Contents

[**SECURITY** 1](#_Toc140749395)

[**Modelo de responsabilidade compartilhada** 1](#_Toc140749396)

[**AWS Organizations** 1](#_Toc140749397)

[**AWS Artifact** é um serviço que fornece acesso sob demanda a relatórios de segurança e conformidade da AWS e a contratos on-line selecionados. O AWS Artifact tem duas seções principais: AWS Artifact Agreements e o AWS Artifact Reports. 2](#_Toc140749398)

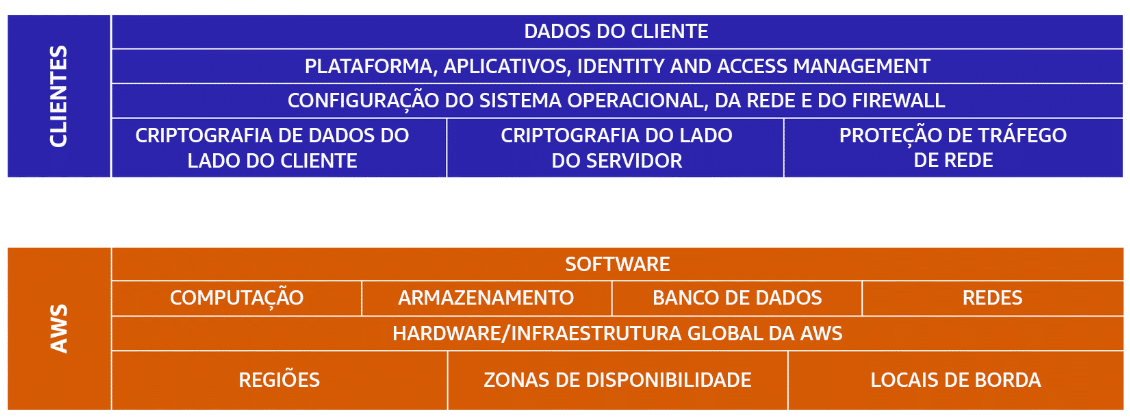
[**DDoS ou DDoS. Negação de serviço distribuída.** 3](#_Toc140749399)

[**AWS Key Management Service (AWS KMS)** 3](#_Toc140749400)

[**AWS WAF** 4](#_Toc140749401)

# **SECURITY**

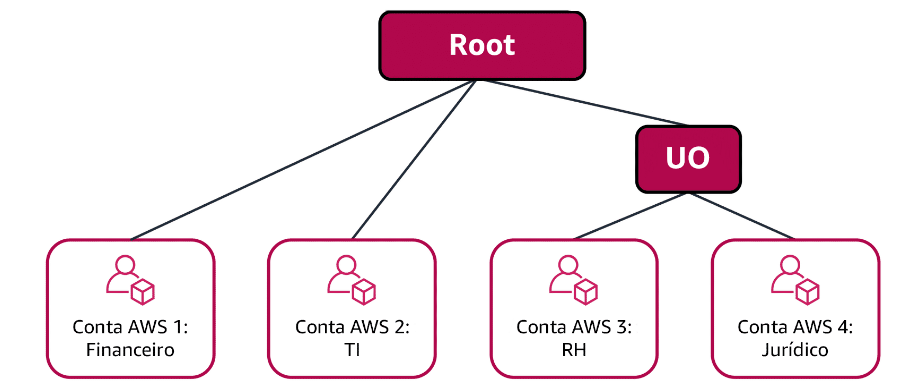
## **Modelo de responsabilidade compartilhada**



## **AWS Organizations**

A maneira mais fácil de pensar no Organizations é como um local central para gerenciar várias contas da AWS.

principais recursos:

* gerenciamento centralizado de todas as suas contas na AWS. Outra vantagem do faturamento consolidado é o desconto em massa.
* agrupamento hierárquico de suas contas para atender a requisitos de segurança, conformidade ou necessidades orçamentais, Isso significa que você pode agrupar contas em unidades organizacionais, ou OUs, tipos de negócios ou business units. 
* faturamento consolidado de todas as contas de membros.  você pode usar a conta principal da sua organização para consolidar e pagar todas as contas de outros membros.
* controle sobre serviços da WS e as ações de API. Cada conta pode acessar como administrador da conta principal de uma organização.

cobrança consolidada é outro recurso do AWS Organizations

## [**AWS Artifact**](https://aws.amazon.com/artifact) é um serviço que fornece acesso sob demanda a relatórios de segurança e conformidade da AWS e a contratos on-line selecionados. O AWS Artifact tem duas seções principais: AWS Artifact Agreements e o AWS Artifact Reports.

