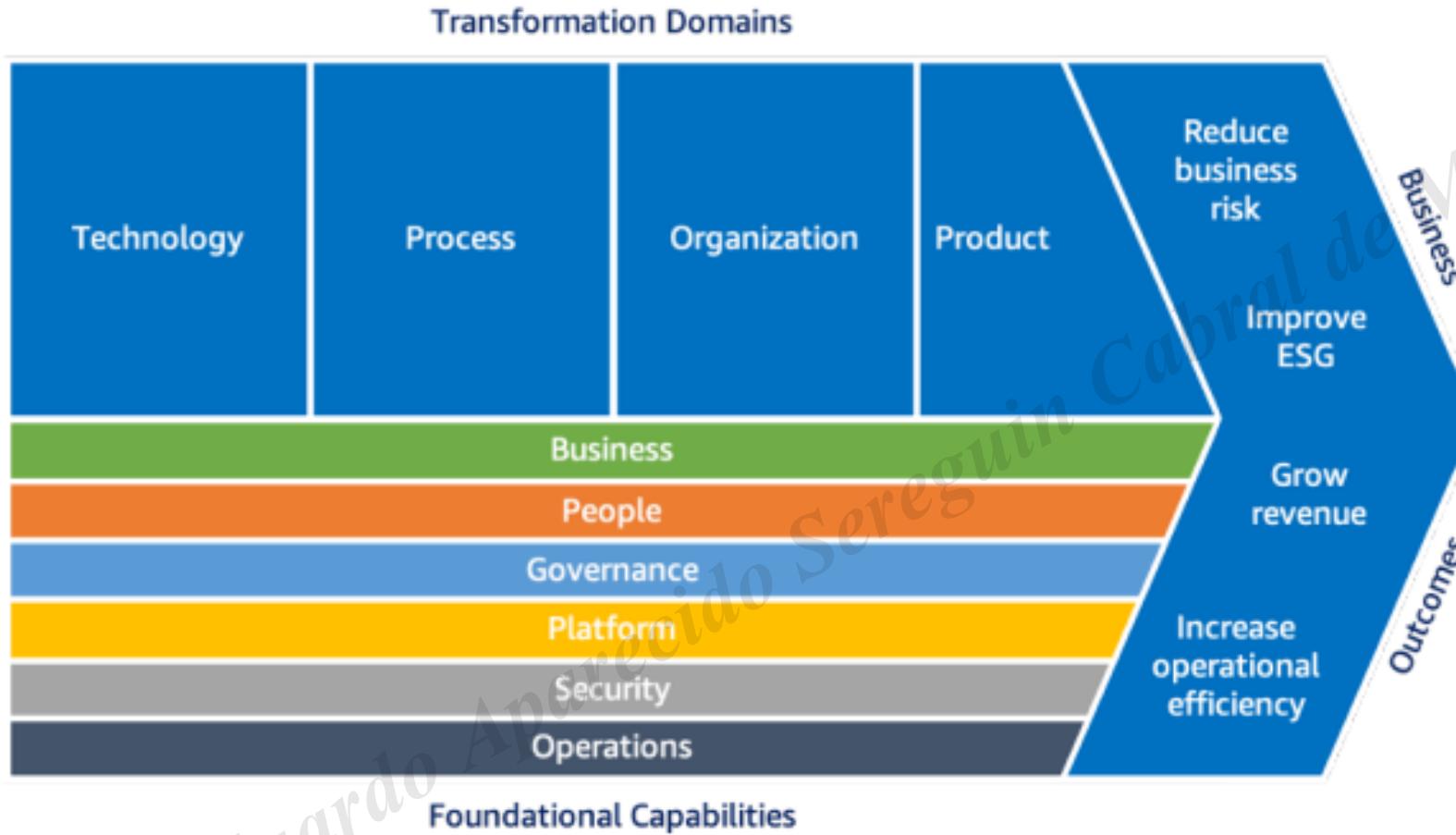
<https://aka.ms/architecture/review>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Cloud Adoption Framework

AWS

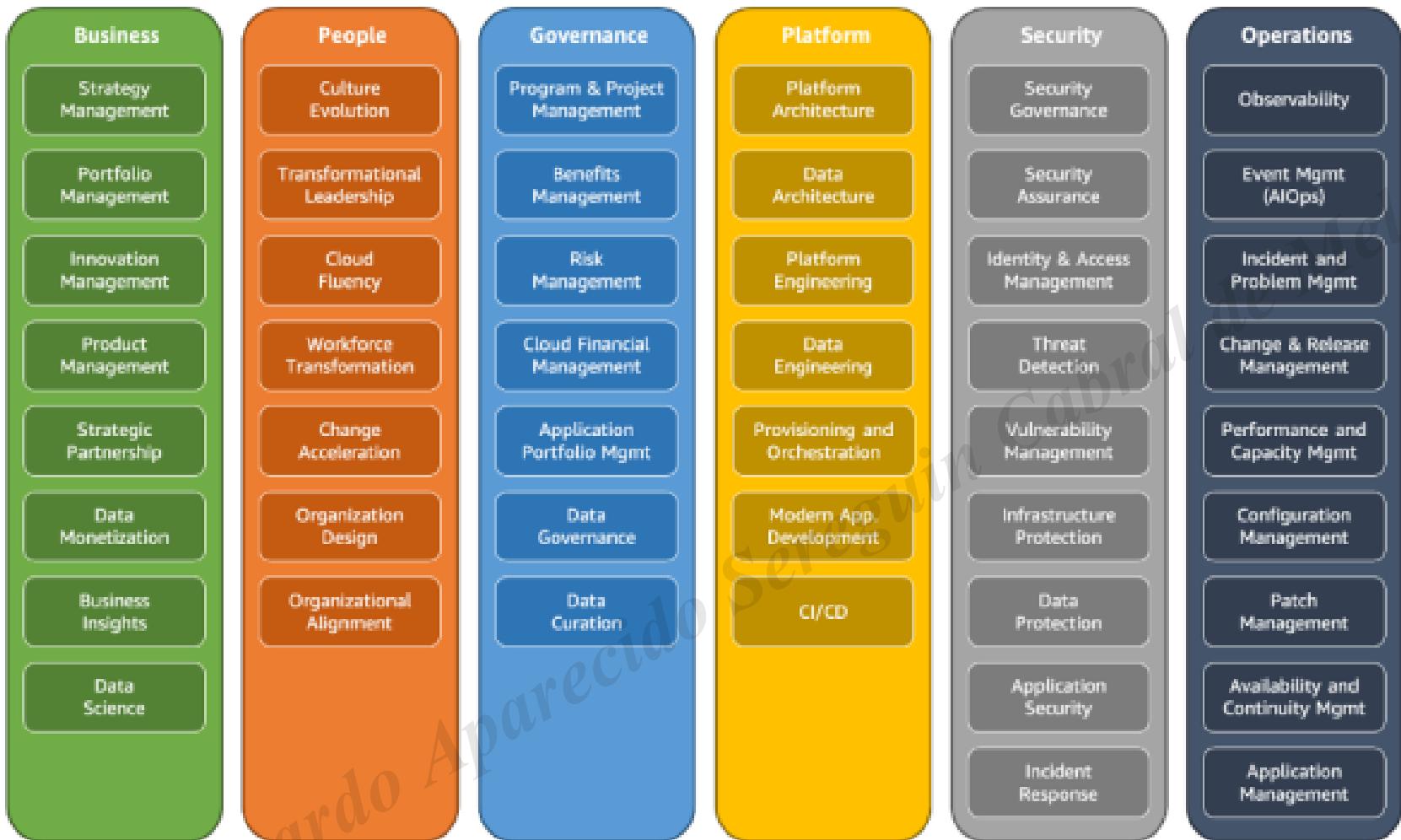


<https://aws.amazon.com/pt/professional-services/CAF/>

https://d1.awsstatic.com/whitepapers/pt_BR/aws-cloud-adoption-framework_pt-BR.pdf

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

CAF - AWS

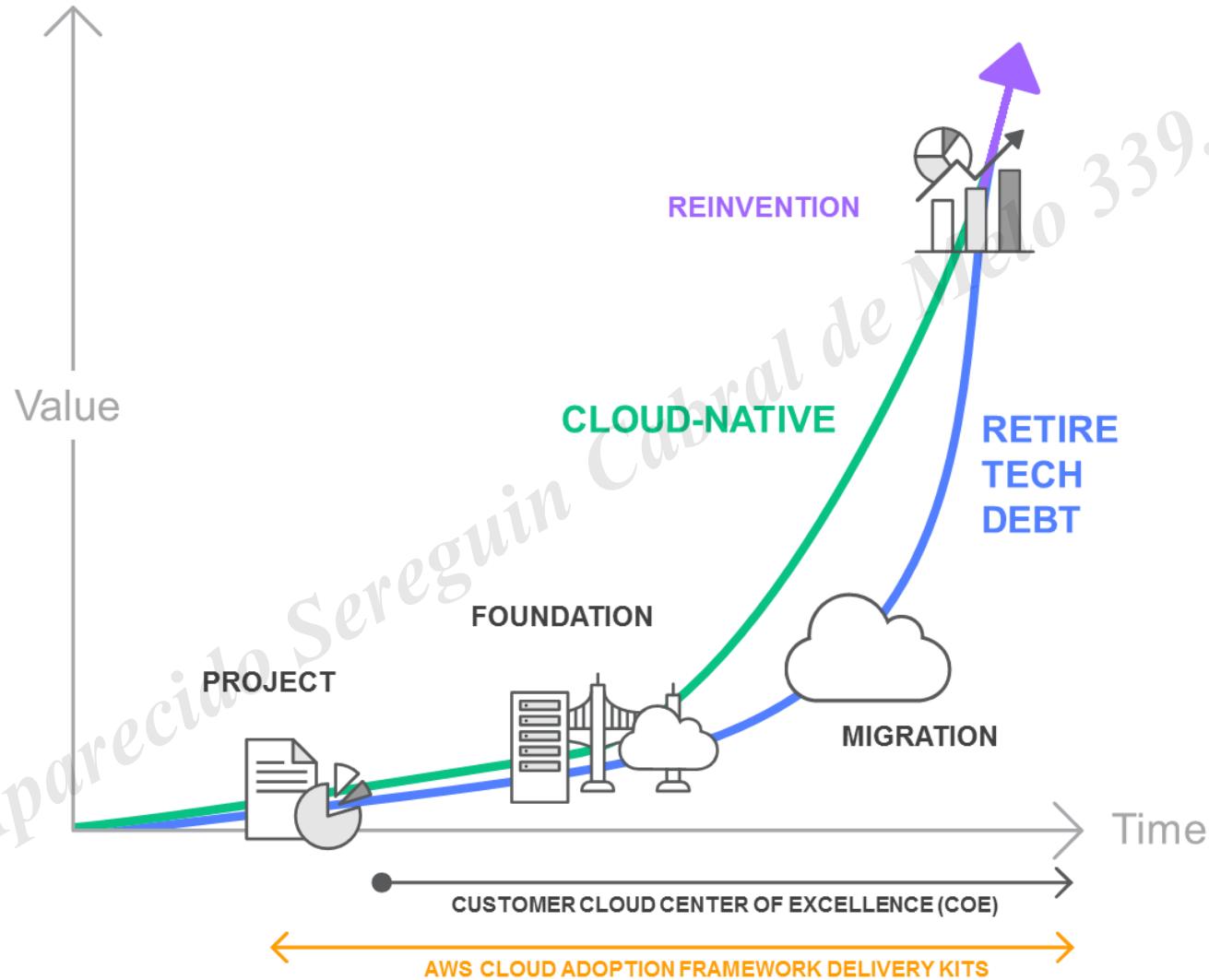


https://d1.awsstatic.com/whitepapers/pt_BR/aws-cloud-adoption-framework_pt-BR.pdf

<https://aws.amazon.com/pt/professional-services/CAF/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

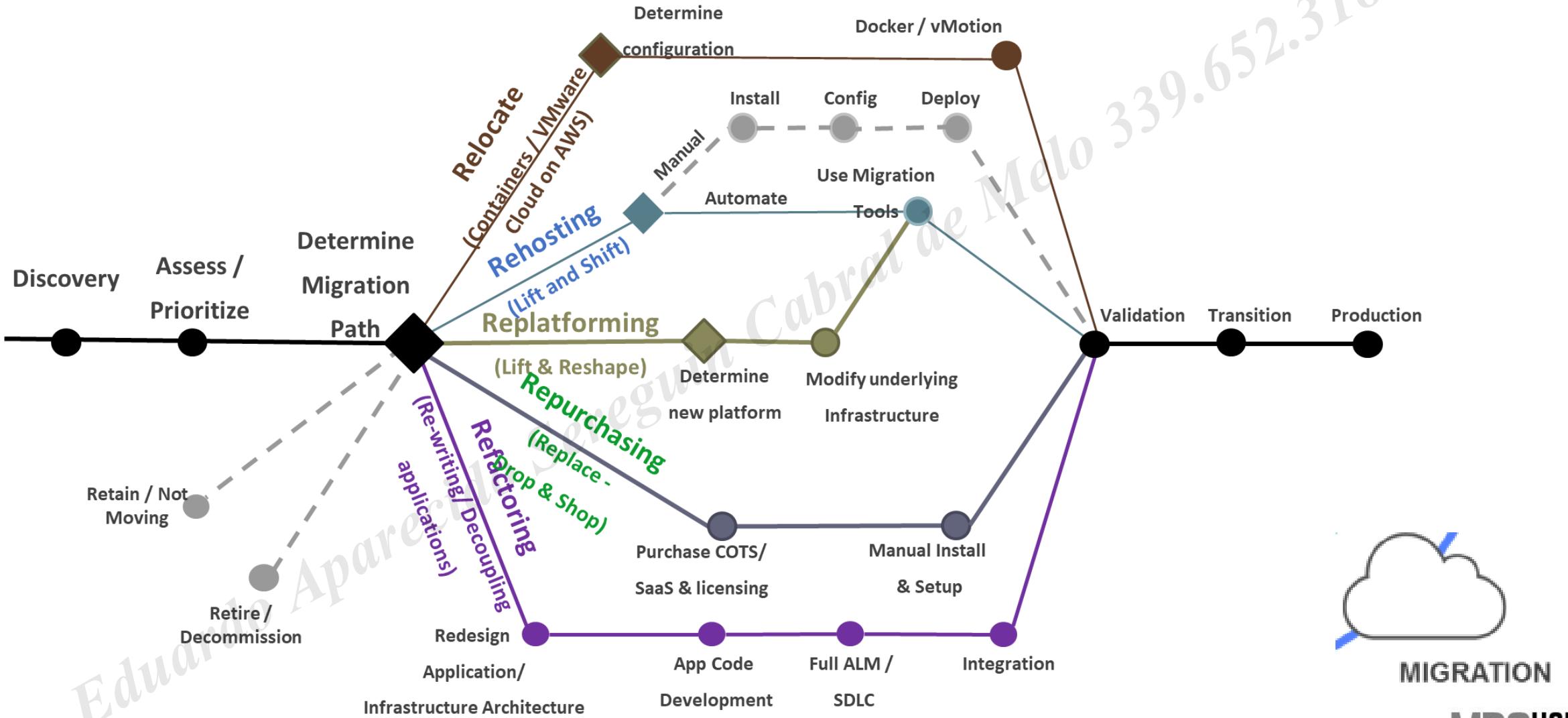
Cloud SofA – Stage of Adoption



<https://aws.amazon.com/blogs/enterprise-strategy/capital-ones-cloud-journey-through-the-stages-of-adoption/>

The total or partial reproduction of this material without authorization is prohibited.

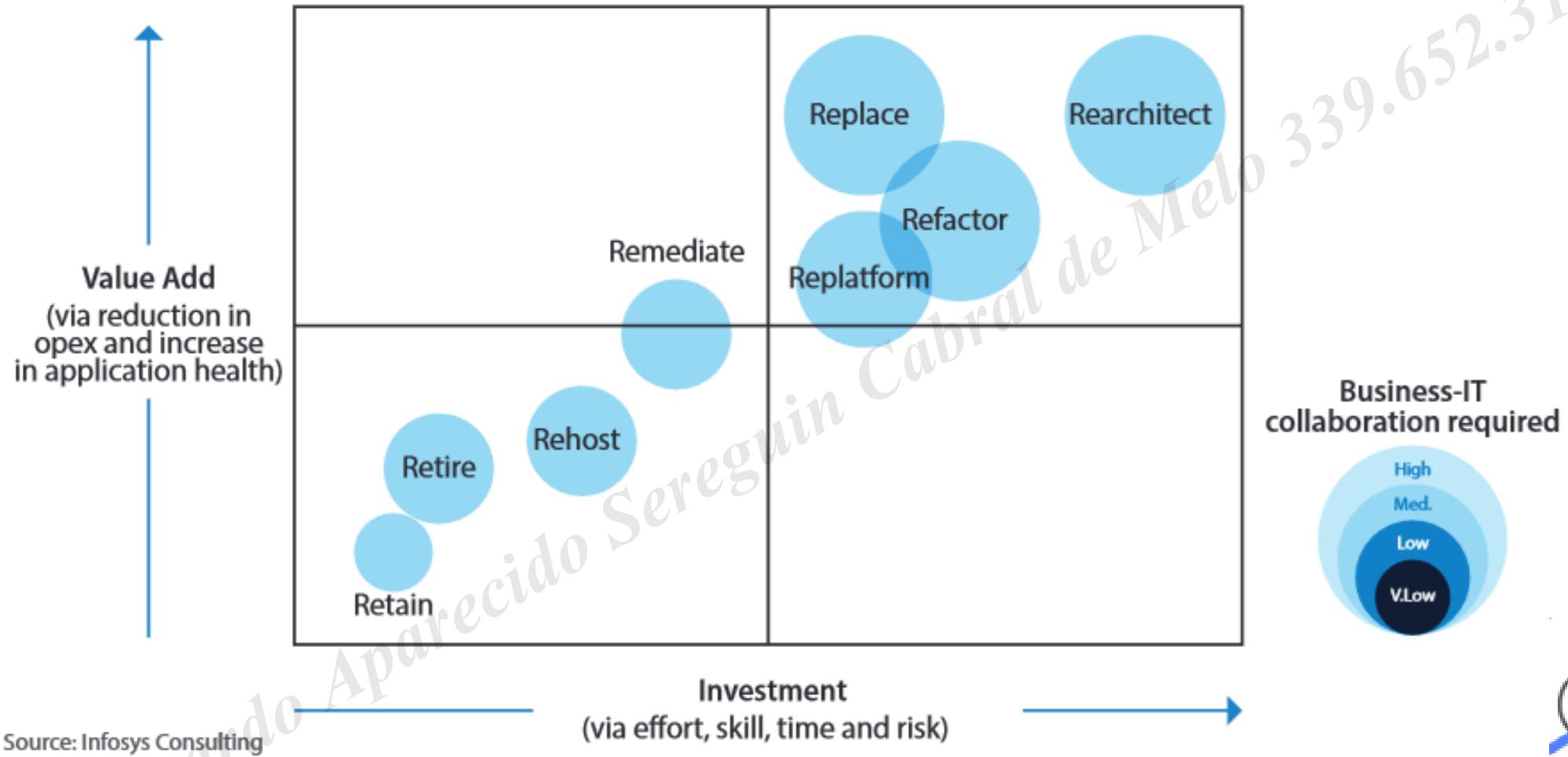
Migration strategies



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Migration strategies



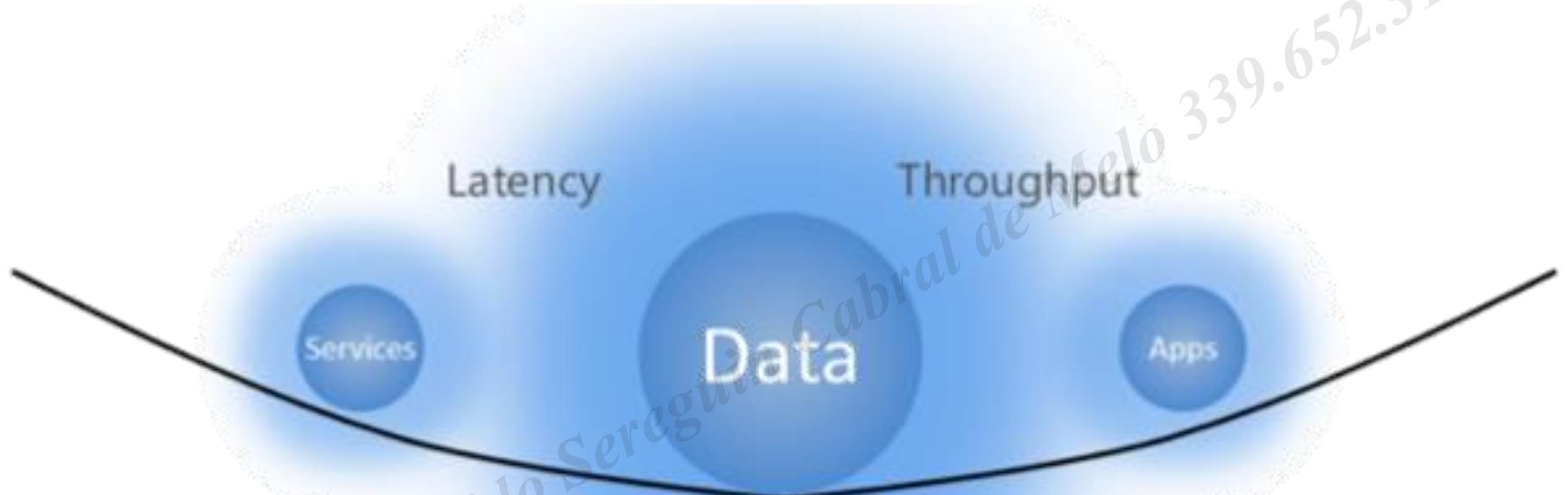
<https://infy.com/3fg8pKT>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.



