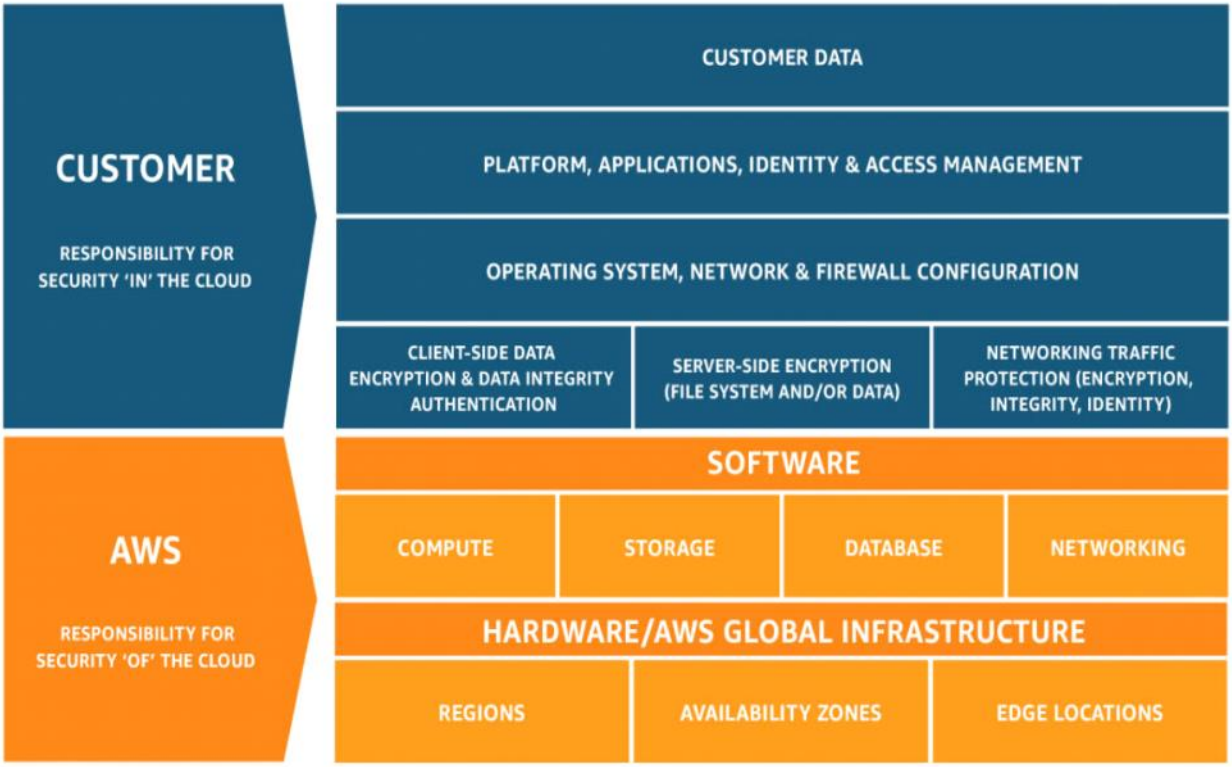
02.AWS Share Responsability Model

terça-feira, 28 de novembro de 2023 18:48

- **Modelo de responsabilidade compartilhada**
- **AWS** - responsável pela segurança "da" nuvem - AWS Fica responsável por manter a segurança de toda infraestrutura física.
- **Cliente** - responsável pela segurança "na" nuvem - Fica responsável por segurança de serviços na nuvem



AWS

- **Compute, Storage, Database e Networking** - O Cliente não precisa ficar preocupado quanto a segurança destes, além da segurança das estruturas físicas como Regions, Availability zones e Edge Locations

Cliente

- **Customer Data -** Tipos de dados que você armazena na nuvem, dados proibidos, fotos proibidas por lei.
- **Platform, Applications, Identity e Acess Management** - Instalação de alguma aplicação impropria ou duvidosa, ou até publica suas credenciais em sites a AWS não se responsabiliza.
- **Operating System, Network e Firewall Configuration** - A configuração do sistema operacional, configuração da parte de rede e do firewall é por sua conta.
- **Encryption client-side** - Encriptação do lado do cliente
- **Encryption server-side** - Encriptação do lado do servidor (VM)
- **Networking Traffic Protection** - Proteção de trafego de conexão

Compartilhamento AWS e Cliente

- Dependendo do tipo de serviço da AWS que está sendo usado (por exemplo, uma instância EC2 versus um banco de dados RDS), a AWS e o cliente compartilharão diferentes partes da responsabilidade de segurança. Por exemplo, para um serviço de infraestrutura como o EC2, a AWS fornece a segurança física, a do hypervisor e a da rede, enquanto o cliente é responsável pelo sistema operacional e pelas aplicações. Para um serviço de contêiner como o RDS, a AWS também é responsável pela segurança do sistema operacional e do serviço de banco de dados, enquanto o cliente ainda é responsável pelas aplicações e dados.