Vc pode **Acessar relatórios de conformidade da AWS sob demanda. Analisar, aceitar e gerenciar seus contratos com a AWS.**

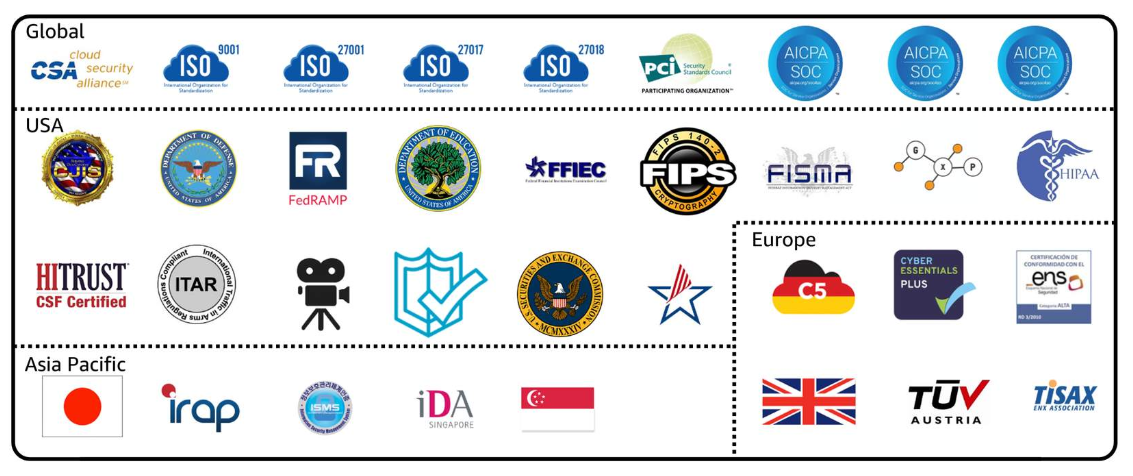
* **AWS Artifact Agreements**

Suponha que sua empresa precise assinar um contrato com a AWS em relação ao uso de determinados tipos de informações em todos os serviços AWS. Você pode fazer isso pelo **AWS Artifact Agreements**.  
No AWS Artifact Agreements, você pode revisar, aceitar e gerenciar contratos para uma conta individual e para todas as suas contas no AWS Organizations. Diferentes tipos de acordos são oferecidos para atender às necessidades dos clientes sujeitos a regulamentações específicas, como a Lei de Portabilidade e Responsabilidade dos Provedores de Saúde dos EUA (HIPAA).

* **AWS Artifact Reports**

Suponha que um membro da equipe de desenvolvimento da sua empresa esteja criando um aplicativo e precise de mais informações sobre a responsabilidade em cumprir determinados padrões regulatórios. Você pode recomendar o acesso a essas informações em **AWS Artifact Reports**.  
O AWS Artifact Reports fornece relatórios de conformidade por auditores terceirizados. Esses auditores testaram e verificaram se a AWS está em conformidade com diversas normas e regulamentações de segurança globais, regionais e específicas do setor. O AWS Artifact Reports se mantém atualizado com os relatórios publicados mais recentes. Você pode fornecer os artefatos de auditoria da AWS aos auditores ou reguladores como evidência dos controles de segurança da AWS.

O [**Centro de conformidade para o cliente**](https://aws.amazon.com/compliance/customer-center/) contém recursos que ajudam você a saber mais sobre a conformidade da AWS.



## **DDoS ou DDoS. Negação de serviço distribuída.**

Em um ataque DDoS, o agente mal-intencionado tenta sobrecarregar a capacidade da sua aplicação para que qualquer outra requisição que ocorra nos seus serviços seja negada.

