

Cloud Bootcamp

Menina de Cybersec



Fundamentos de segurança na nuvem



Cloud Bootcamp MCS - 2025

Fundamentos de segurança na nuvem



Responsabilidade compartilhada



Fundamentos de segurança na nuvem



Responsabilidade compartilhada

- Segurança **DA** nuvem
- Segurança **NA** nuvem



Fundamentos de segurança na nuvem



Segurança **DA** nuvem


- **O provedor é responsável por:**
 - Segurança física dos datacenters
 - Infraestrutura global (zonas de disponibilidade, rede, energia, etc.)
 - Hardware e virtualização
 - Serviços gerenciados (patch de hosts, storage físico)
- **Garantias do provedor:**
 - Certificações como ISO 27001, SOC2, PCI-DSS
 - SLAs e disponibilidade
 - Monitoramento físico 24/7



Fundamentos de segurança na nuvem



Segurança **NA** nuvem

- O **cliente** é responsável por:
 - Configuração correta dos serviços
 - Gestão de identidades e acessos (IAM)
 - Criptografia e controle de dados sensíveis
 - Patching de sistemas em EC2 (SO, apps, middleware)
 - Configuração de segurança de rede (SG, NACL, VPC)
 -
-  Erros comuns:
 - Buckets S3 públicos sem querer
 - EC2 com SSH aberto (0.0.0.0/0)
 - IAM roles com permissões amplas demais (ex: AdministratorAccess)



Fundamentos de segurança na nuvem



Responsabilidade por modelo (IaaS, PaaS, SaaS)



Responsabilidade por modelo (IaaS, PaaS, SaaS)

- **IaaS** (Infra como Serviço) → Você gerencia quase tudo
- **PaaS** (Plataforma como Serviço) → Você gerencia dados e lógica
- **SaaS** (Software como Serviço) → Você gerencia acesso e uso

Serviço	Modelo	Responsabilidade AWS	Responsabilidade Cliente
Amazon EC2	IaaS	Hardware, rede, virtualização	SO, app, patch, IAM, Security Groups, dados
Amazon RDS	PaaS	SO, banco, backup, alta disponibilidade	Acesso aos dados, criptografia, roles, monitoramento
AWS Lambda	PaaS	Infraestrutura, runtime, scaling	Lógica da função, permissões, dados
Amazon WorkSpaces	SaaS	Infra, SO, manutenção da plataforma	Acesso, políticas, criptografia, versionamento
Amazon QuickSight	SaaS	Infra, engine de BI, patch automático	Dados enviados, permissões de usuários



Frameworks de segurança em Cloud



Cloud Bootcamp MCS - 2025

Frameworks de segurança em Cloud



Por que seguir frameworks de segurança?



Por que seguir frameworks de segurança?

- Reduz **riscos** ao seguir práticas reconhecidas globalmente
- Facilita **auditorias** e certificações (LGPD, ISO 27001, SOC2 etc.)
- Evita “reinventar a roda” e garante **consistência** na segurança



Introdução ao CIS Benchmarks



- Criado pelo Center for Internet Security (CIS)
- Regras práticas para **hardening** de sistemas e serviços (incluindo AWS, Linux, Windows)
- CIS **AWS** Foundations Benchmark: foco em práticas essenciais (CloudTrail, MFA, logs, segurança de rede, etc.)



Introdução ao CIS Benchmarks



Exemplos:

- "CIS 1.1 – Garantir que **CloudTrail** esteja habilitado em todas as regiões"
- "CIS 1.20 – Garantir que não existam **Security Groups** permitindo 0.0.0.0/0 na porta 22"



Introdução ao NIST



- National Institute of Standards and Technology (**NIST**)
- NIST Cybersecurity Framework (CSF): usado **globalmente**, até fora dos EUA
- Organizado em 5 funções: **Identify**, Protect, **Detect**, Respond, **Recover**



Introdução ao CIS Benchmarks



Exemplos:

- Permite **alinhar** ações técnicas (como **IAM** e monitoramento) a metas estratégicas de **segurança**



Frameworks de segurança em Cloud



Framaework	Objetivo	Aplicação na AWS
CIS Benchmarks	Hardening técnico por serviço	Checklist técnico (Prowler, Security Hub)
NIST CSF	Visão estratégica e organizacional	Gestão de riscos e políticas corporativas
ISO 27001	Certificação de segurança da informação	Avaliação contínua e auditorias
AWS Well-Architected (Security Pillar)	Boas práticas de arquitetura segura	Guia direto da AWS para workloads



Dúvidas



Obrigado



@luizmachadoaws