Data severity



How to migrate large volumes of data?

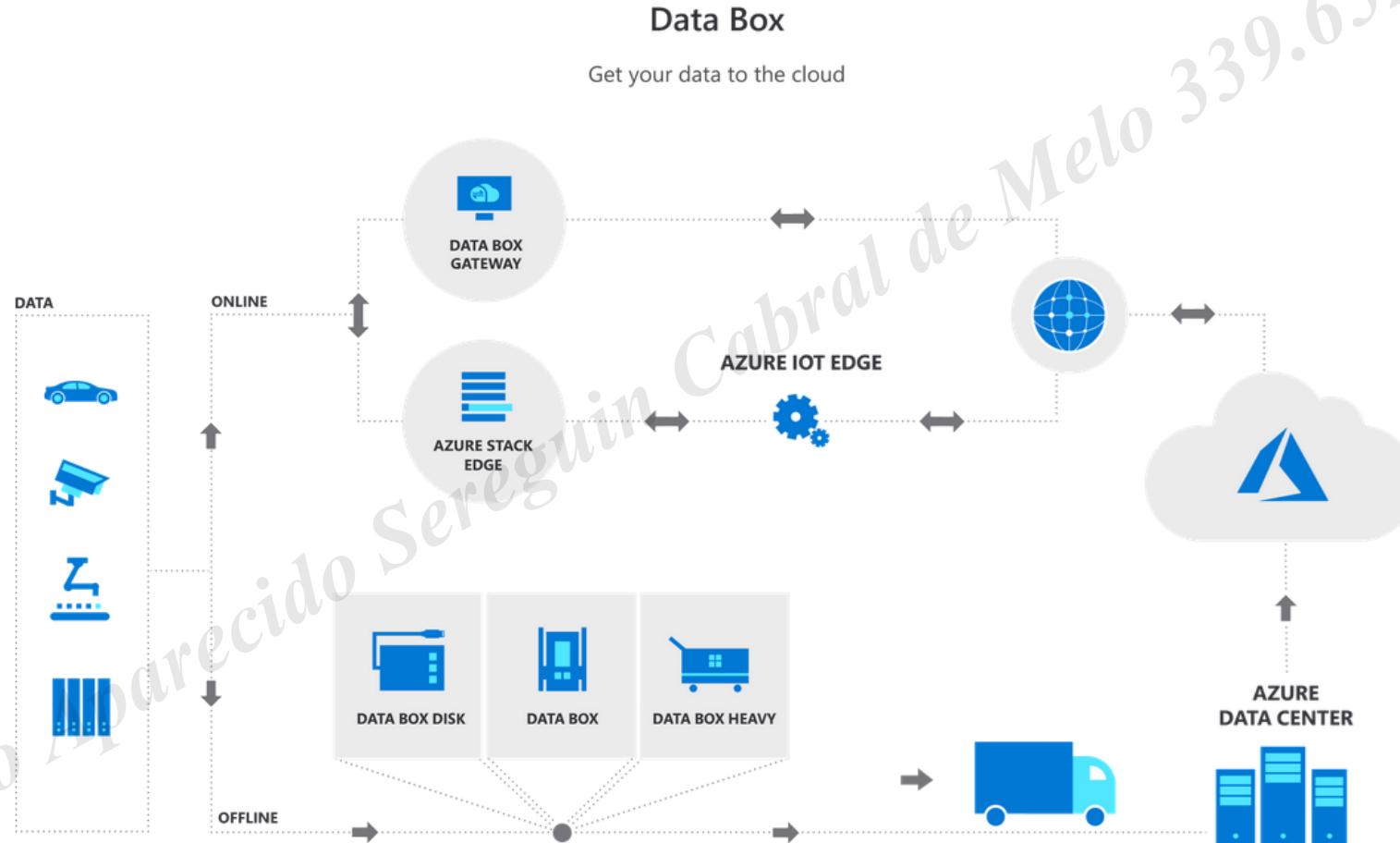


<https://go.aws/2MJKgQu>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization **is prohibited**.

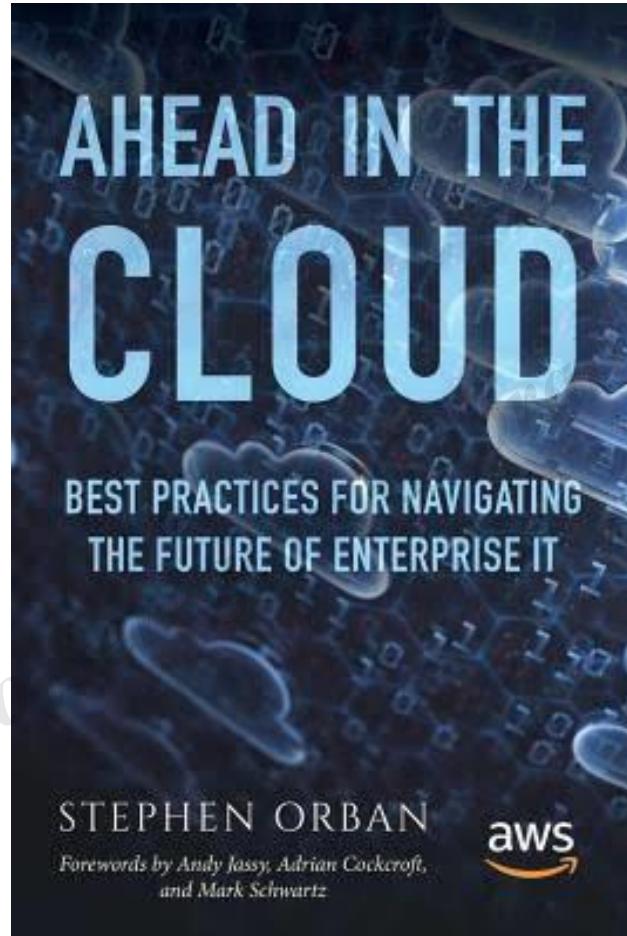
How to migrate large volumes of data?



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Recommended book

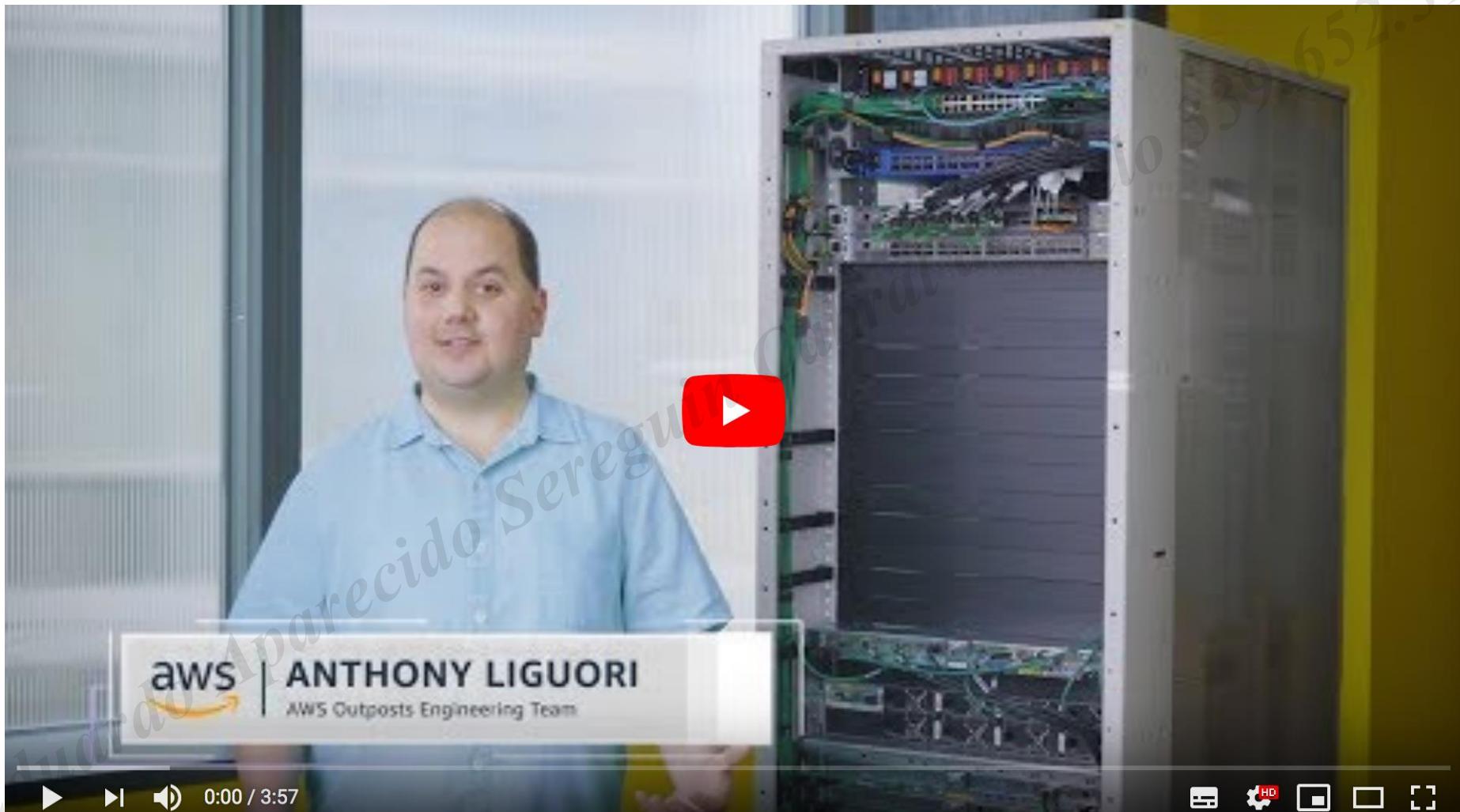


<https://amzn.to/3fdeI1H>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

The Cloud in your Datacenter



<https://bit.ly/3cS5erd>

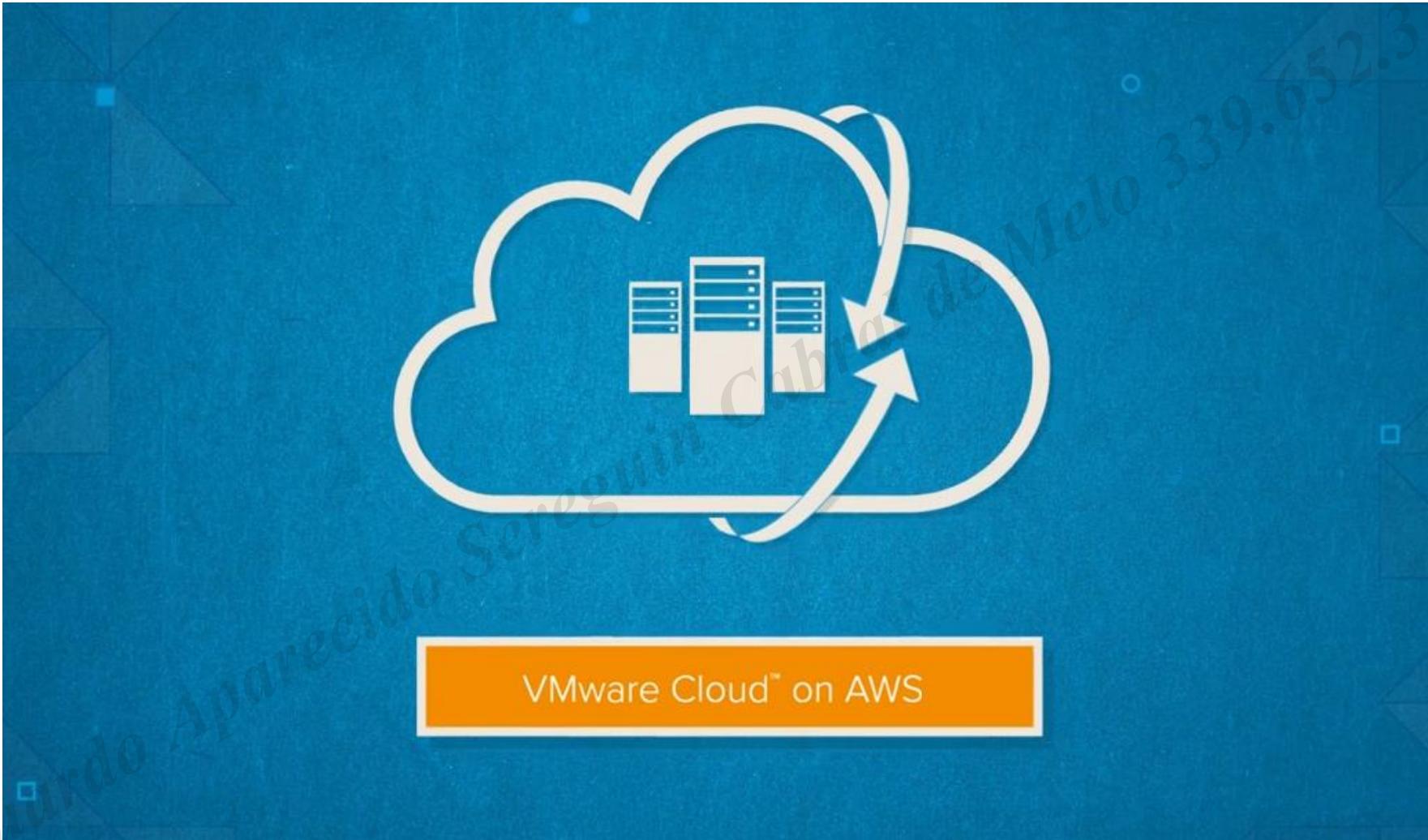
*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

The Cloud in your Datacenter

Azure Stack is an extension of Azure

Vmware Hybrid Cloud



<https://bit.ly/3hjFGGD>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Vmware Hybrid Cloud

Azure VMware Solution

Run your VMware workloads natively on Azure

Contact sales

Product overview Features Security Pricing Documentation Customer stories FAQs

Move or extend on-premises VMware environments to Azure

Seamlessly move VMware-based workloads from your datacenter to Azure and integrate your VMware environment with Azure. Keep managing your existing environments with the same VMware tools you already know while you modernize your applications with Azure native services. Azure VMware Solution is a Microsoft service, verified by VMware, that runs on Azure infrastructure.

VMWARE CLOUD VERIFIED

<https://azure.microsoft.com/en-us/services/azure-vmware/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Class Agenda

3

Security OF X IN Cloud

What is the role of security?

“CIOs and CISOs need to stop obsessing over unsubstantiated cloud security worries, and instead apply their imagination and energy to developing new approaches to cloud control, allowing them to securely, compliantly and reliably leverage the benefits of this increasingly ubiquitous computing model.”

Jay Heiser

Clouds Are Secure: Are You Using Them Securely?

Published: 22 September 2015

Gartner.

Do not be Dr. NO



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

It is no longer a choice



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Cloud brings advantages for Data Security

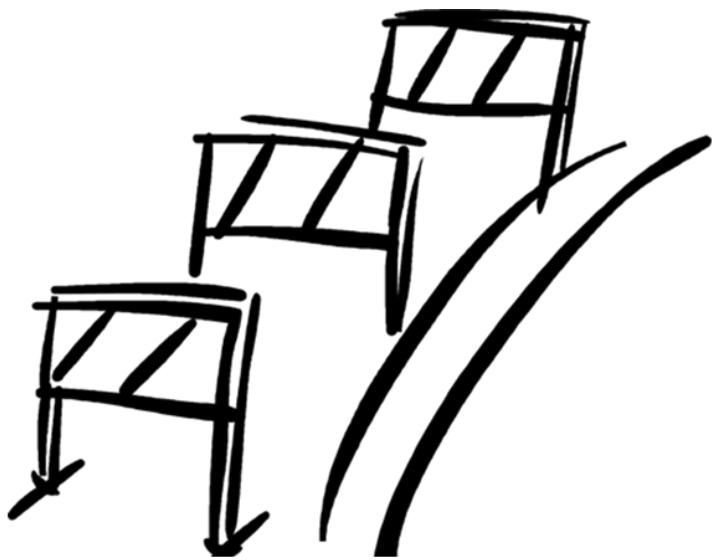
Traditional Environment

1. Big investments Upfront.
2. It takes a lot of time to implement.
3. Impact in the performance, damaging the use and business.
4. Manual process, little automated, not scalable.

Cloud

1. Native solutions, without extra cost, or in the model Pay as you Go.
2. Native security solutions that can be implemented only clicks away without damaging the use and business.
3. Automation of complex processes and scalable security solutions.
4. Use of cloud technologies for the cloud protection.

Use cloud is also positive for SI



Different
Layers

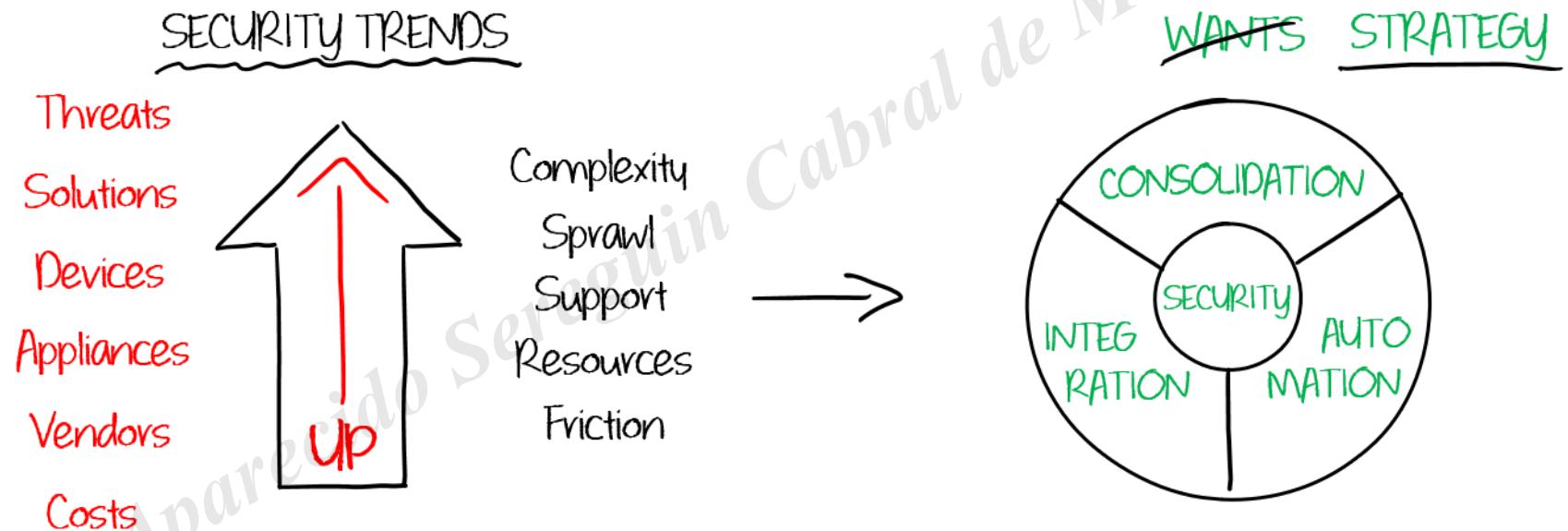


Validation
by Third
parties



Global
Presence

Cloud Cyber Security



Two keywords



Visibility



Automation

Cryptography in Scale

Volume Encryption

Disk Encryption
(EBS)

Files

Partner solutions/
Marketplace

Object Encryption

S3 Server Side
Encryption (SSE)

S3 SSE with clients keys

Client-side Encryption

Database Encryption

MSSQL

ORACLE

MYSQL

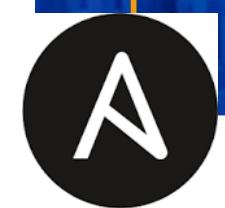
PostgreSQL

Redshift

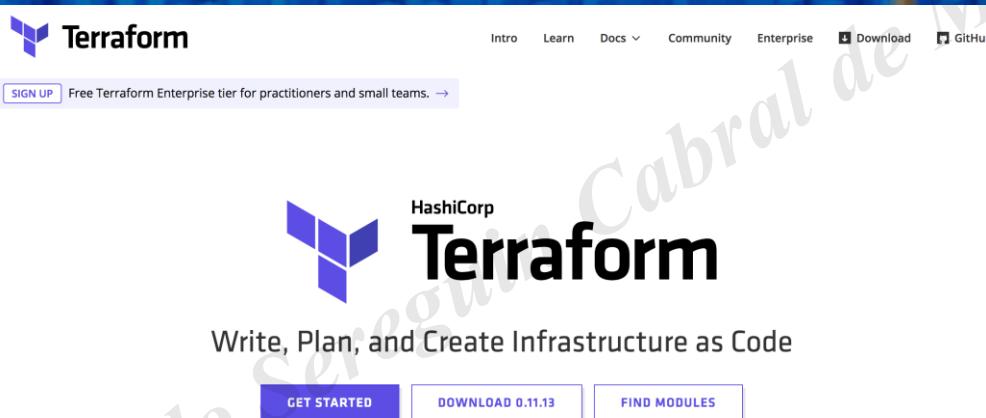
Technologies available only a click away

- WAF
- Firewall
- ML / AI
- IAM
- Full Logs
- MFA
- Cryptography in Scale
- Incident response automation
-

Security by Design / Security as code



ANSIBLE



- Regras de Firewall
- Somente uso de imagens de servidores seguras e autorizadas
- Configurações corretas a prova de erros
- Full DevSecOps



Azure Resource Manager templates

ARM stands for **Azure Resource Manager**. It's an API provisioning engine that is built into Azure and exposed as an API service. ARM enables you to deploy, update, delete, and manage the resources contained in Azure resource group in a single, coordinated operation. You provide the engine with a JSON-based template that specifies the resources you require and their configuration. ARM automatically orchestrates the deployment in the correct order respecting dependencies. The engine ensures idempotency. If a desired resource already exists with the same configuration, provisioning will be ignored.