**AWS Shield Standard** protege automaticamente todos os clientes AWS sem nenhum custo. Ele protege seus recursos AWS contra os tipos de ataques DDoS mais comuns e frequentes.  
À medida que o tráfego de rede ingressa em seus aplicativos, o AWS Shield Standard usa diversas técnicas de análise para detectar tráfego mal-intencionado em tempo real e mitigá-lo automaticamente.

O **AWS Shield Advanced** é um serviço pago que fornece diagnósticos detalhados de ataques e a capacidade de detectar e mitigar ataques elaborados de DDoS.  
Ele também se integra a outros serviços, como o Amazon CloudFront, o Amazon Route 53 e o Elastic Load Balancing. Além disso, você pode integrar o AWS Shield ao AWS WAF escrevendo regras personalizadas para mitigar ataques complexos de DDoS.

## [**AWS Key Management Service (AWS KMS)**](https://aws.amazon.com/kms)

permite que você execute operações de criptografia pelo uso de **chaves de criptografia**. Uma chave de criptografia é uma cadeia aleatória de dígitos usada para bloquear (criptografar) e desbloquear (descriptografar) dados. Você pode usar o AWS KMS para criar, gerenciar e usar chaves de criptografia. Você também pode controlar o uso de chaves em uma ampla gama de serviços e em seus aplicativos.

você deve garantir que os dados de seus aplicativos estejam protegidos durante o armazenamento **(criptografia em repouso)** e sendo transmitidos **(criptografia em trânsito)**.

## [**AWS WAF**](https://aws.amazon.com/waf)

é um firewall de aplicativo web que permite monitorar solicitações de rede que entram em seus aplicativos web.

O AWS WAF trabalha em conjunto com o Amazon CloudFront e um balanceador de carga de aplicativo. Lembre-se das listas de controle de acesso de rede que você aprendeu em um módulo anterior. O AWS WAF funciona de forma semelhante para bloquear ou permitir o tráfego. No entanto, ele faz isso usando uma [**lista de controle de acesso (ACL) da web**](https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html) para proteger seus recursos AWS.

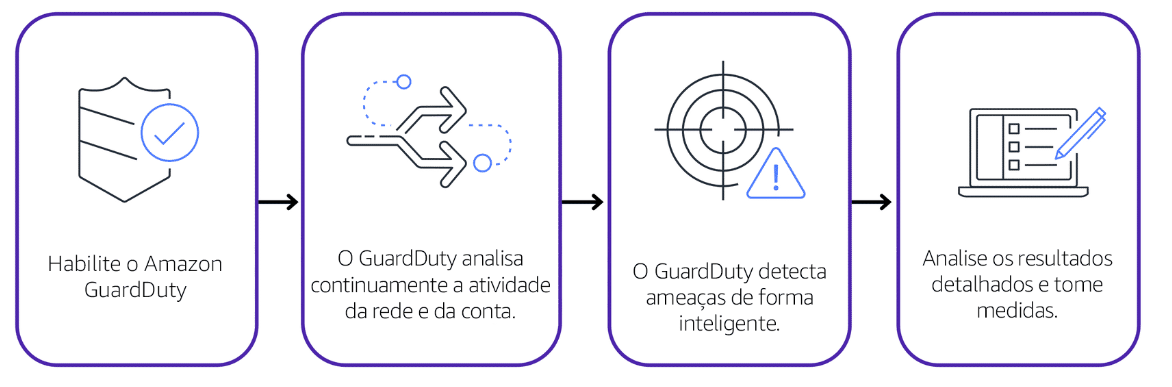
Veja um exemplo de como você pode usar o AWS WAF para permitir e bloquear solicitações específicas.

Suponha que o aplicativo tenha recebido solicitações de rede mal-intencionadas de vários endereços IP. Você quer impedir que essas solicitações continuem a acessar seu aplicativo, mas também deseja garantir que usuários legítimos ainda possam acessá-lo. Você configura a ACL da web para permitir todas as solicitações, exceto aquelas dos endereços IP que você especificou.

Quando uma solicitação entra no AWS WAF, ele confere a lista de regras configurada na ACL da web. Se uma solicitação não for proveniente de um dos endereços IP bloqueados, o AWS WAF permite o acesso ao aplicativo.

