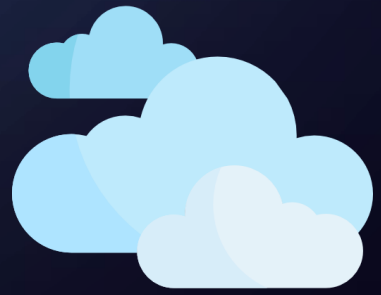
RESPONSABILIDADE COMPARTILHADA NA AWS

A AWS E O CLIENTE TÊM PAPÉIS DISTINTOS NA SEGURANÇA E CONFORMIDADE DA NUVEM. ESSA DIVISÃO É CONHECIDA COMO **MODELO DE RESPONSABILIDADE COMPARTILHADA.**

por Thays Lira



MODELO DE RESPONSABILIDADE COMPARTILHADA

- **AWS** – Responsável pela **segurança da nuvem**, incluindo infraestrutura global, hardware, software e serviços principais.

- **Cliente** – Responsável pela **segurança na nuvem**, incluindo configuração de permissões, proteção de dados, criptografia e gestão de acesso.

por Thays Lira

Modelo de Responsabilidade Compartilhada na AWS

AWS

Segurança da Nuvem

- Infraestrutura Global
- Hardware
- Software
- Serviços Principais

Cliente

Segurança na Nuvem

- Configuração de Permissões
- Proteção de Dados
- Criptografia
- Gestão de Acesso

por Thays Lira

EXEMPLO PRÁTICO: PROTEÇÃO DE UM SITE NA AWS

📌 **Situação:** Uma empresa hospeda seu site em um servidor EC2 e armazena dados no Amazon S3.

AWS

✅ Infraestrutura segura dos servidores e data centers.

✅ Proteção física e redundância dos sistemas.

Cliente

✅ Configuração correta das permissões no **IAM** para evitar acessos indevidos.

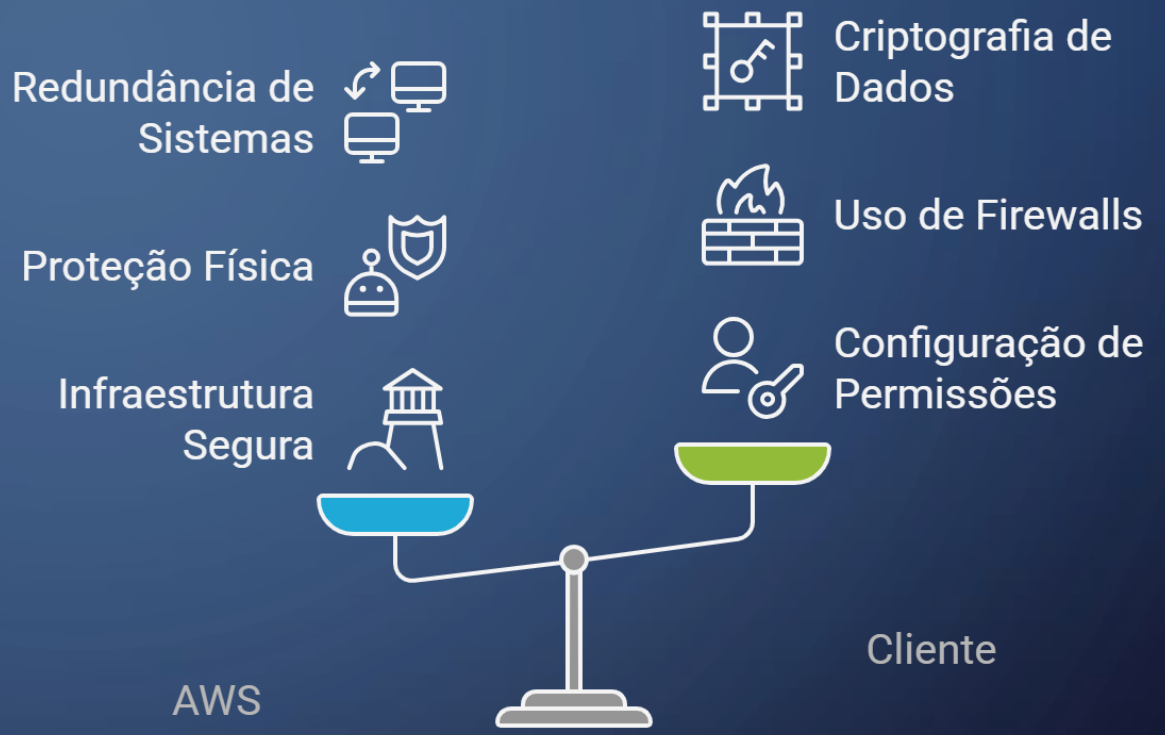
✅ Uso de **firewalls e grupos de segurança** para proteger a instância EC2.

✅ Criptografia dos dados no **S3** para garantir privacidade

por Thays Lira

CONCLUSÃO:

A AWS fornece uma infraestrutura confiável, mas cabe ao cliente configurar corretamente os serviços para garantir a proteção dos dados.



Equilibrando Responsabilidades de Segurança na Nuvem

por Thays Lira

MELHORES PRÁTICAS:

Para garantir que a responsabilidade compartilhada na AWS seja bem aplicada:

- **Entender o modelo** – Saiba exatamente quais aspectos da segurança são gerenciados pela AWS e quais são sua responsabilidade como cliente.
- **Gerenciamento de identidade e acesso (IAM)** – Use **privilégios mínimos** para garantir que usuários e serviços tenham apenas as permissões necessárias.
- **Proteção de dados** – Implemente **criptografia** para dados em trânsito e em repouso, além de configurar backups regulares.
- **Monitoramento e auditoria** – Utilize ferramentas como **AWS CloudTrail** e **AWS Config** para rastrear atividades e garantir conformidade.
- **Configuração segura** – Certifique-se de que **grupos de segurança** e **firewalls** estejam corretamente configurados para evitar acessos indevidos.
- **Atualizações e patches** – Mantenha **sistemas operacionais** e **aplicativos** sempre atualizados para evitar vulnerabilidades.

por Thays Lira