Azure Resource Manager templates are a JSON-based language for defining various resources in Azure. The basic schema looks something like Figure 10-14.

```
JSON
{
  "schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "",
  "apiProfile": "",
  "parameters": { },
  "variables": { },
  "functions": [ ],
  "resources": [ ],
  "outputs": { }
}
```

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Democratization of security resources



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization **is prohibited**.

I may be more Safe but ...

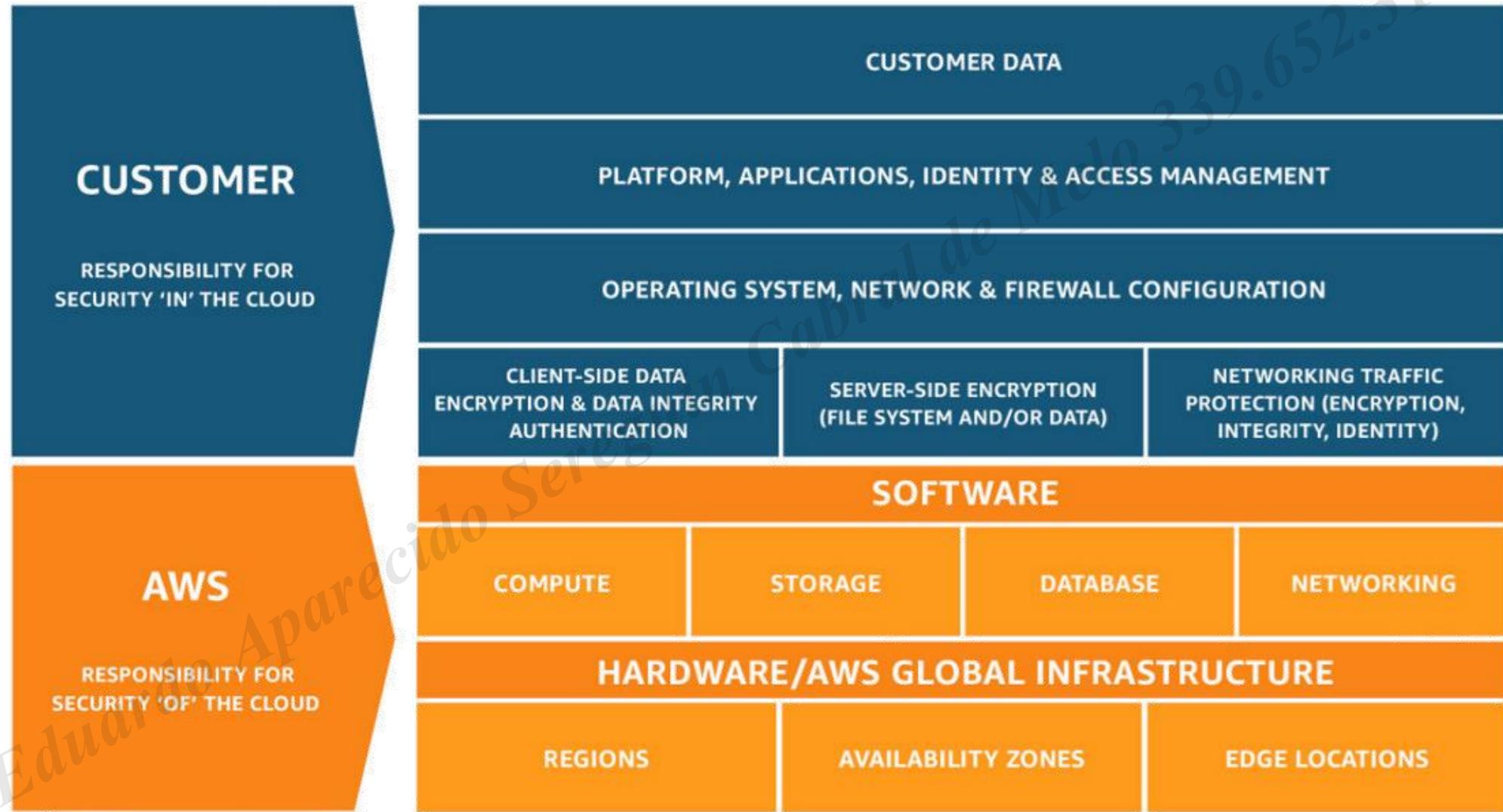
Shared responsibility model



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Shared Responsibility

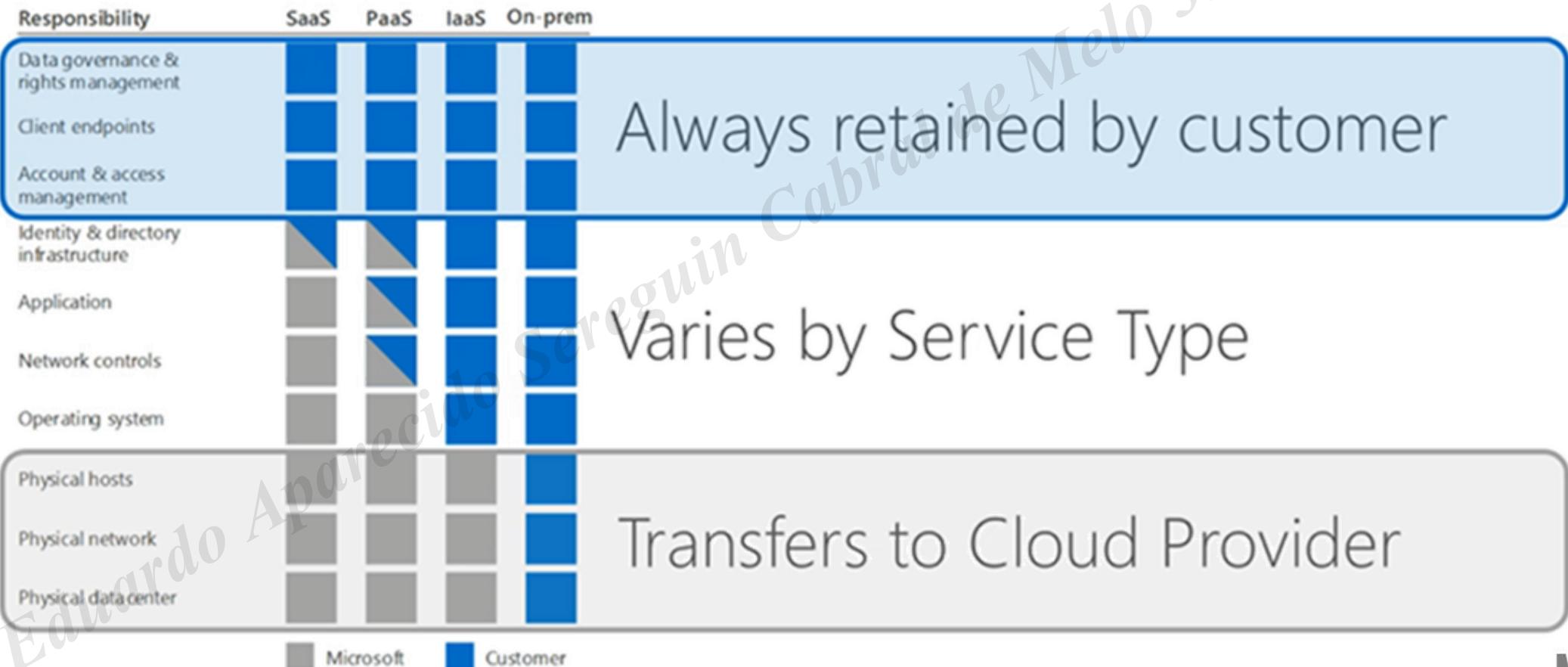


*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Shared Responsibility

Responsibility Zones

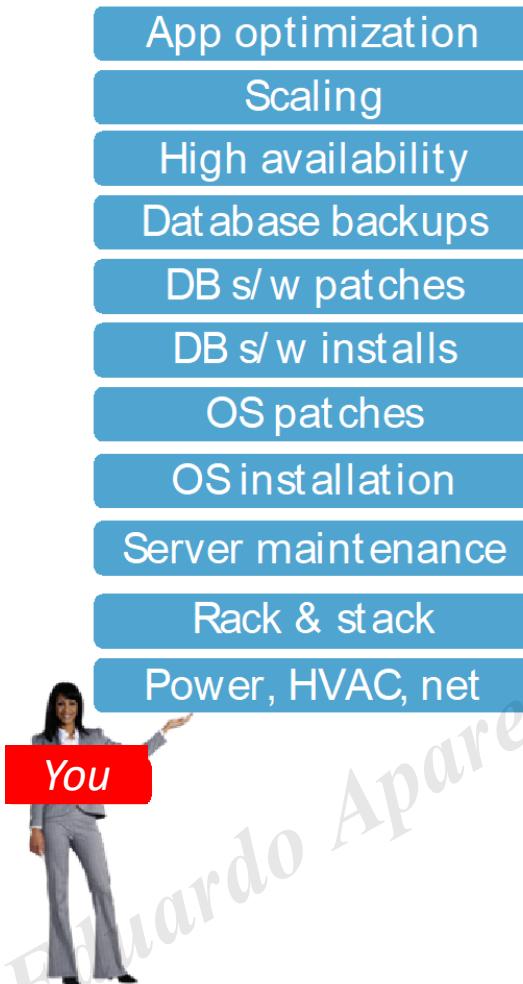


*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

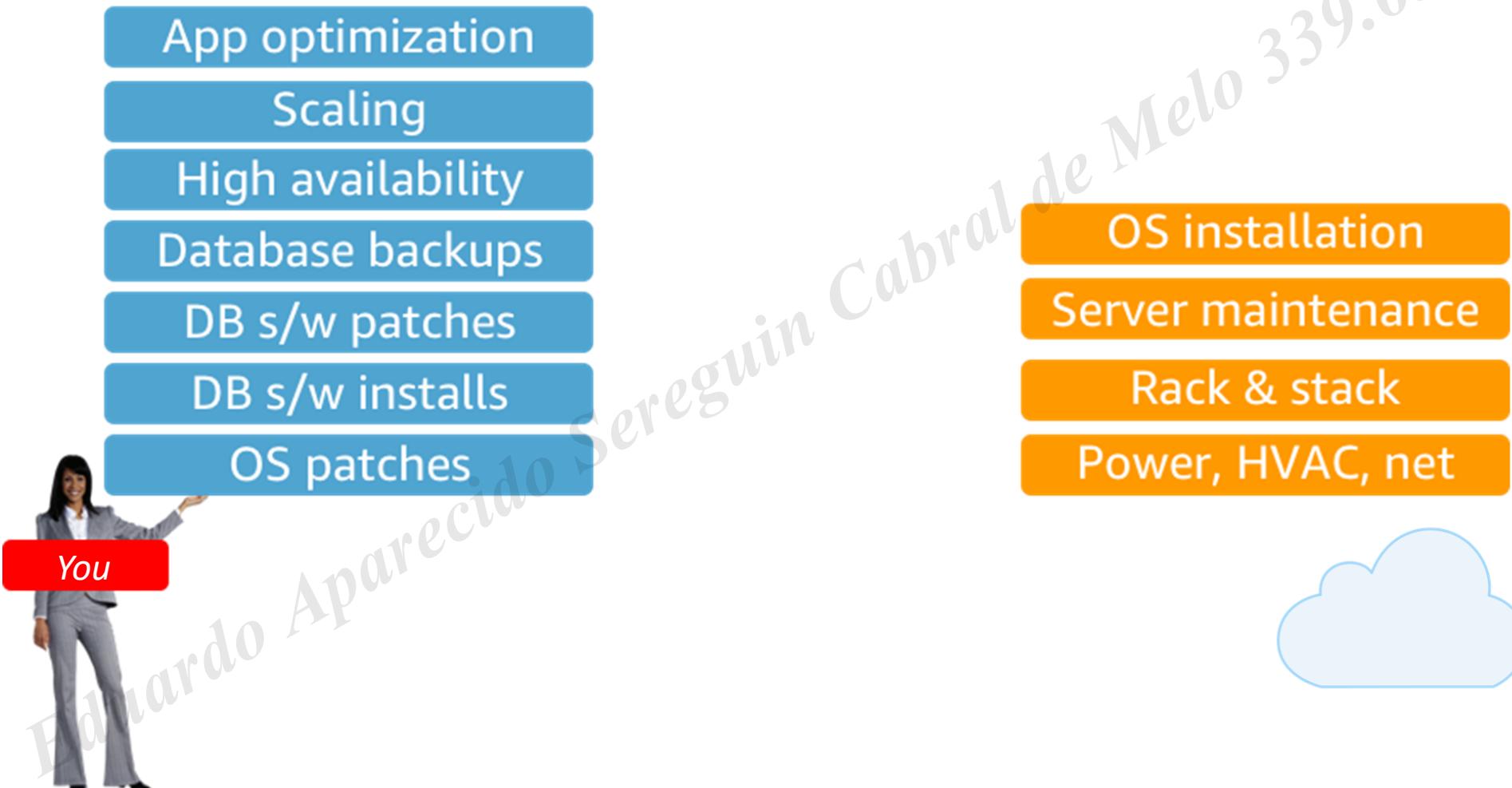
Practical example

DB in traditional environment



Practical example

DB in IaaS



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Practical example

DB in PaaS



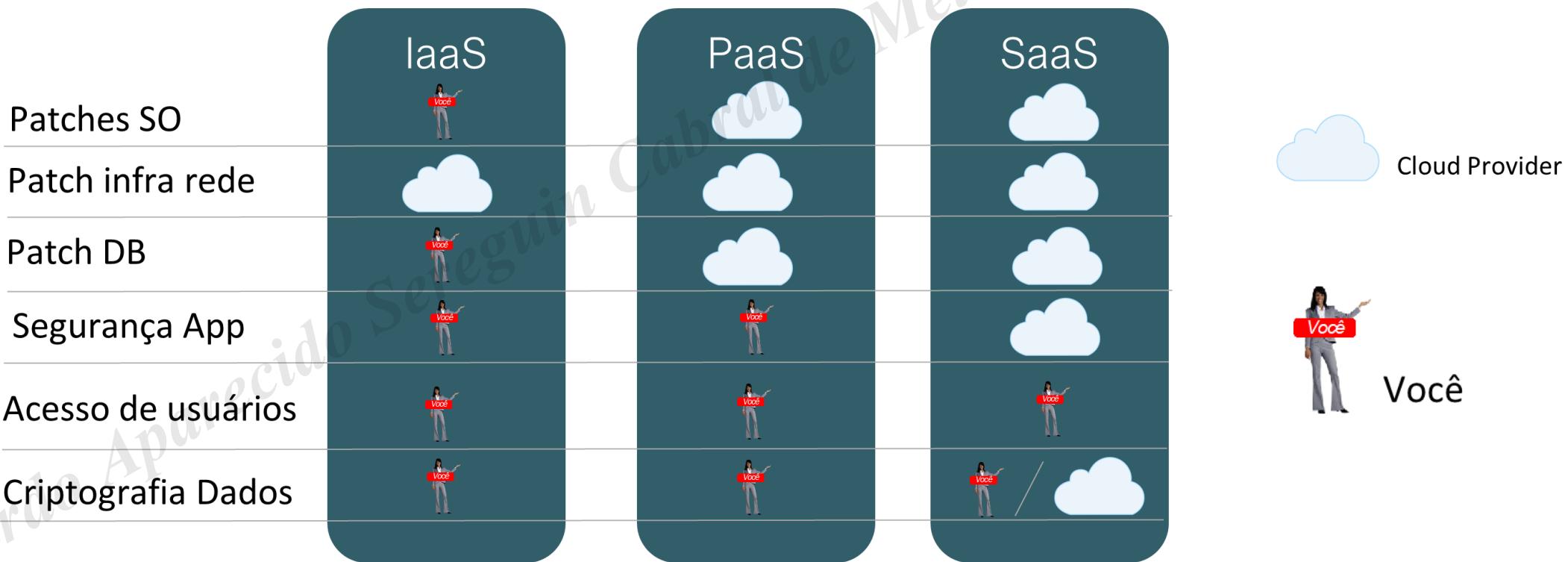
You

App optimization

- Scaling
- High availability
- Database backups
- DB s/w patches
- DB s/w installs
- OS patches
- OS installation
- Server maintenance
- Rack & stack
- Power, HVAC, net



Examples of some security discipline



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Class Agenda

4

Creating your security journey

2

Where to start?



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization **is prohibited**.

Relevant certificates for the industry



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Relevant regulations for the industry



BANCO CENTRAL

RESOLUÇÃO Nº 4.658, DE 26

Dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições do pagamento autorizadas a funcionar

BANCO CENTRAL DO BRASIL

CIRCULAR Nº 3.909, DE 16 DE AGOSTO DE 2018



Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições do pagamento autorizadas a funcionar

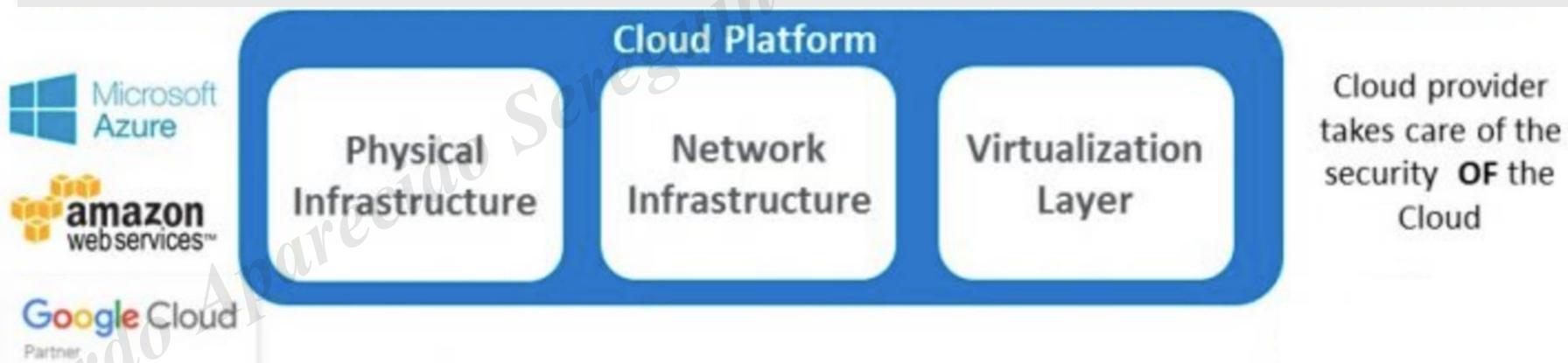
Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

[LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.](#)

Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

Alright, but how do I do “my part”

- Define the migration Journey
- Creating the security foundation
 - Governance Structure and professional profiles
 - Adoption of security principles
 - Adoption of Security services available **IN** cloud



Security Foundations

“The time to repair the roof
is when the sun is shining.”