[**Amazon GuardDuty**](https://aws.amazon.com/guardduty)

é um serviço que fornece detecção inteligente de ameaças para sua infraestrutura e seus recursos AWS. Ele identifica ameaças monitorando continuamente a atividade da rede e o comportamento da conta no seu ambiente AWS.



Depois de habilitar o GuardDuty para sua conta AWS, ele começa a monitorar sua atividade de rede e conta. Você não precisa implantar ou gerenciar nenhum outro software de segurança. O GuardDuty analisa continuamente dados de várias fontes da AWS, incluindo logs de fluxo de VPC e logs de DNS.

Se ele detectar ameaças, você poderá revisar as descobertas detalhadas no AWS Management Console. As descobertas incluem etapas recomendadas para a correção. Você também pode configurar as funções do AWS Lambda para executar as etapas de correção automaticamente em resposta às descobertas de segurança do GuardDuty.

O Amazon GuardDuty é um serviço de detecção de ameaças(não causa raiz) que monitora continuamente suas contas e workloads da para detectar atividade maliciosa e fornece resultados de segurança detalhados para visibilidade e correção.

<https://aws.amazon.com/guardduty/?nc2=h_ql_prod_se_gd>

<https://aws.amazon.com/pt/guardduty/?nc2=type_a>

<https://aws.amazon.com/pt/guardduty/>

**Amazon Macie**

O Amazon Macie é um serviço de segurança e privacidade de dados totalmente gerenciado que usa machine learning e correspondência de padrões para descobrir e proteger seus dados confidenciais na AWS. À medida que as organizações gerenciam volumes crescentes de dados, identificar e proteger seus dados confidenciais em escala pode se tornar cada vez mais complexo, caro e demorado.

<https://aws.amazon.com/macie/?nc2=h_ql_prod_se_ma>

**AWS Well-Architected**

A AWS Well-Architected ajuda arquitetos de nuvem a construir infraestruturas seguras, resilientes, eficientes e de alta performance para aplicações e workloads. Baseado em seis pilares (excelência operacional, segurança, confiabilidade, eficiência de performance, otimização de custos e sustentabilidade), o AWS Well-Architected fornece uma abordagem consistente para que clientes e parceiros avaliem arquiteturas e implementem designs que podem se expandir com o tempo.

**AWS Well-Architected possui 6 pilares**

* Pilar Excelência operacional
* Pilar Segurança
* Pilar Confiabilidade
* Pilar Eficiência de performance
* Pilar Otimização de custos

Pilar Sustentabilidade

<https://aws.amazon.com/pt/architecture/well-architected/?nc1=h_ls>

<https://docs.aws.amazon.com/pt_br/wellarchitected/latest/framework/introduction.html>

<https://aws.amazon.com/pt/architecture/well-architected/>

**Amazon Inspector**

É um agente que faz varredura em instancia EC2 para encontrar vulnerabilidade de segurança.

**Segurança Dados em Transito**

A transferência de dados de entrada e saída da sua infra estrutura AWS. A seguranção de dados em transito é através dos protocolos de segurança.

* SSL/TLS pela web
* IPSec para conexões on-premises
  + VPN
  + AWS Direct Connect
* Importar e exportar dados com Snowball

Os dados transferia via apis da AWS

* As chamadas de apis da aws usam o protocolo HTTPS

Todas as chamadas são assinadas com Sigv4

**Segurança Dados em Repouso**

Os dados armazenados (em repouso) dentro da infra estrutura da AWS são seguros pois utilizam criptografias e chave de acesso privadas.

Os dados armazenados no S3 são privados por padrão e exige credenciais da aws para serem acessados.

* OS acesos aos objetos do S3 são realizados via protocolo HTTP ou HTTPS.
* Possui auditoria de acesso de todos os objetos (Configurados)
* È permitido criar politicas baseadas em recursos como por exemplo:
  + Buckets
  + Prefixos (diretório/pasta) dentro do bucket

<https://aws.amazon.com/pt/iam/features/?nc=sn&loc=2>

<https://aws.amazon.com/pt/iam/faqs/?nc=sn&loc=5>

<https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/best-practices.html>

<https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/IAMBestPracticesAndUseCases.html>

**Criptografia de dados**

OS dados podem ser criptografa de 2 modos, do lado do servidor e do lado do cliente.

* **Criptografia no lado do servidor**
  + Chaves gerenciadas pelo Amazon SE (SSE-S3)
  + Chaves gerenciadas pela AWS KMS (SSE-KMS)
  + Chaves providas pelo cliente (SSE-C)
* **Criptografia no lado do cliente**
  + Chave primária do cliente gerenciada pela AWS KMS (CSE-KMS)

Chave primária do lado do cliente (CSE-C)

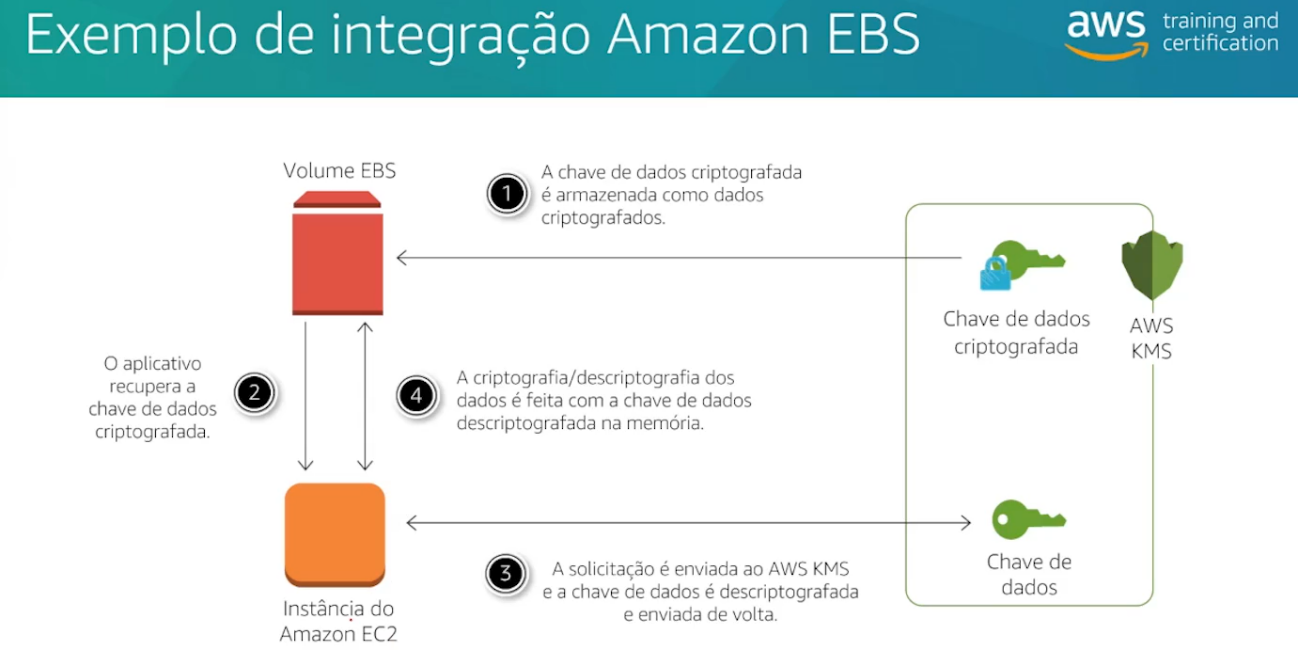
**AWS KMS (Key Management Service)**

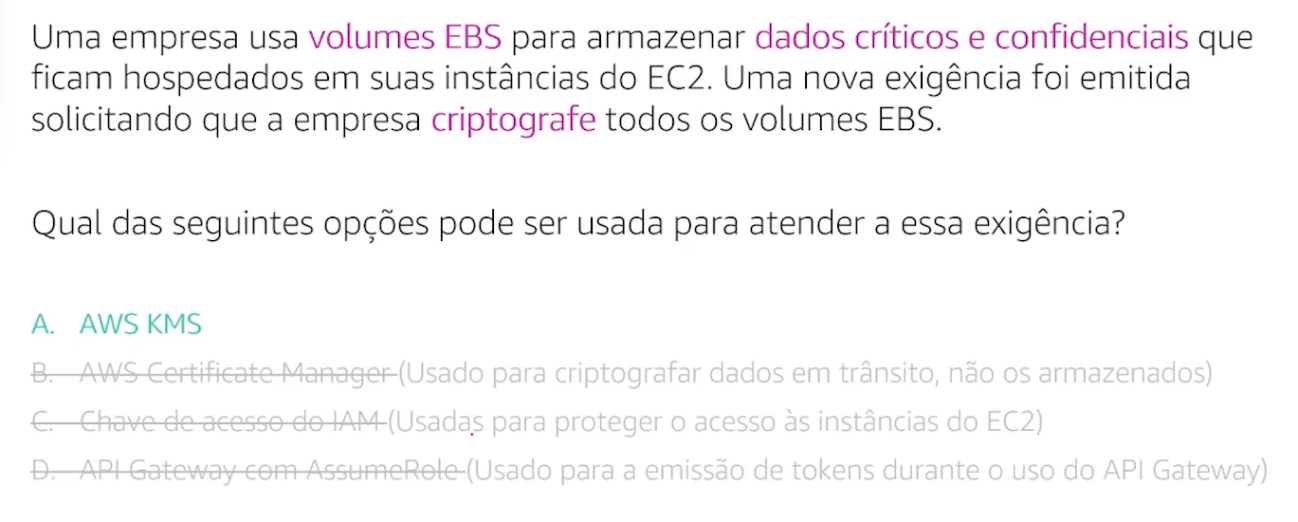
O AWS Key Management Service (KMS) facilita a criação e o gerenciamento de chaves criptográficas e o controle do seu uso em uma ampla variedade de serviços da AWS e nas suas aplicações. O AWS KMS é um serviço seguro e resiliente que usa módulos de segurança de hardware validados ou em processo de validação pelo FIPS 140-2 para proteger suas chaves. O AWS KMS é integrado ao AWS CloudTrail para fornecer logs contendo toda a utilização das chaves para ajudar a cumprir requisitos normativos e de compatibilidade

* Serviço de gerenciamento de chaves de criptografia
* Possibilita que o conteúdo da chave do cliente seja importado
* Aceita chamadas diretas ds aplicações para criptografia/descriptografia de chave
* Alterna as chaves automaticamente e gerencia o uso de chaves antigas.
* Trabalha somente com criptografia simétrica
* Possui um modelo de cobrança por chamada de apis dentro da aws e por chaves gerenciadas.
* E totalmente gerenciado pela AWS

O KMS possui integração com diversos serviços e recursos da AWS

* Amazon EBS
* Amazon S3
* Amazon DynamoDB
* Amazon RDS
* Amazon EMR
* Amazon SES
* Amazon Redshift
* Amazon CloudTrail
* Entre outros....-