John F. Kennedy, *State of the Union*, 1962

Security Foundations to the Cloud

Governance Structure and Professional Profiles

Principles of Security

Identity and Access Management

Audit and Traceability

Security in multiple layers – Zero Trust

Automation of Security

Protection of data

Incident response



CLOUD SECURITY
SOLUTIONS

Security Foundations to the Cloud

Estrutura de Governança e perfis profissionais

Princípios de Segurança

Gestão de Identidade e Acessos

Auditona e Rastreabilidade

Segurança em múltiplas camadas

Automação de Segurança

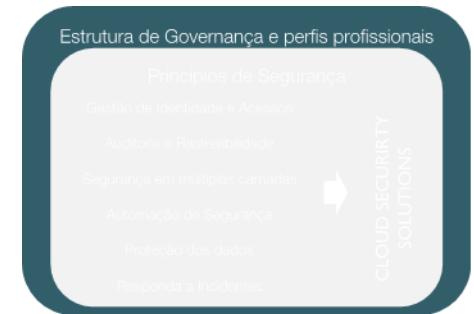
Proteção dos dados

Responda a Incidentes

CLOUD SECURITY
SOLUTIONS

Structure of governance and professional profiles

1. Evaluate questions of compliance, contractual and controls of the relevant supplier.
 - Relevant certificates and security requirements that must be in contracts
 - Governance mechanisms to evaluate periodically if security levels are aligned with the expectations and contractual definitions
 - Locals in the globe that may be limiters by regulatory issues



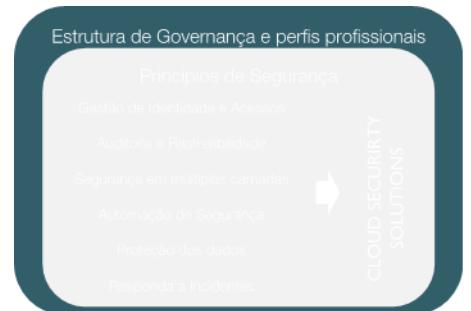
*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Structure of governance and professional profiles

2. The Security team needs to have new professionals profiles

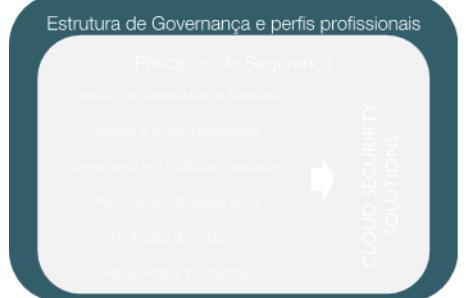
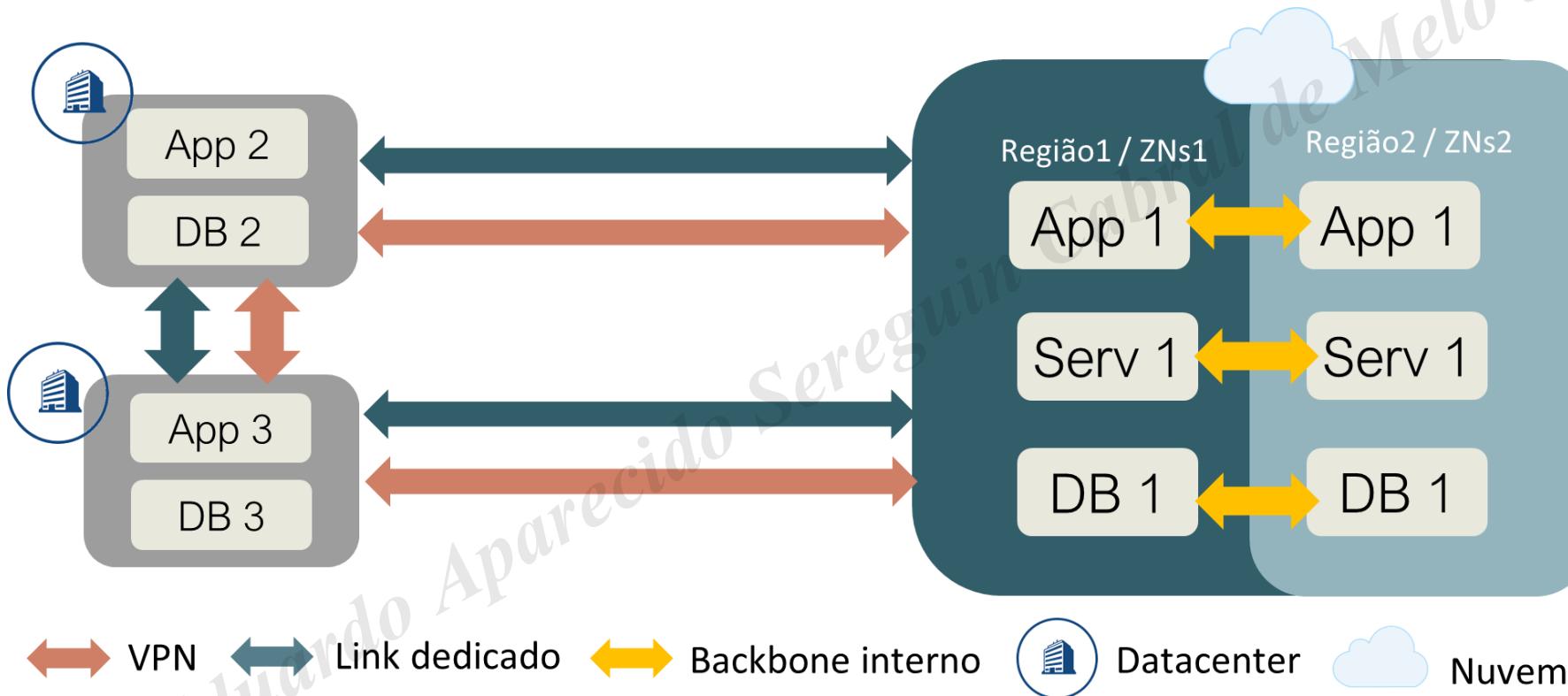
- Developers to automate security
- Connoisseurs of security OF / IN Cloud
- Internal responsibility shared with the teams of Cloud, DevOps as cloud is adopted
- Security started to have a role beyond the normative and implementation of technological controls to be provider of Self Service security services that accelerate the implementation of security.



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Structure of governance and professional profiles

3. Review your BIA

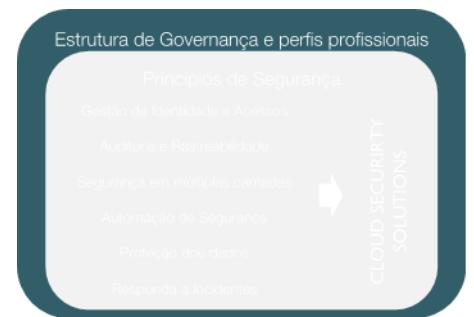
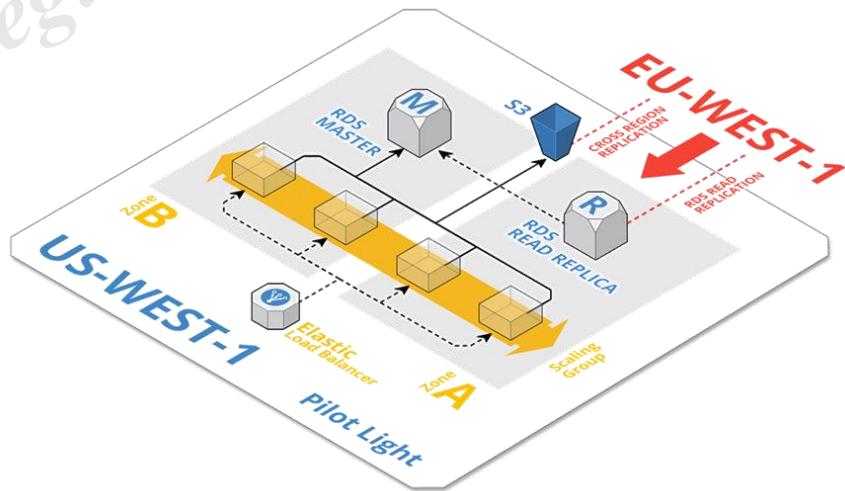
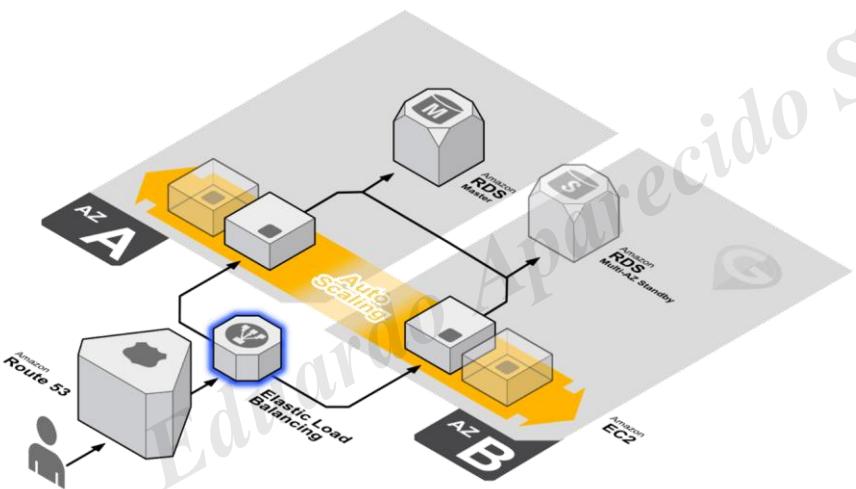


*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Structure of governance and professional profiles

4. Test and document the plan (Continuity and DR) considering the resources and features of the cloud that can improve RTO and RPO, spreading copies out across multiple Zones.



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Security Foundations to the Cloud

Estrutura de Governança e perfis profissionais

Princípios de Segurança

Gestão de Identidade e Acessos

Auditória e Rastreabilidade

Segurança em múltiplas camadas

Automação de Segurança

Proteção dos dados

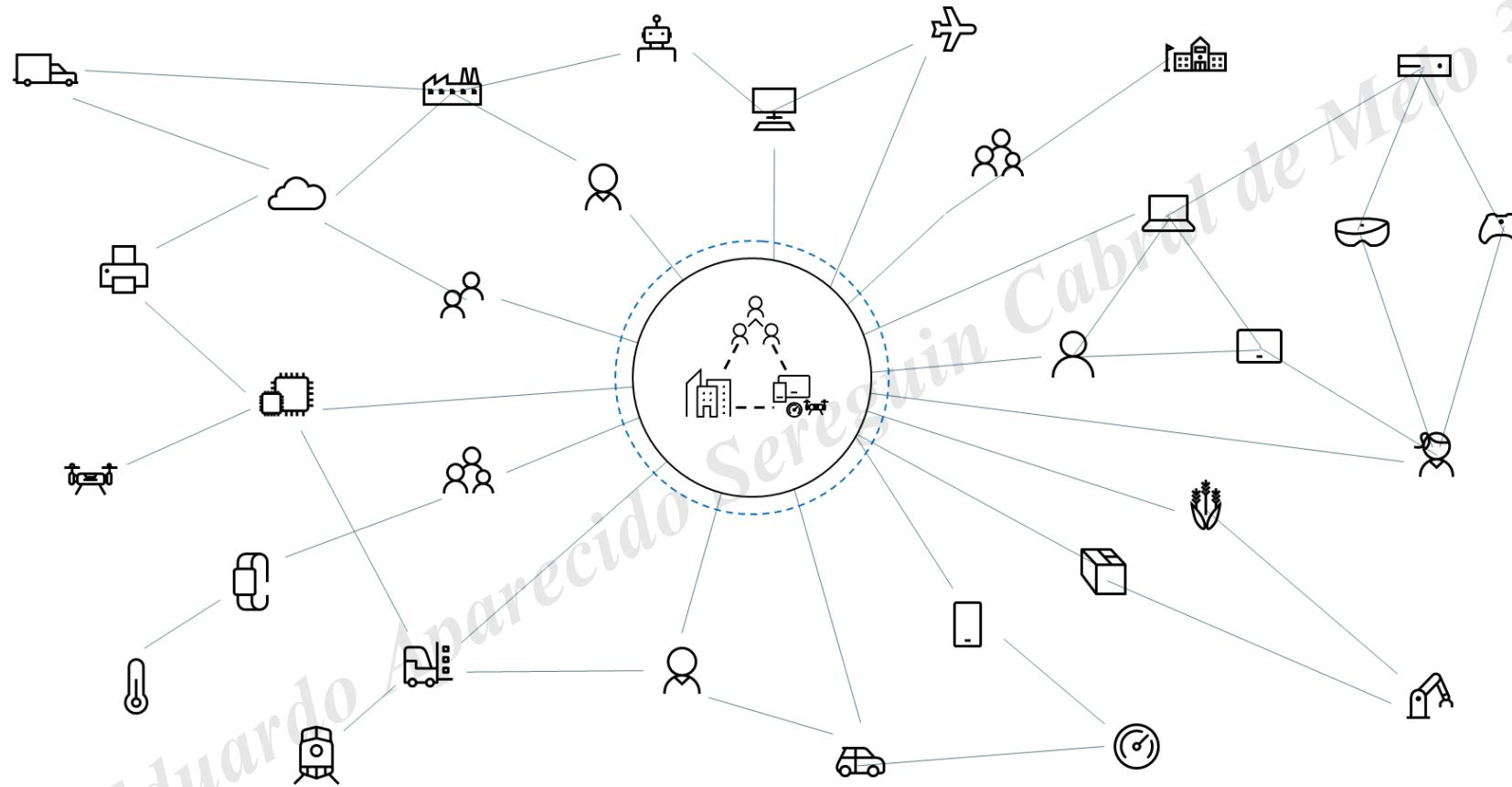
Responda a Incidentes



CLOUD SECURITY
SOLUTIONS

Layer security

The identity is the Control Plane



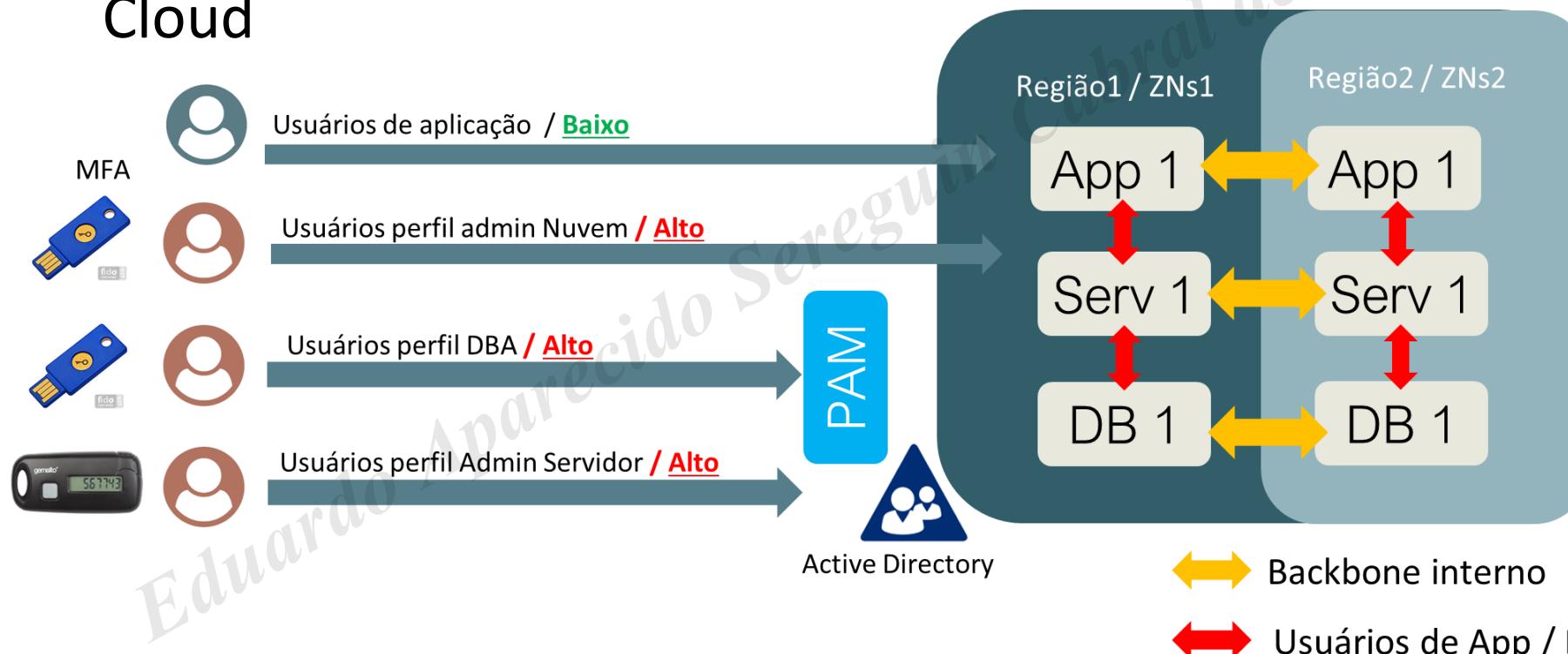
*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Identity Management and Accesses

1. You do what you need

- It is the backbone to create a good security base in Cloud



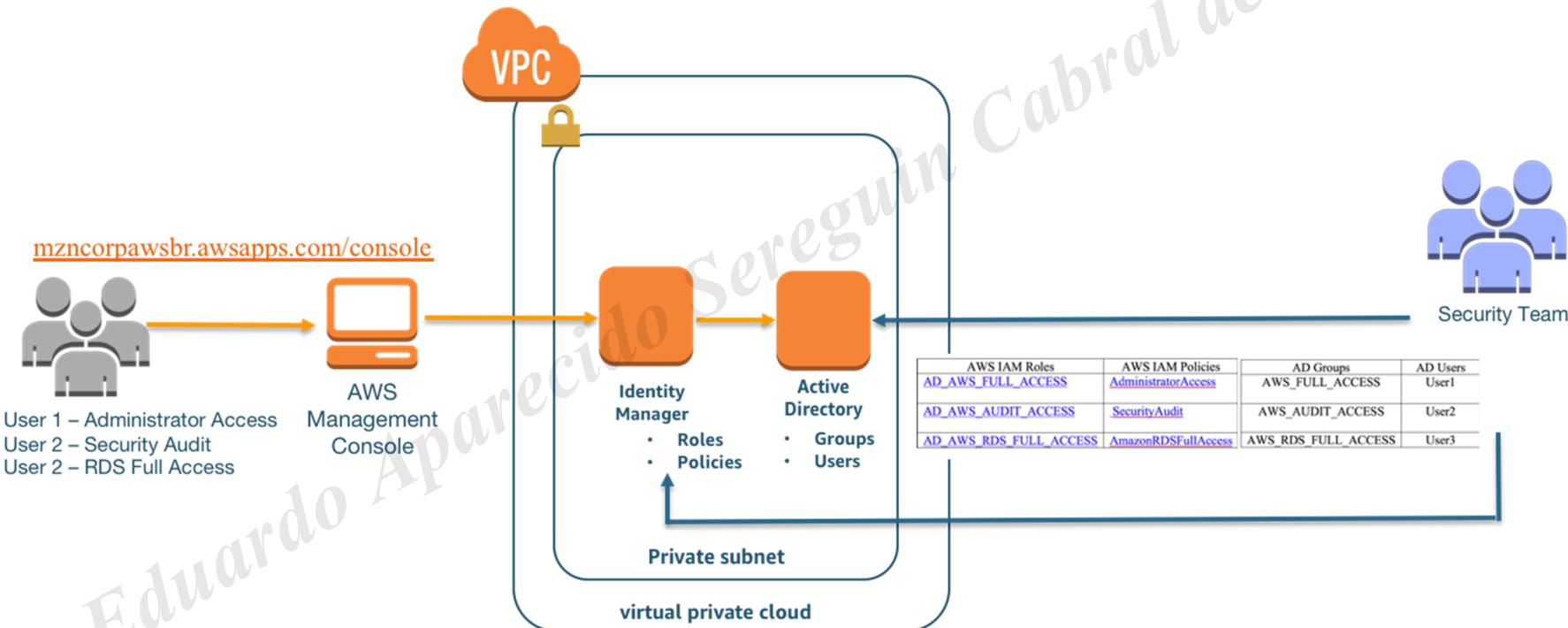
*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Identity Management and Accesses