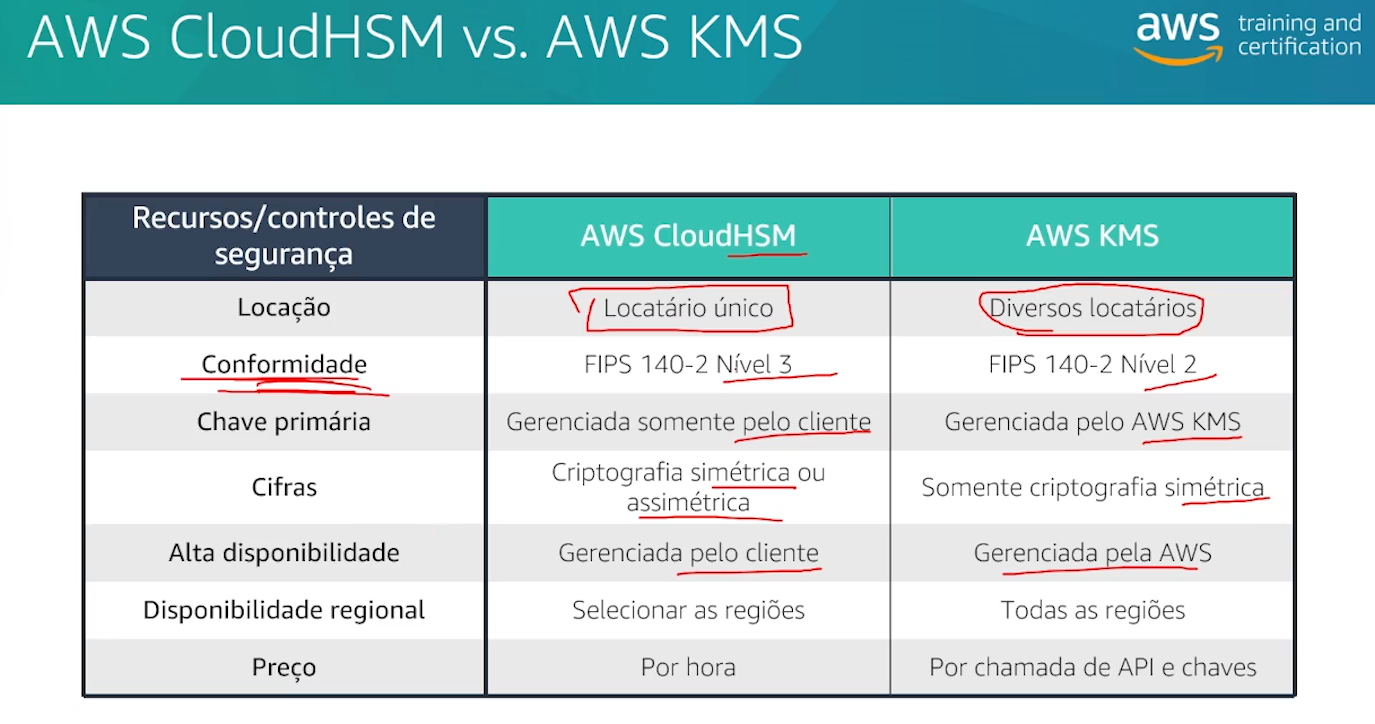
Amazon CloudHMS

O AWS CloudHSM é um Hardware Security Module (HSM – Módulo de segurança de hardware) baseado na nuvem que permite gerar e usar facilmente suas próprias chaves de criptografia na Nuvem AWS. Com o CloudHSM, você pode gerenciar suas próprias chaves de criptografia usando HSMs validados pelo FIPS 140-2 nível 3. O CloudHSM oferece a flexibilidade de integrar-se aos seus aplicativos usando APIs padrão do setor, como bibliotecas Microsoft CryptoNG (CNG), PKCS#11 e Java Cryptography Extensions (JCE).

O CloudHSM está em conformidade com as normas do setor e permite exportar todas as chaves para a maioria dos outros HSMs disponíveis no mercado, dependendo das suas configurações. Ele é um serviço gerenciado que automatiza para você tarefas administrativas demoradas, como provisionamento de hardware, aplicação de patches de software, alta disponibilidade e backups. O CloudHSM também permite que você ajuste a escala rapidamente ao adicionar e remover capacidade HSM sob demanda, sem custos antecipados.

* Gerenciamento de chave de criptografia baseado em hardware
* O CloudHSM gera e armazena com segurança as chaves criptografada
* Pode ser usada dentro do próprio aplicativo do cliente
* As chaves são gerenciadas somente pelo cliente
* CloudHSM ainda não está disponível em todas as regiões
* Possui um modelo de cobrança por hora e o KMS possui o modelo de cobrança por chamadas de api com uso de chaves.
* Trabalha com um modelo de criptografia simétrica ou assimétrica

**Diferença entre CloudHSM X KMS**



<https://docs.aws.amazon.com/pt_br/AmazonS3/latest/userguide/serv-side-encryption.html>

Sempre gratuito

[https://aws.amazon.com/pt/free/?all-free-tier.sort-by=item.additionalFields.SortRank&all-free-tier.sort-order=asc&awsf.Free%20Tier%20Types=\*all&awsf.Free%20Tier%20Categories=\*all](https://aws.amazon.com/pt/free/?all-free-tier.sort-by=item.additionalFields.SortRank&all-free-tier.sort-order=asc&awsf.Free%20Tier%20Types=*all&awsf.Free%20Tier%20Categories=*all)

<https://aws.amazon.com/pt/premiumsupport/plans/>