2. You do ONLY what you need to do

- Minimum privileges possible, access profiles

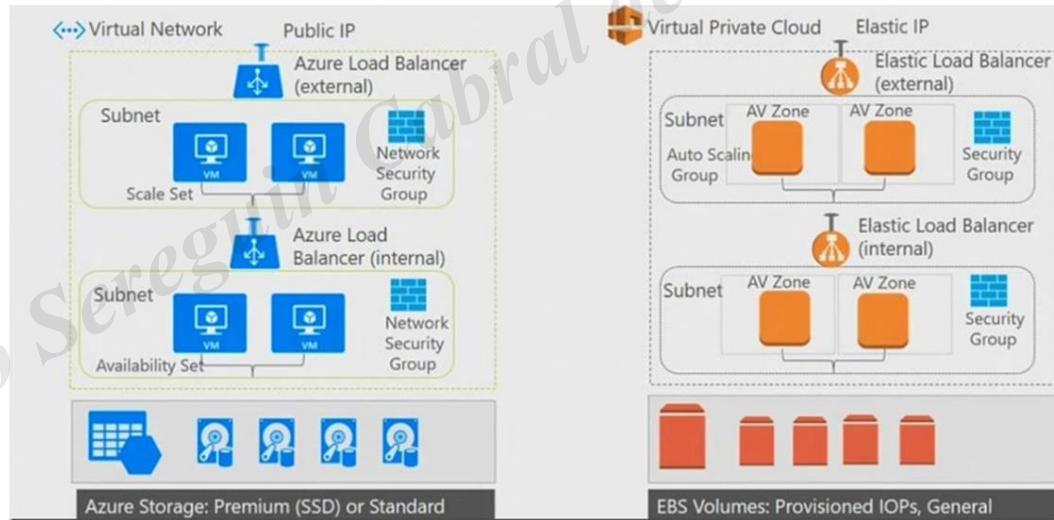
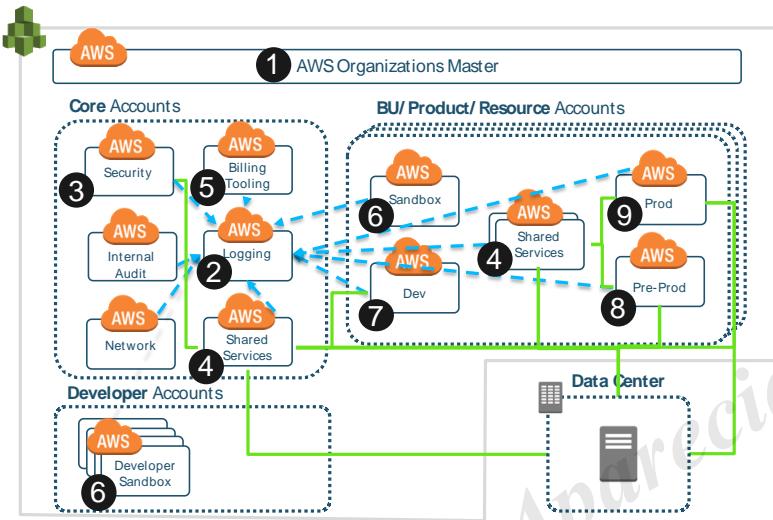


*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Security principles

2. Creating segregation of accounts / subscription / projects



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Security Foundations to the Cloud

Estrutura de Governança e perfis profissionais

Princípios de Segurança

Auditoria e Rastreabilidade



Audit and Traceability

1. You do, I Know

- Centralize, monitor, and generate alert of actions and changes performed in your environments in real time.
- Integrate alerts and metrics to obtain automatic answers.



Ocorre uma
atividade



Serviço captura e
grava o evento
no log

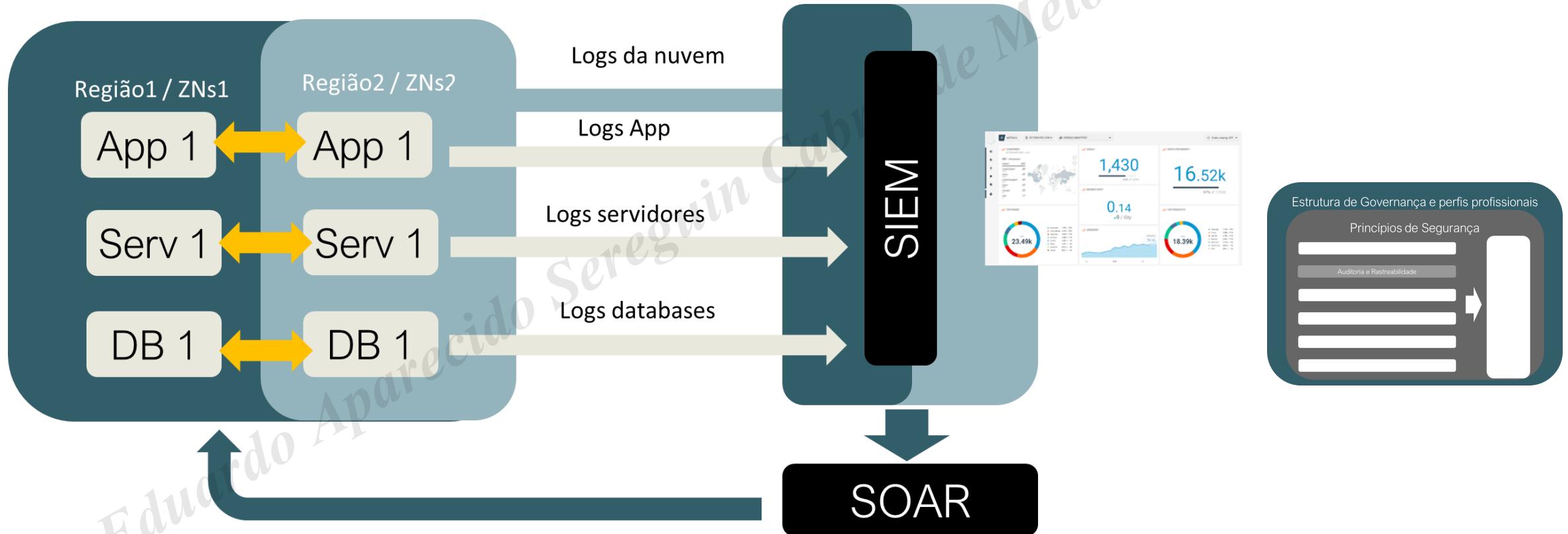


Pode ver e
investigar a
atividade



Audit and Traceability

2. You do, I Know



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Security Foundations to the Cloud

Estrutura de Governança e perfis profissionais

Princípios de Segurança

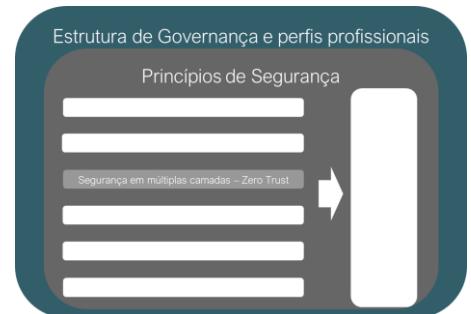
Segurança em múltiplas camadas – Zero Trust



Layer security

1. Protecting the crown jewels

- Isolate servers and applications
- Implement mechanisms of micro segmentation
- Limit the attack surface

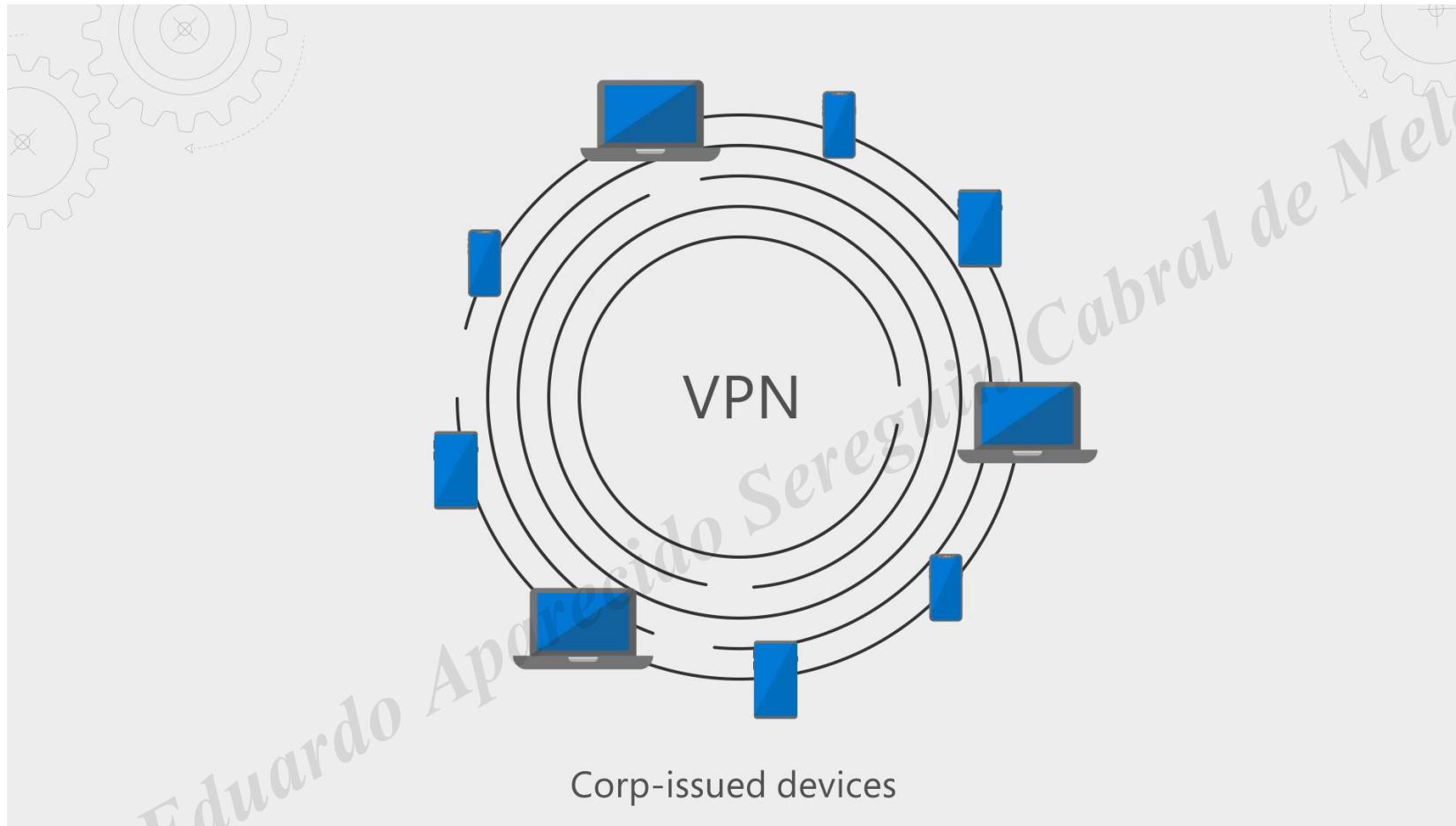


*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Layer security

Zero Trust

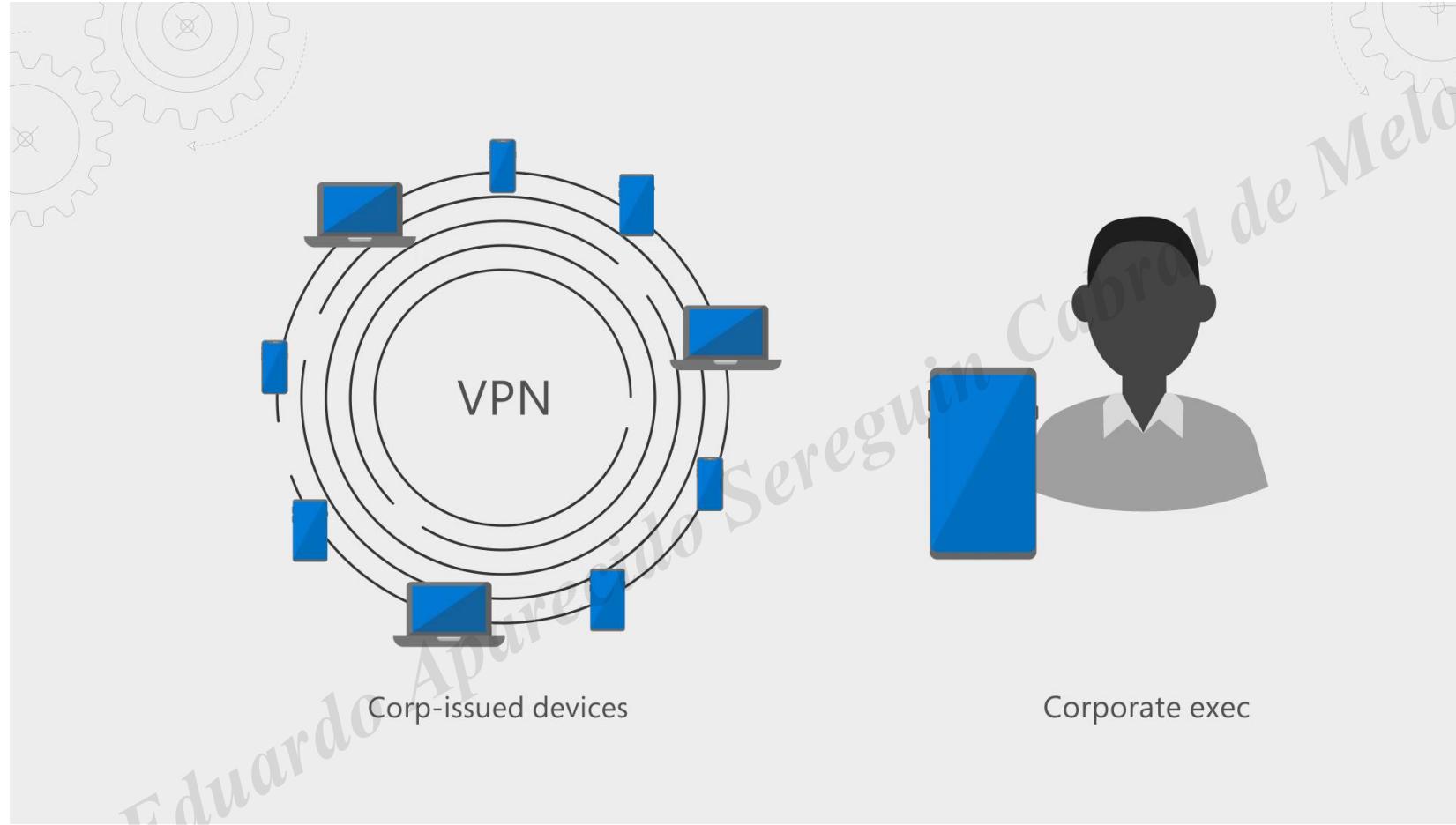


*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Layer security

Zero Trust



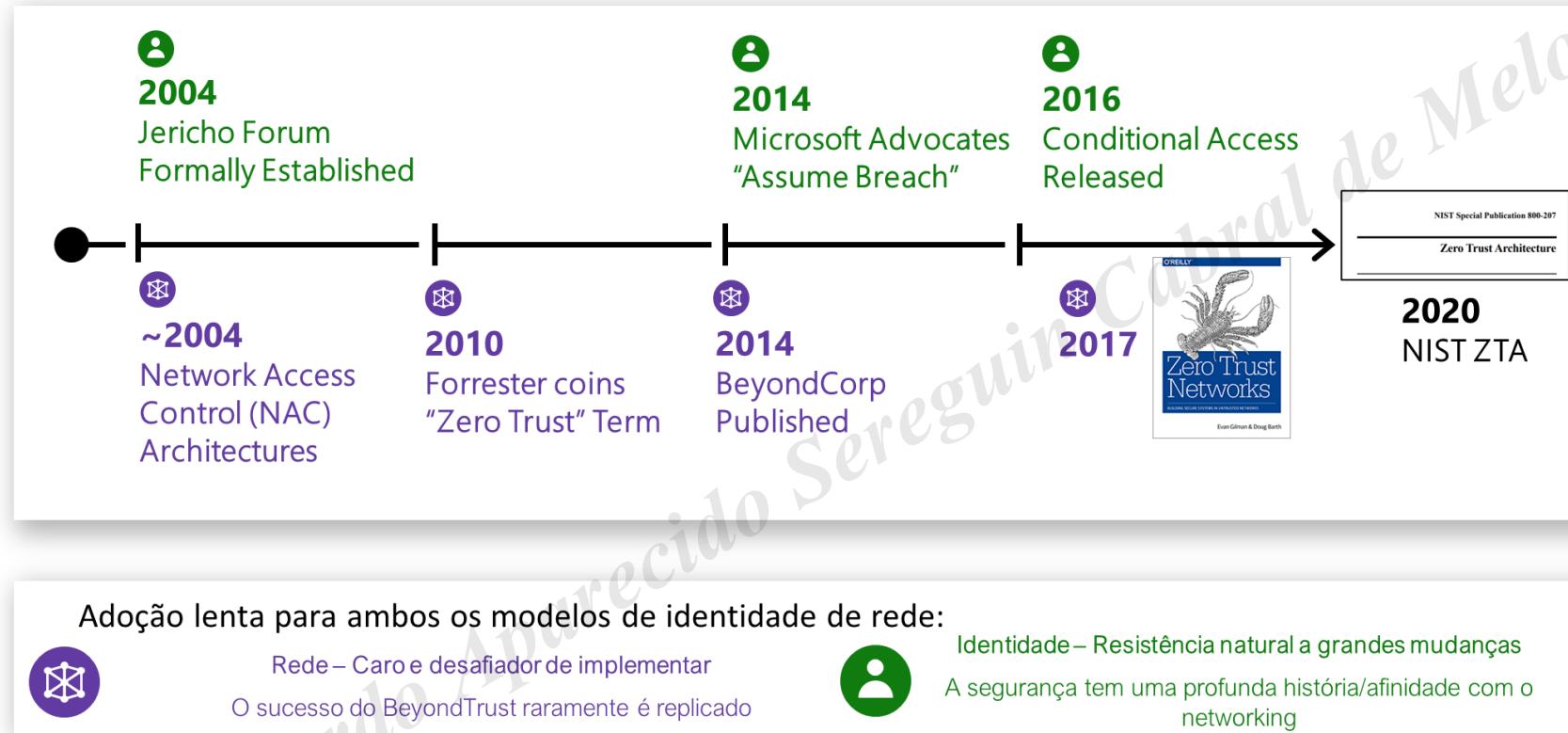
*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization **is prohibited**.



Layer security

The idea of "Zero Trust" has been evolved for some time.

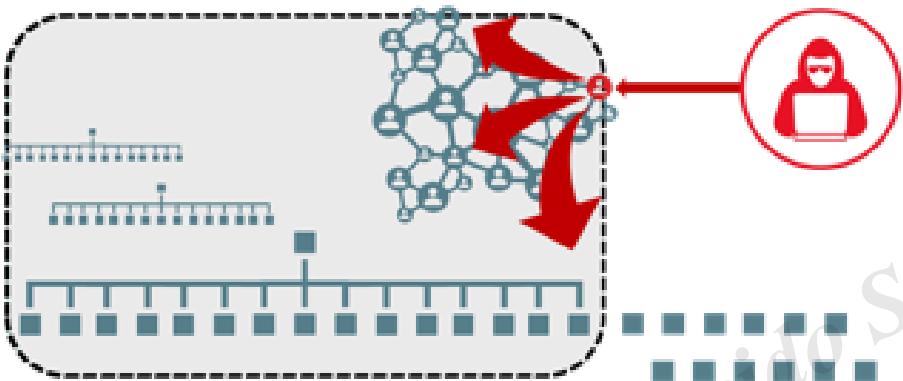


*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

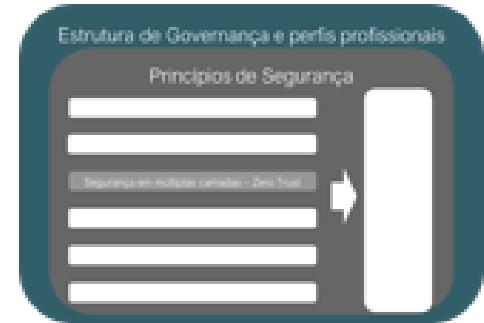
Layer security

Why should we approach Zero Trust?

The objective is to keep the **actives** distant from the **attackers**.



1. Complexity in Security in IT
 - Much devices, users, conexions and networks
2. Network Security Strategies
 - Attacks based on networks
 - Apparently simple and economic
 - Confidence in safe network segmentation
3. Actives leaving the network
 - BYOD, WFH, Mobile, and SaaS
4. Attackers focusing on identity
 - Phishing and credential theft

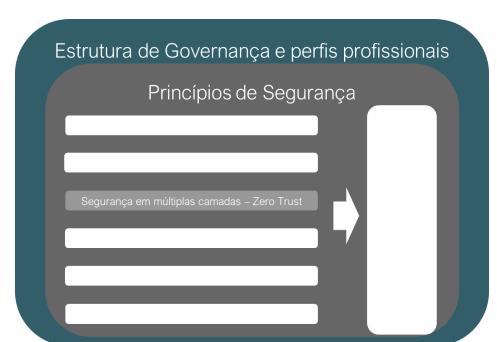


Layer security

Main principle of Zero Trust

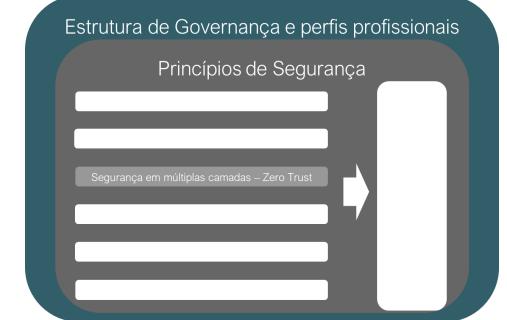
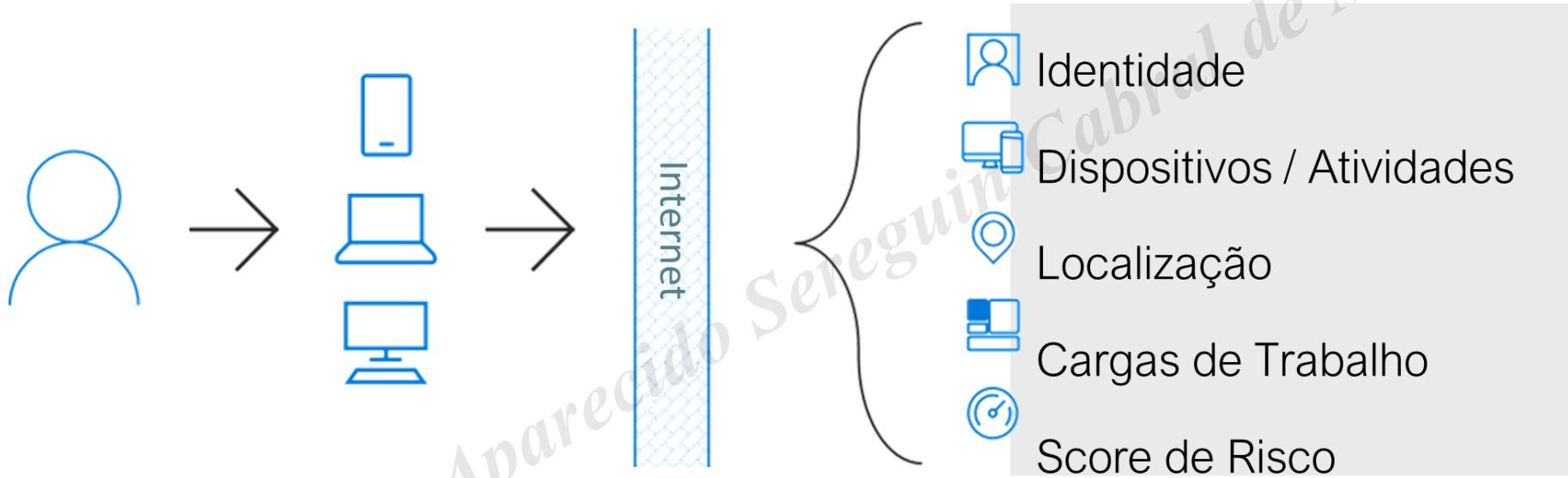


1. Usuários e dispositivos devem ser capazes de trabalhar de qualquer rede e de qualquer lugar com o mesmo nível de segurança.



Layer security

Adopt a premise that all resources are connected
on the Internet



Security Foundations to the Cloud

Estrutura de Governança e perfis profissionais

Princípios de Segurança

Automação de Segurança

Automation and Security

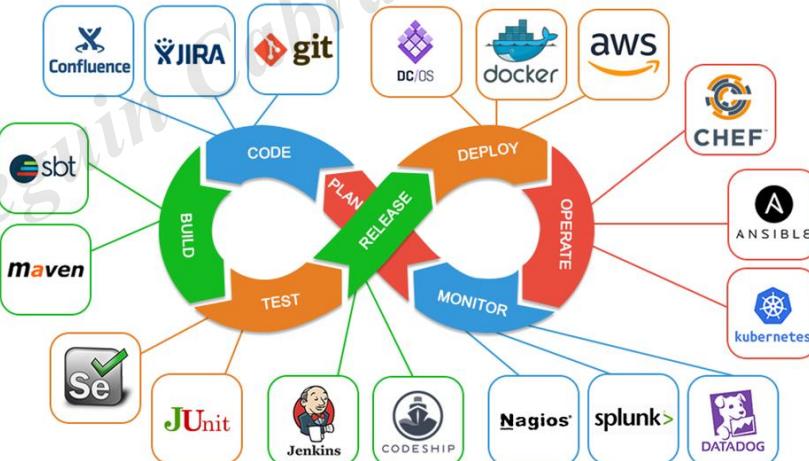
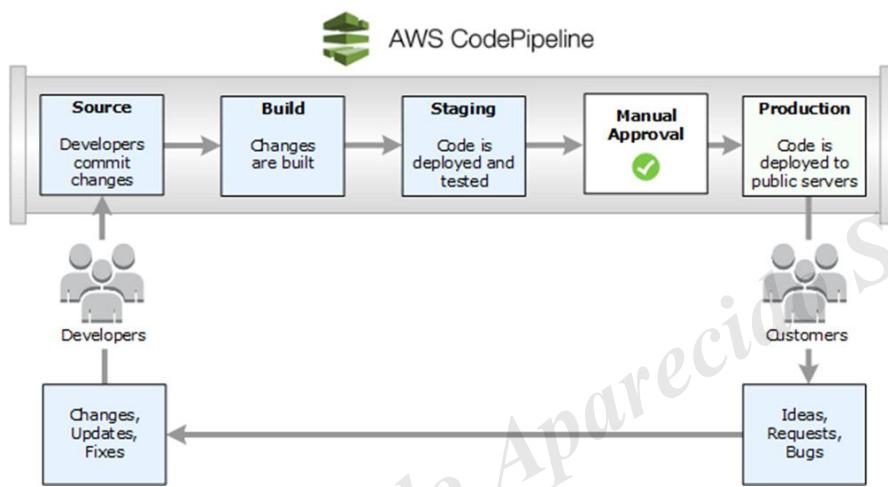
Humans don't touch the data

- Provisionamento de recursos de forma padronizada e segura
- Resposta a incidentes, eventos e recuperação de forma automática.
- Avalie a segurança de aplicações de forma contínua



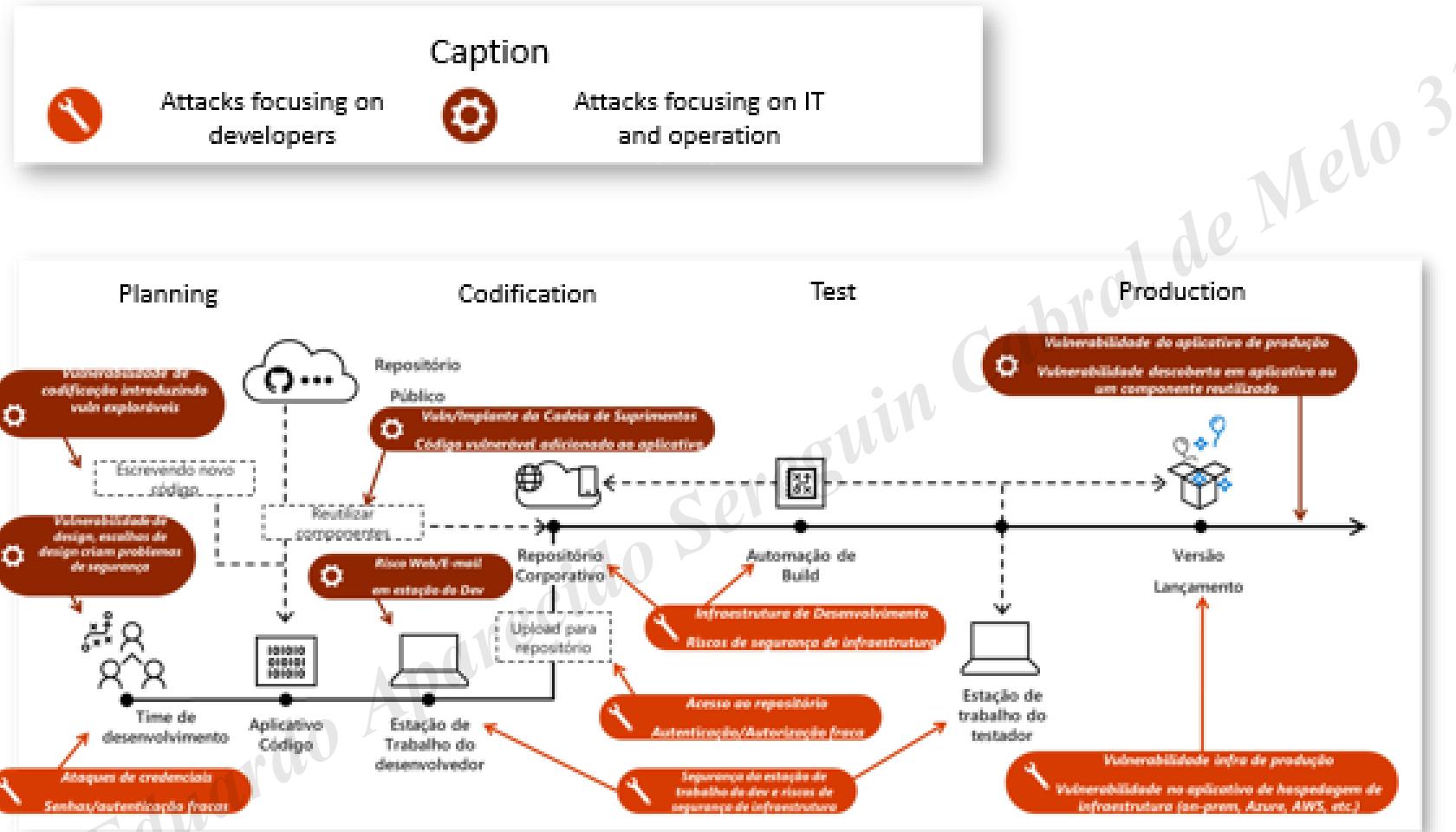
Automation and Security

Humans don't touch the data



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Risks in the development environment



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Protect your DevOps

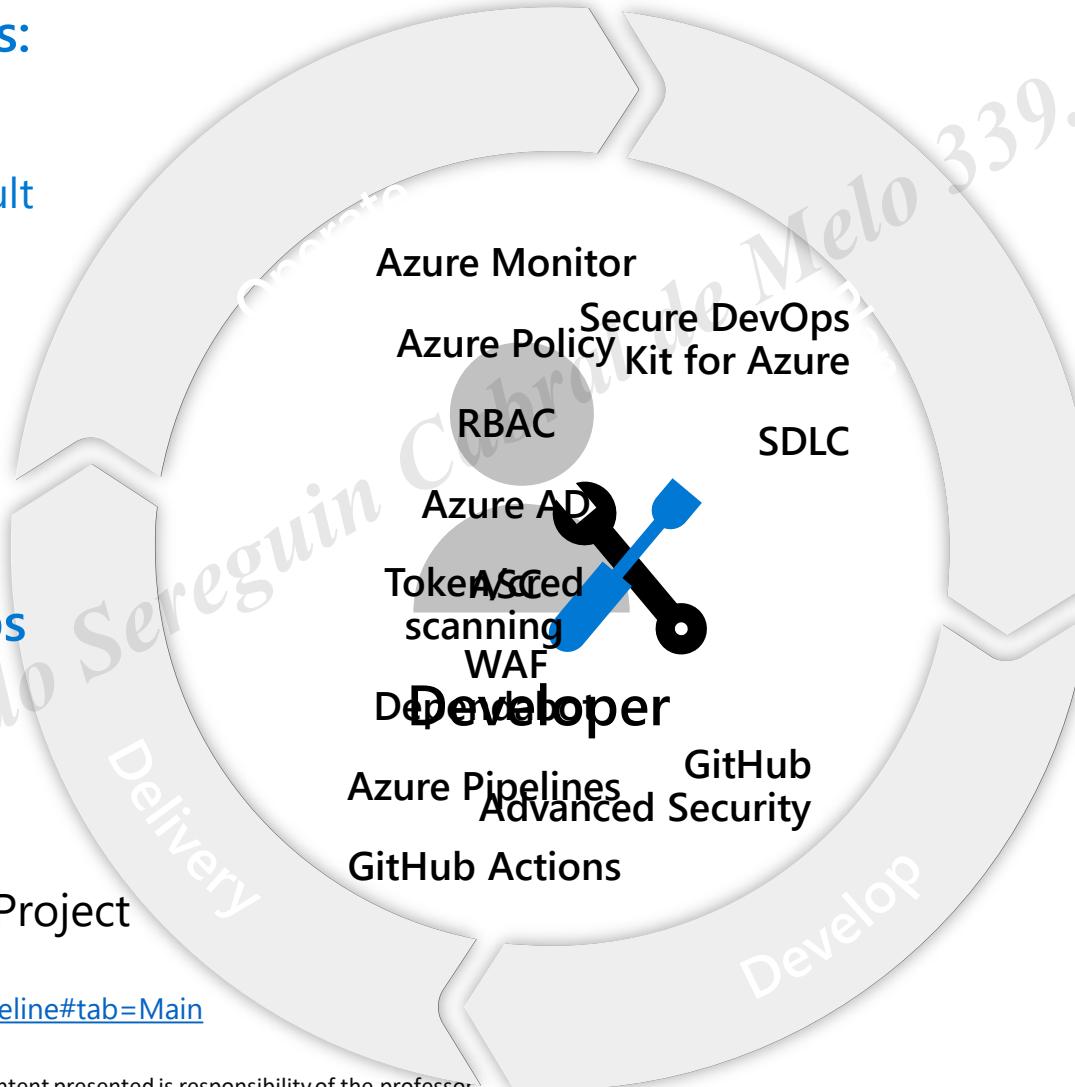
Define the Security requirements:

- Threat modeling in major releases
- Execute code security analysis Store secrets safely using [Azure Security Vault](#)

Establish a standard incident response process

Protect the development of Apps

- Microsoft Secure DevOps Toolkit –
<https://azsk.azurewebsites.net/>
- Organization for Web App Security Project (OWASP) DevOps Pipeline security
https://www.owasp.org/index.php/OWASP_AppSec_Pipeline#tab=Main



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Security Foundations to the Cloud

Estrutura de Governança e perfis profissionais

Princípios de Segurança



Proteção dos dados



*The responsi-

Data Protection

Humans don't see the data

- Protect data in transit
- Protect the data at rest
- Use tokenization resources
- Backup policies
- Masking and monitoring of data use



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Data Protection

Humans don't see the data

Criptografia de volumes

Criptografia de Disco (EBS)

Arquivos

Soluções de parceiros / MarketPlace

Criptografia de Objetos

S3 Server Side Encryption (SSE)

S3 SSE com chaves do cliente

Criptografia do lado do cliente

Criptografia de Bases de Dados

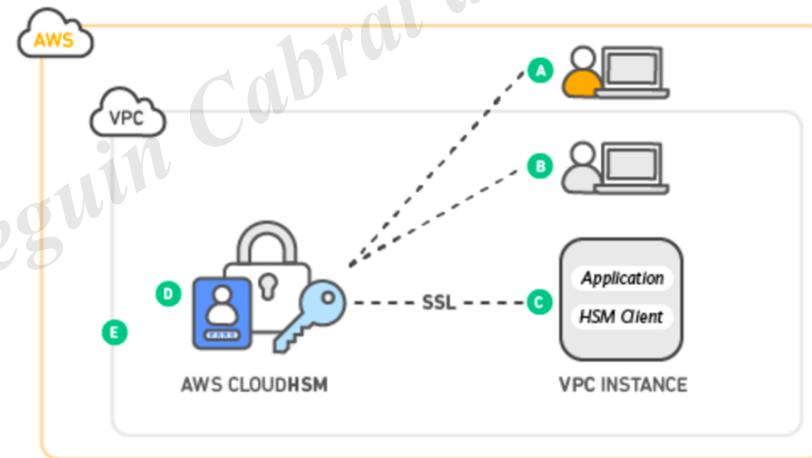
MSSQL

ORACLE

MYSQL

PostgreSQL

Redshift



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Security Foundations to the Cloud

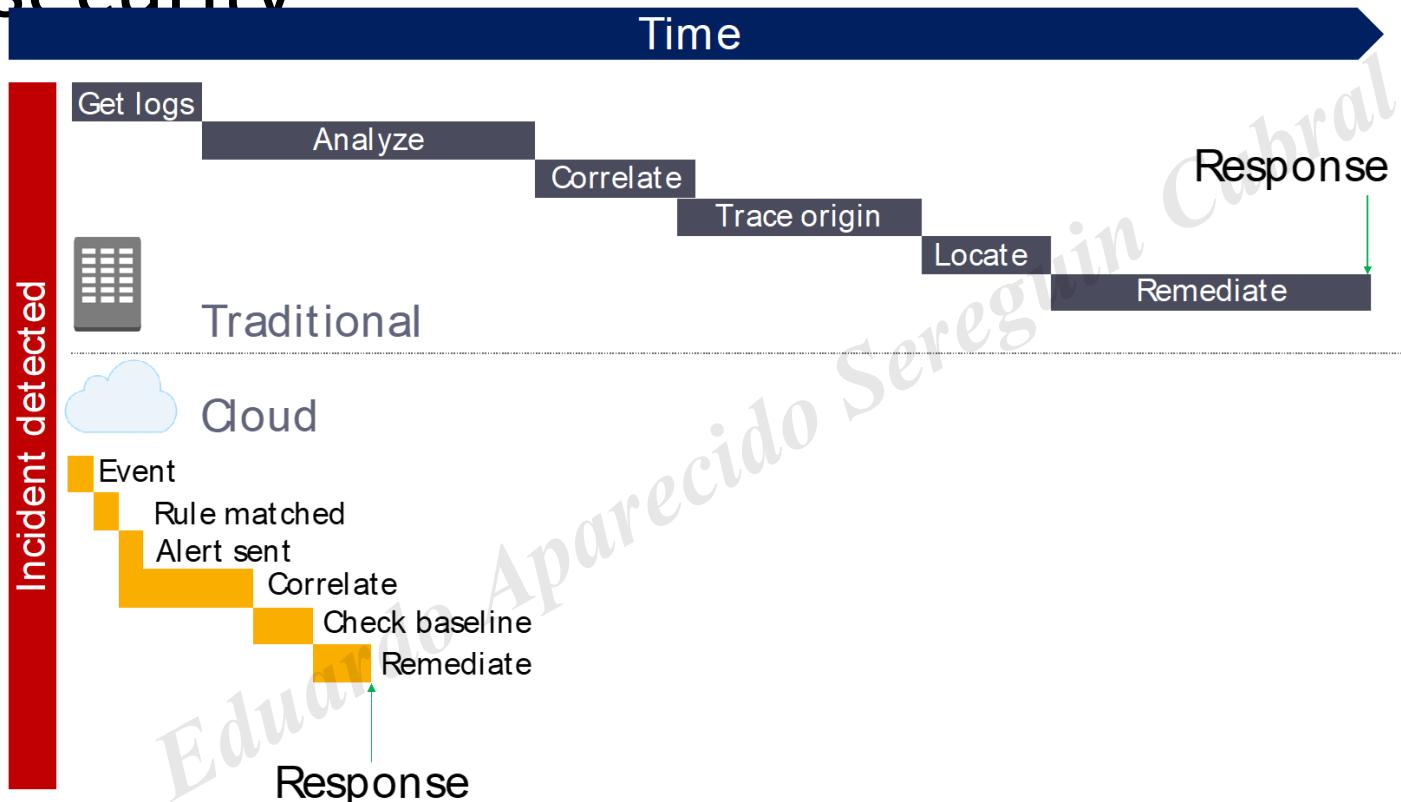
Estrutura de Governança e perfis profissionais

Princípios de Segurança

Responda a Incidentes

Incident response

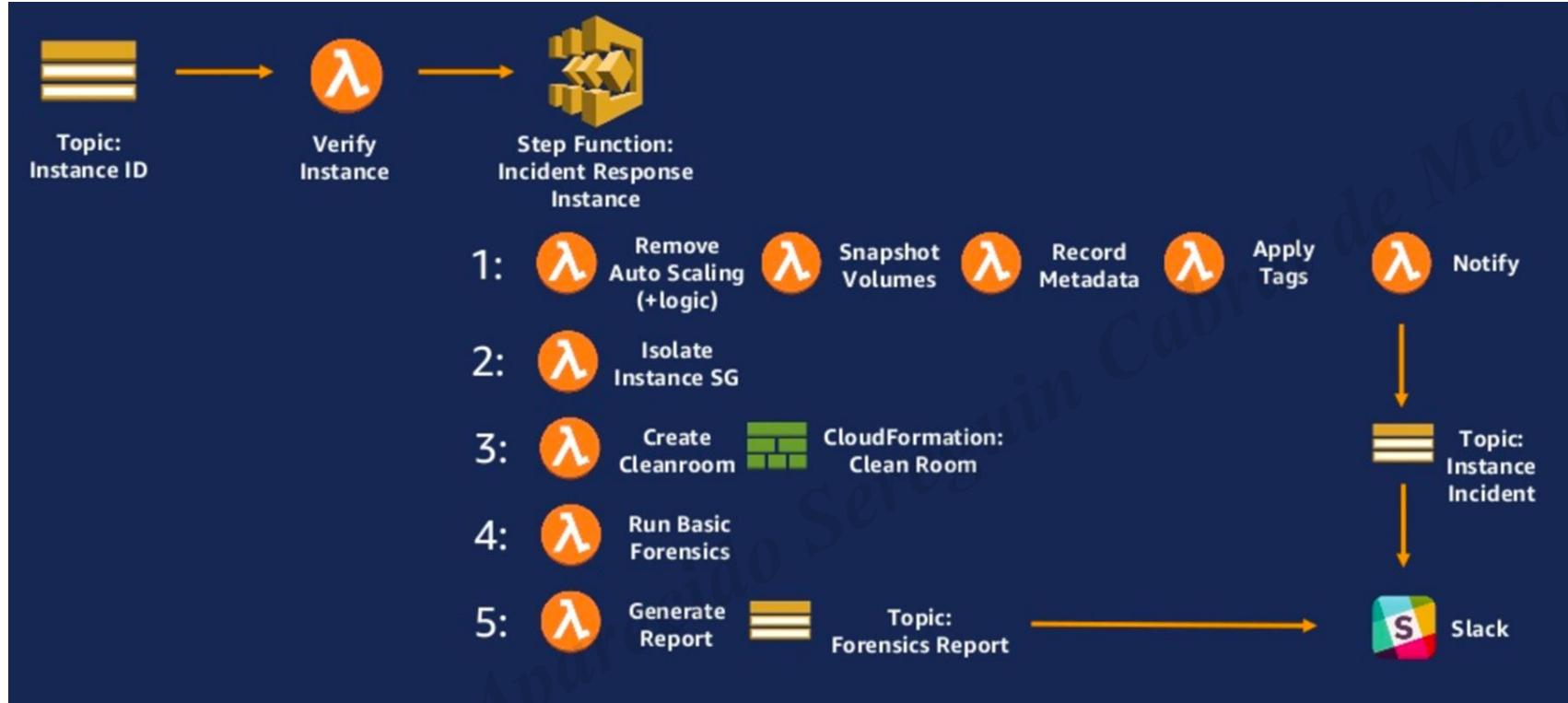
Prepare yourself for incidents
responses of cloud security in large
security



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

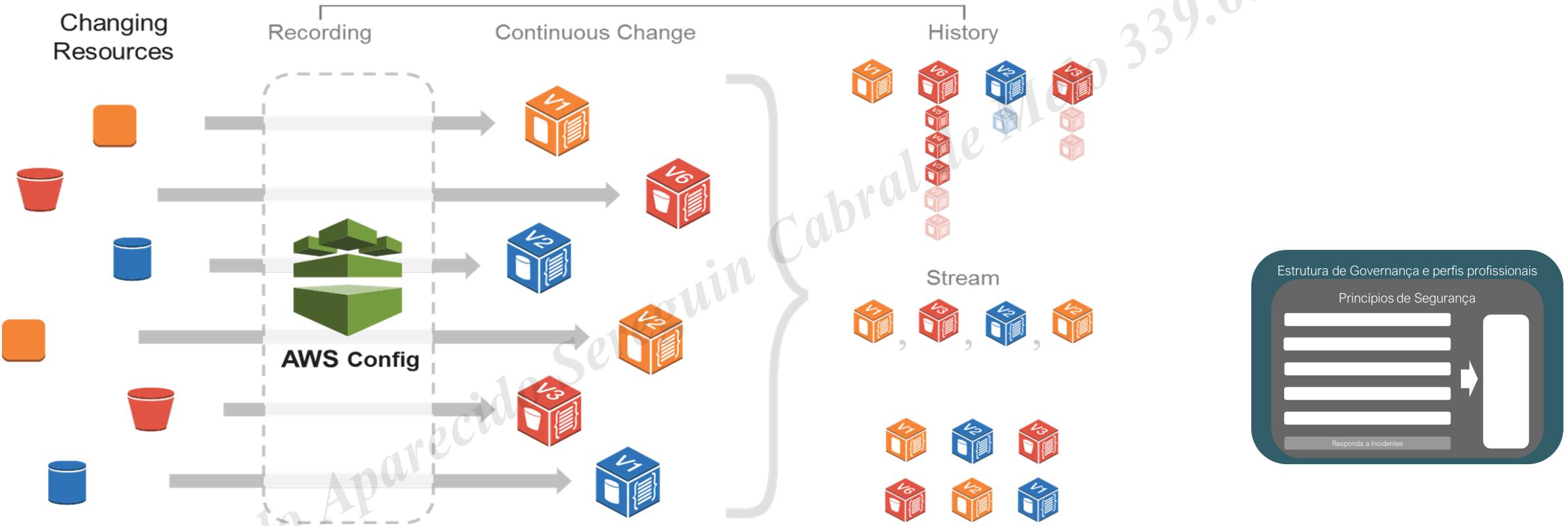
Incident response



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Incident response



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Security Foundations to the Cloud

Estrutura de Governança e perfis profissionais

Princípios de Segurança

CLOUD SECURITY
SOLUTIONS

Cloud Native Solutions

Understand the potential of Cloud Native solutions

Data protection

AWS provides services that help you protect your data, accounts, and workloads from unauthorized access. AWS data protection services provide encryption and key management and threat detection that continuously monitors and protects your accounts and workloads.

Threat detection & continuous monitoring

AWS identifies threats by continuously monitoring the network activity and account behavior within your cloud environment.

Identity & access management

AWS Identity Services enable you to securely manage identities, resources, and permissions at scale. With AWS, you have identity services for your workforce and customer-facing applications to get started quickly and manage access to your workloads and applications.

[Learn more »](#)

Compliance & data privacy

AWS gives you a comprehensive view of your compliance status and continuously monitors your environment using automated compliance checks based on the AWS best practices and industry standards your organization follows.

Network & application protection

Network and application protection services enable you to enforce fine-grained security policy at network control points across your organization. AWS services help you inspect and filter traffic to prevent unauthorized resource access at the host-, network-, and application-level boundaries.

[Learn more »](#)



Cloud Native Solutions

Identity and Access Management

Identity & access management

Securely manage access to services and resources



[AWS Identity & Access Management \(IAM\)](#)

Cloud single-sign-on (SSO) service



[AWS Single Sign-On](#)

Identity management for your apps



[Amazon Cognito](#)

Managed Microsoft Active Directory



[AWS Directory Service](#)

Simple, secure service to share AWS resources



[AWS Resource Access Manager](#)

Central governance and management across AWS accounts



[AWS Organizations](#)



Cloud Native Solutions

Detection

Detection

Automate AWS security checks and centralize security alerts



Protect AWS accounts with intelligent threat detection



Automate vulnerability management



Record and evaluate configurations of your AWS resources



Track user activity and API usage



Security management for IoT devices



Cloud Native Solutions

Network and application protection

Network and application protection

Network security	 AWS Network Firewall
DDoS protection	 AWS Shield
Filter and control outbound DNS traffic for your VPCs	 Amazon Route 53 Resolver DNS Firewall
Filter malicious web traffic	 AWS Web Application Firewall (WAF)
Central management of firewall rules	 AWS Firewall Manager



<https://aws.amazon.com/products/security/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Cloud Native Solutions

Data Protection

Data protection	Discover and protect your sensitive data at scale	 Amazon Macie
	Key storage and management	 AWS Key Management Service (KMS)
	Hardware based key storage for regulatory compliance	 AWS CloudHSM
	Provision, manage, and deploy public and private SSL/TLS certificates	 AWS Certificate Manager
	Rotate, manage, and retrieve secrets	 AWS Secrets Manager



<https://aws.amazon.com/products/security/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Cloud Native Solutions

Incident Response

Incident response

Investigate potential security issues



Amazon Detective

Scalable, cost-effective application recovery to AWS



AWS Elastic Disaster Recovery



<https://aws.amazon.com/products/security/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Cloud Native Solutions

Compliance

Compliance

No cost, self-service portal for on-demand access to AWS' compliance reports



AWS Artifact

Continuously audit your AWS usage to simplify how you assess risk and compliance



AWS Audit Manager



Cloud Native Solutions

Security, Identity and Compliance

Security

Protect your enterprise from advanced threats across hybrid cloud workloads

Azure Sentinel

Standing watch, by your side. Intelligent security analytics for your entire enterprise

Key Vault

Safeguard and maintain control of keys and other secrets

Azure Information Protection

Better protect your sensitive information—anytime, anywhere

Azure Active Directory

Synchronize on-premises directories and enable single sign-on

Azure Dedicated HSM

Manage hardware security modules that you use in the cloud

Security Center

Unify security management and enable advanced threat protection across hybrid cloud workloads

Application Gateway

Build secure, scalable, and highly available web front ends in Azure

VPN Gateway

Establish secure, cross-premises connectivity

Azure DDoS Protection

Protect your applications from Distributed Denial of Service (DDoS) attacks



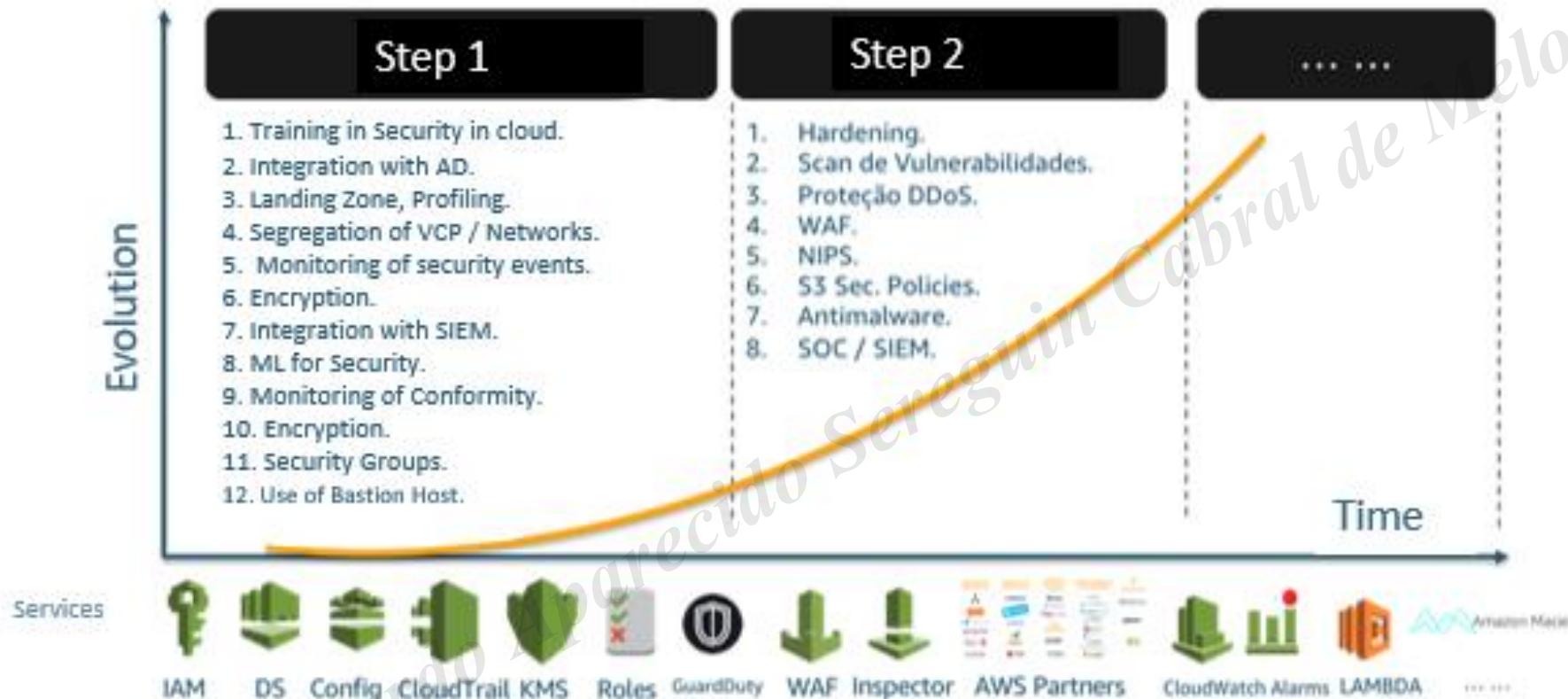
Class Agenda

4

Creating your security journey

2

Example of Safe Journey

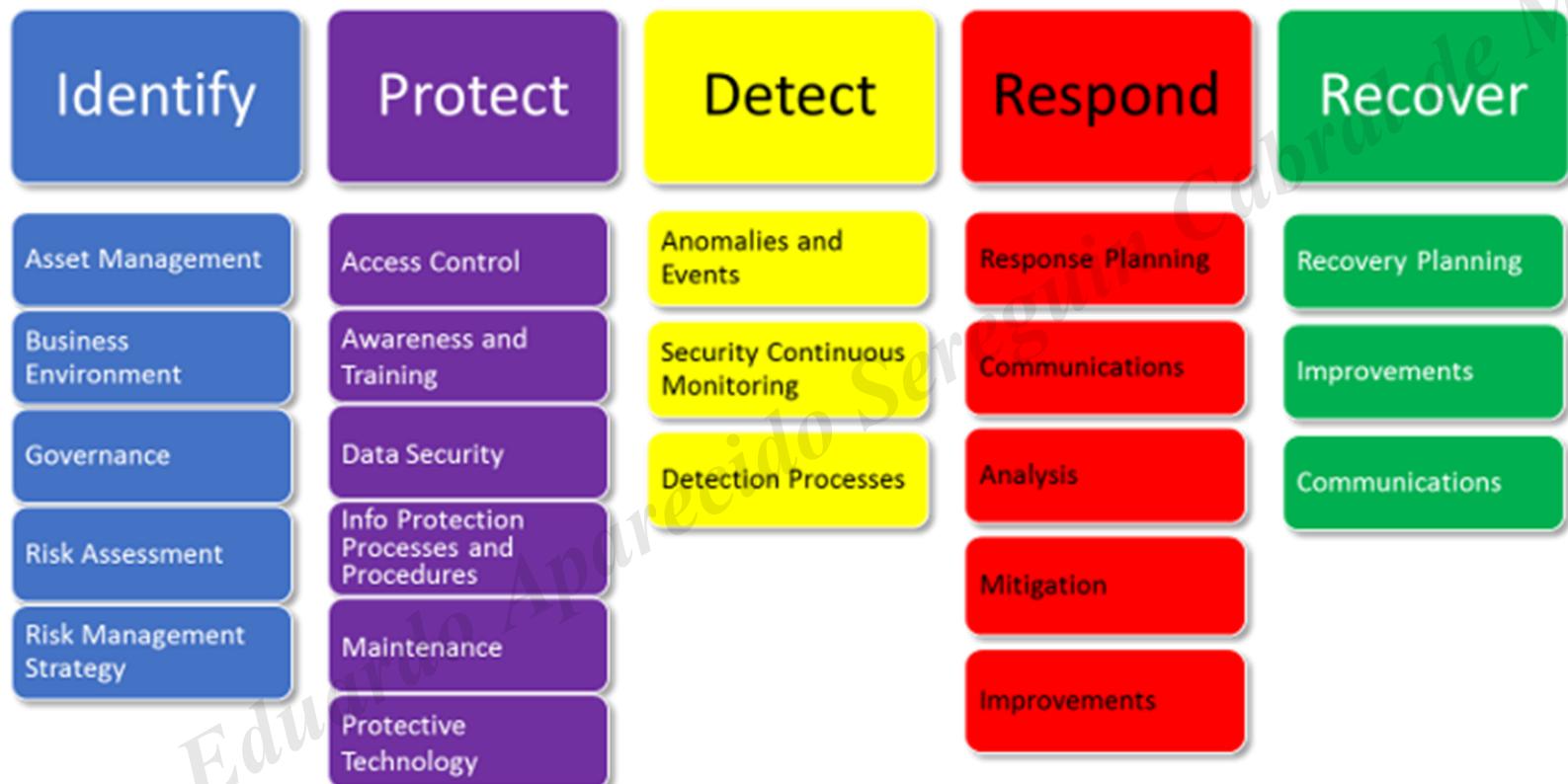


*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

NIST CSF / Framework

NIST Cyber Security Framework



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

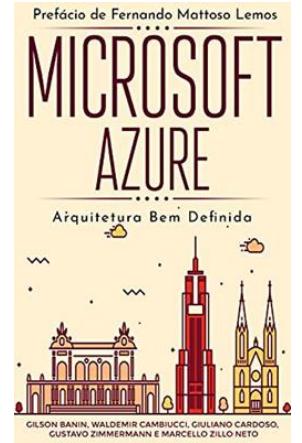
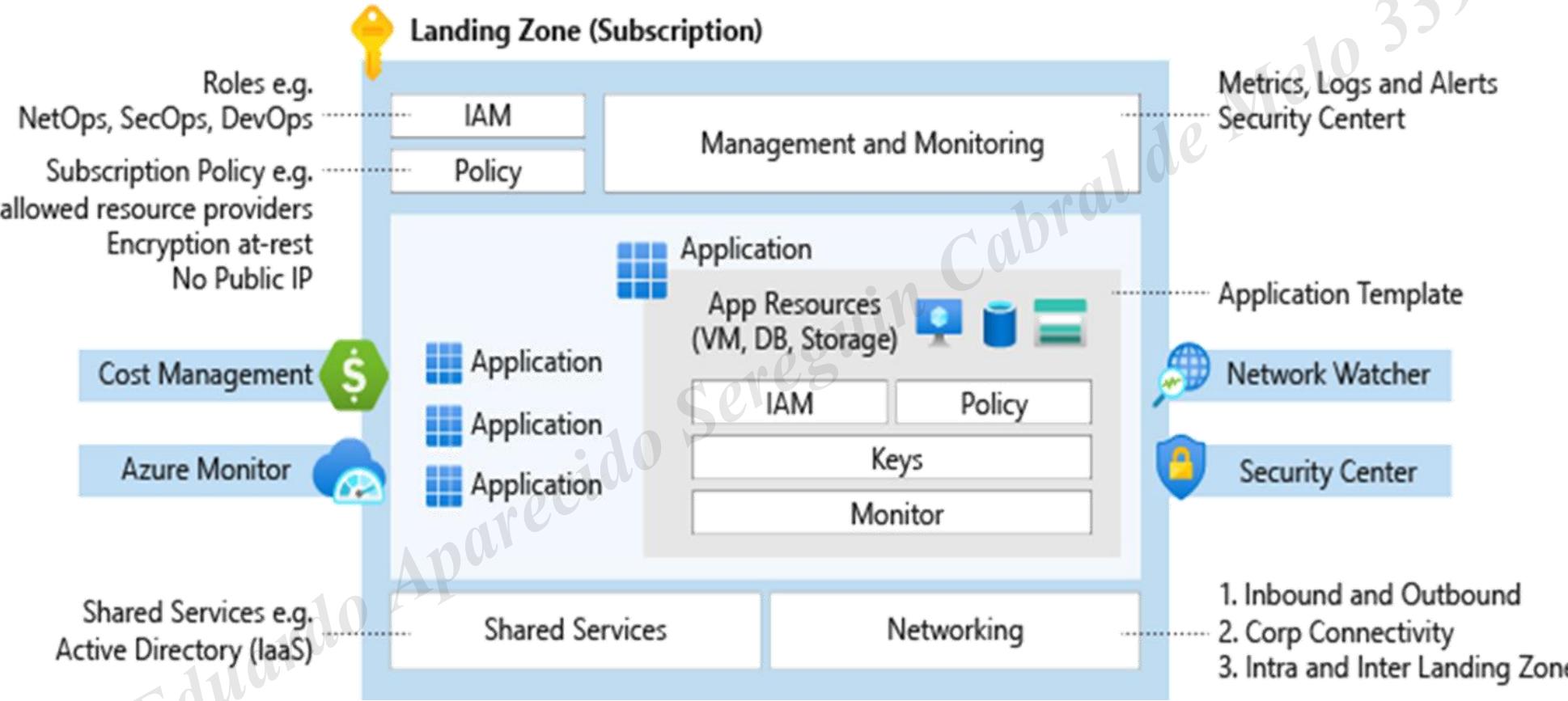
The total or partial reproduction of this material without authorization is prohibited.

Azure journey

Acionável, Holístico, Curto e longo prazo



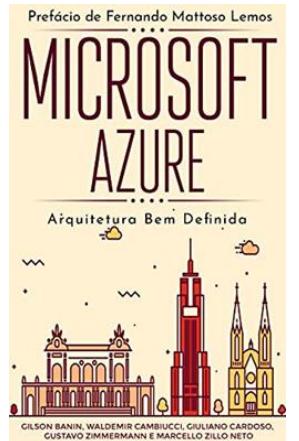
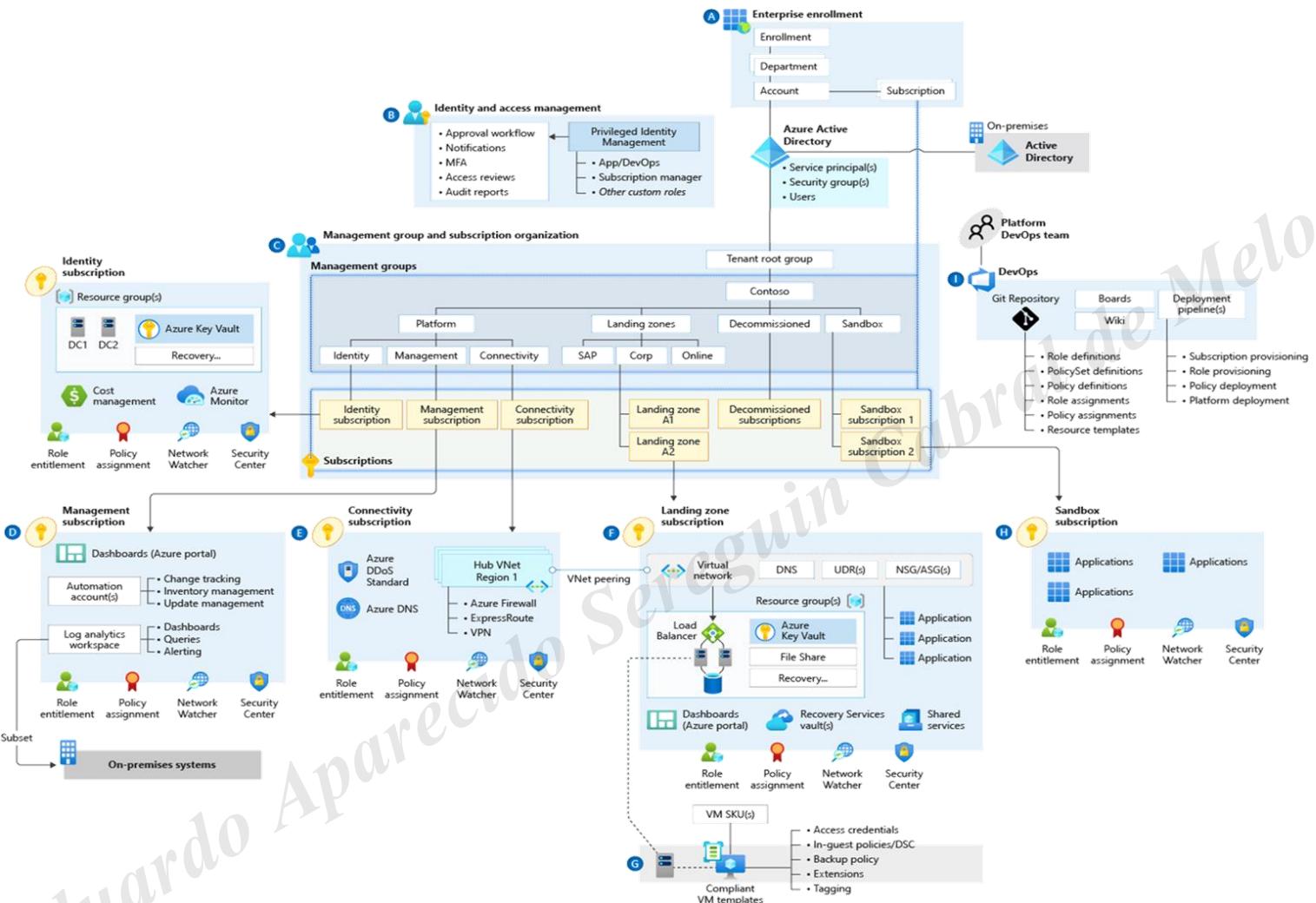
Recommended Book



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

Recommended Book



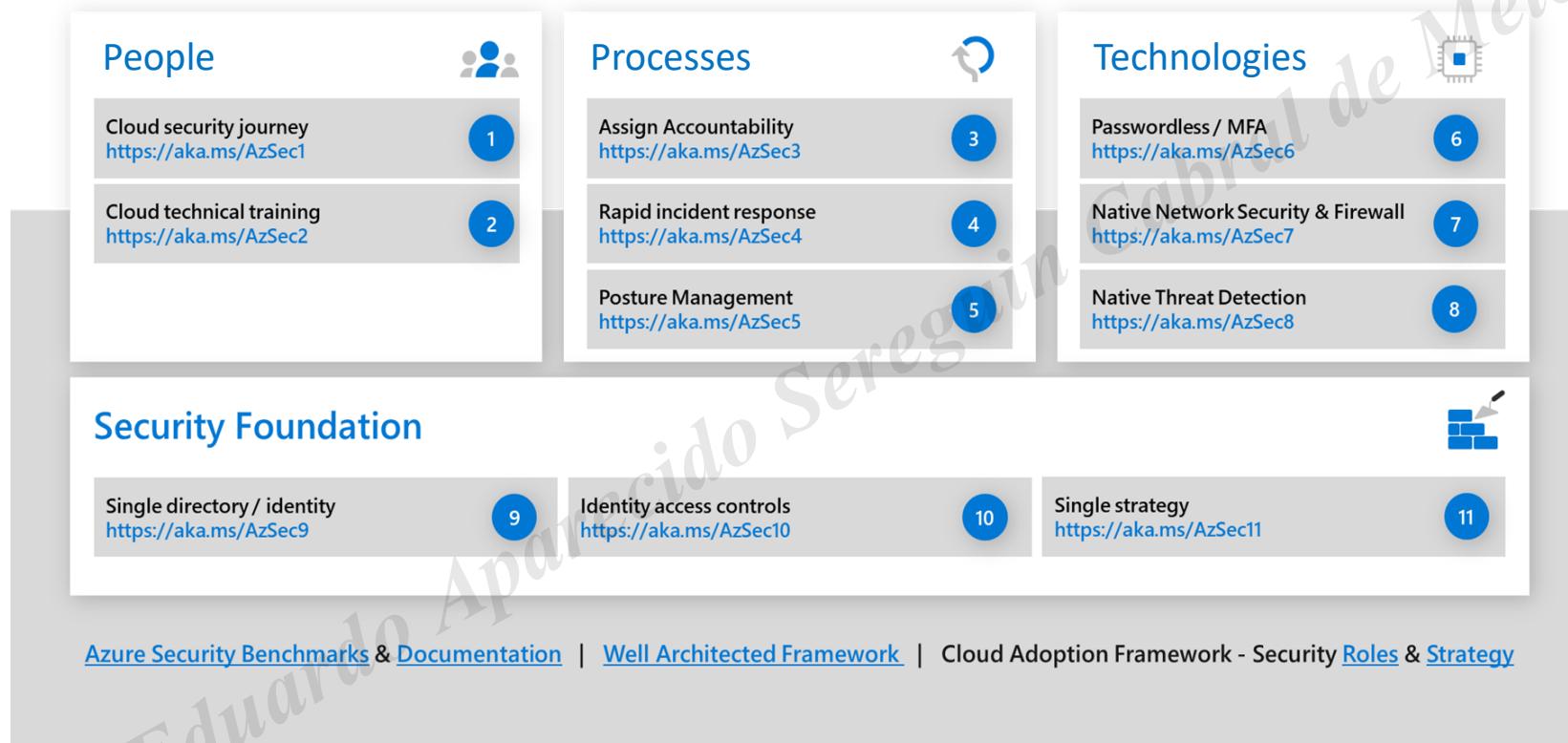
<https://github.com/Azure/Enterprise-Scale>

*The responsibility for any conditions or originality of work rests with the author(s) and not the professor.

Security Best Practices

Top 10 (+1) Best Practices

<https://aka.ms/AzureSecurityTop10>



*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

AWS Analytics Services

The screenshot shows the AWS Analytics Services landing page. At the top, there's a navigation bar with links for Products, Solutions, Pricing, Documentation, Learn, Partner Network, AWS Marketplace, Customer Enablement, Events, Explore More, and a search icon. To the right are Contact Us, Support, English, My Account, Sign In, and a prominent orange "Create an AWS Account" button. Below the navigation is a banner with the text "Analytics on AWS" and a large number "200,000+ data lakes run on AWS". The banner also features five cards with icons and text: "faster with Amazon EMR than standard Apache Spark", "better price performance than other cloud data warehouses", "savings on storage cost for data in data lakes", and "of data storage in a single cluster with Amazon OpenSearch Service". The main content area is titled "AWS analytics services" and contains a table. The table has three columns: "Category", "Use cases", and "AWS service". The "Category" column lists "Analytics" and "Data movement". The "Use cases" column lists various scenarios like Interactive analytics, Big data processing, Data warehousing, etc. The "AWS service" column lists nine services with their respective icons: Amazon Athena, Amazon EMR, Amazon Redshift, Amazon Kinesis, Amazon OpenSearch Service, Amazon Quicksight, AWS Glue DataBrew, AWS Glue, and Amazon Managed Streaming for Apache Kafka (MSK). A large AWS logo is visible on the right side of the page.

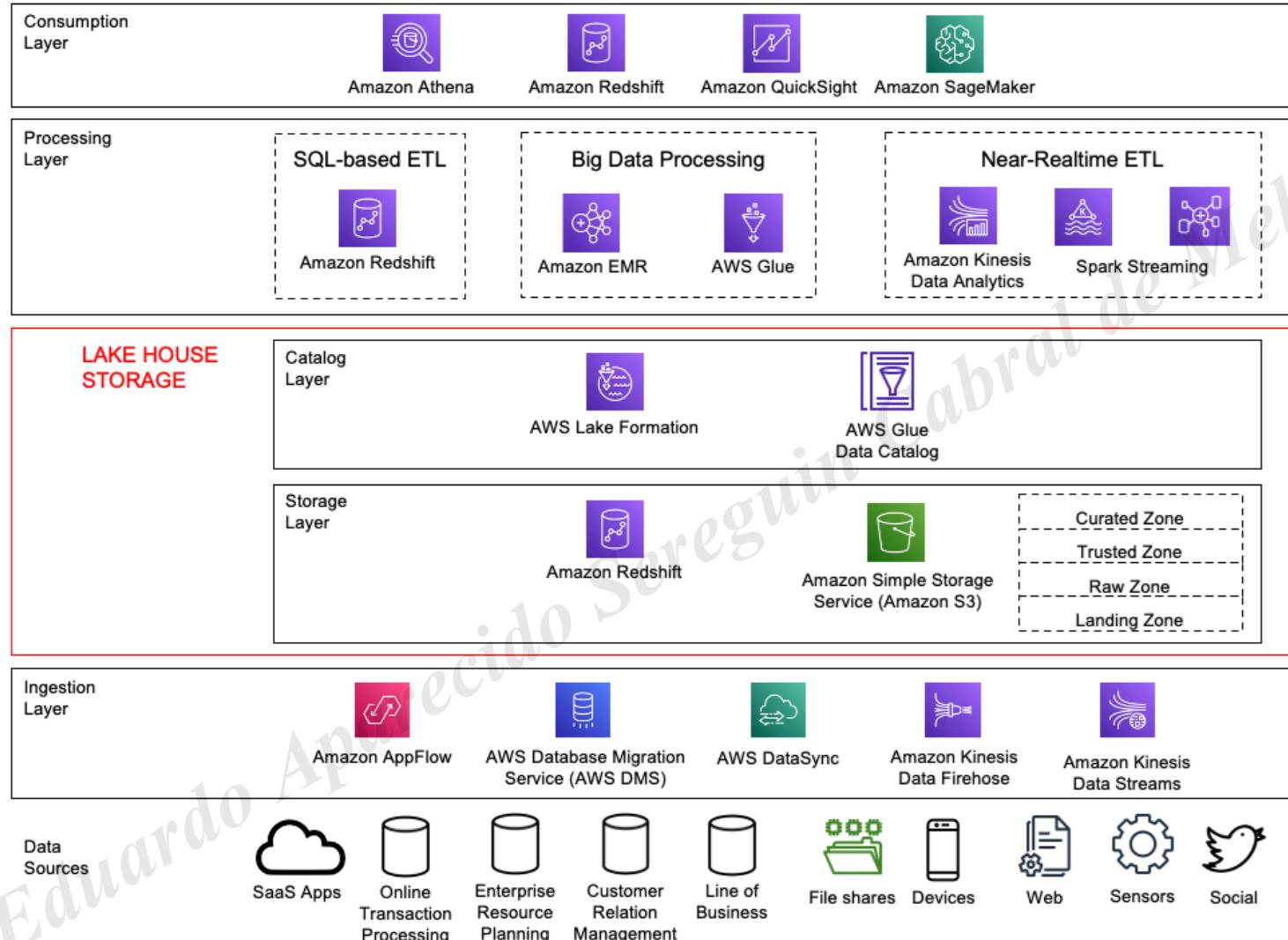
Category	Use cases	AWS service
Analytics	Interactive analytics Big data processing Data warehousing Interactive analytics Operational analytics Dashboards and visualizations Visual data preparation	Amazon Athena Amazon EMR Amazon Redshift Amazon Kinesis Amazon OpenSearch Service Amazon Quicksight AWS Glue DataBrew
Data movement	Real-time data movement	AWS Glue Amazon Managed Streaming for Apache Kafka (MSK)

<https://aws.amazon.com/big-data/datalakes-and-analytics/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

AWS Analytics Architecture



*The responsibility for the correctness and quality of the didactic content included is the responsibility of the professor.
<https://aws.amazon.com/blogs/big-data/new-available-deeply-detailed-guidance-on-the-data-analytics-lens-for-aws-well-architected-framework/>

Azure Analytics Services

 Azure Explore Products Solutions Pricing Partners Resources

Search 

Docs Support Contact Sales [Free account](#) Sign in

Analytics

A comprehensive set of solutions that turn your data into actionable insights

Find the analytics product you need

IF YOU WANT...	USE THIS
Limitless analytics with unmatched time to insight	Azure Synapse Analytics
A fully managed, fast, easy and collaborative Apache® Spark™ based analytics platform optimized for Azure	Azure Databricks
A fully managed cloud Hadoop and Spark service backed by 99.9% SLA for your enterprise	HDInsight
A data integration service to orchestrate and automate data movement and transformation	Azure Data Factory
Open and elastic AI development spanning the cloud and the edge	Azure Machine Learning
Real-time data stream processing from millions of IoT devices	Azure Stream Analytics
A fully managed on-demand pay-per-job analytics service with enterprise-grade security, auditing, and support	Data Lake Analytics
Enterprise grade analytics engine as a service	Azure Analysis Services

<https://azure.microsoft.com/en-us/product-categories/analytics/>

The total or partial reproduction of this material without authorization is prohibited.



Azure Analytics Architecture

Filter

Search Search

Clear all

AI + Machine Learning × Analytics × Databases × Storage ×

Products

Find a product

- ✓ .NET
- ✓ Azure
- Dynamics
- ✓ Dynamics 365
- GitHub
- ✓ Microsoft Power Platform
- ✓ Office
- Office 365
- SQL Server

Categories

Find a category

284 results

ARCHITECTURE
Automate document processing by using Azure Form Recognizer

Extraction

Trigger

Azure Blob Storage

Azure Functions

Azure Cosmos DB

Other sources of data

Attachments (email or social media app)

File ingestion

Browser

Azure Application Firewall

Azure Application Gateway

Back-end application

Azure Form Recognizer

ARCHITECTURE
Multiparty computing architecture design

User

SQL

Ledger view

Back-end application



If you forgot everything that I said

1. Remember about SofA
2. Think on the pillars of the cloud adoption and how to create an embracing plan.
3. Think on a migration by steps, improving the operation, management and with native application in cloud posteriorly or in parallel.
4. Don't be Doctor No, it is possible to adopt safely.

If you forgot everything that I said

5. Understand and discuss the shared responsibility model, understand the services that will be used.
6. Evaluate the relevant regulations and certificates for your company for contractual matters.
7. Define governance model and review your BIA, PCN, DR.
8. Define the requirements / principles for adopting cloud safely.

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

The total or partial reproduction of this material without authorization is prohibited.

If you forgot everything that I said

9. Integrate with internal framework already existing – NIST CSF.
10. Remember security in technologies as LAMBDA.
11. Enjoy the RIDE → The NEW SECURITY AND BETTER WORLD.

Final thoughts

- Segurança na nuvem tem que ser top-down

- Restrinja acesso de **Pessoas** aos dados.
- Comece pelo básico/ **Patching / Log / Proteção de credencias**
- **Encryption ... I see encryption everywhere.**

- Crie indicadores de performance (exemplos)

- **Appsec reviews**
- Índice de **Automação**
- Auditorias de **terceiros**
- Conformidade com **SLA**
- Tempo para coleta de **métricas**.

Biography & References

- CSSP Official Study Guide

by Brian T 'O Hara

Ben Mailsow

- AWS Well Architected

<http://tinyurl.com/y7ataqo9>

- AWS Well Architected Security Pillar

<http://tinyurl.com/y2k87dwv>

- AWS CAF – Cloud Adoption framework

<https://aws.amazon.com/pt/professional-services/CAF/>

*The responsibility for trustworthiness, originality, and legality of the didactic content presented is responsibility of the professor.

Biography & References

- NIST SCF Framework

<https://www.nist.gov/cyberframework>

- NIST SCF on AWS

<http://tinyurl.com/y43cjtlp>

- AWS Compliance programs

<https://aws.amazon.com/pt/compliance/programs/>

- MS Compliance programs

<http://tinyurl.com/y4vue42s>

Biography & References

- Cloud security Alliance

<https://cloudsecurityalliance.org/>

- CSA Questionnaire AWS

<http://tinyurl.com/y539z5fq>

- CSA Questionnaire MS

<http://tinyurl.com/y3efgkjq>

- Google Compliance reports.

<https://cloud.google.com/security/compliance/#/>

Biography & References

- AWS Migration

<https://aws.amazon.com/pt/cloud-migration/>

- Resolução 4.658

<http://tinyurl.com/y7aapn2k>

- Resolução 3.909

<http://tinyurl.com/y3fdterc>

- LGPD

http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Biography & References

- Serviços de Segurança AWS

<https://aws.amazon.com/pt/products/security/>

- Serviços de Segurança MS

<https://azure.microsoft.com/en-us/product-categories/security/>

Biography & References

- **Cloud-Based Services Are Making It Easier for Companies to Use AI**

<https://hbr.org/sponsored/2019/03/cloud-based-services-are-making-it-easier-for-companies-to-use-ai>

- **Adopting Hybrid Cloud Becomes a Strategic Imperative**

<https://hbr.org/2017/09/adopting-hybrid-cloud-becomes-a-strategic-imperative>