Criptografia de Dados na Nuvem

Termos de Uso

Propriedade Growdev

Todo o conteúdo deste documento é propriedade da Growdev. O mesmo pode ser utilizado livremente para estudo pessoal.

É proibida qualquer utilização desse material que não se enquadre nas condições acima sem o prévio consentimento formal, por escrito, da Growdev. O uso indevido está sujeito às medidas legais cabíveis.

Segurança

O que é Criptografia?

A **criptografia** é uma técnica de segurança que protege dados convertendo informações legíveis em um formato codificado, tornando-as acessíveis apenas a quem possui a chave de decodificação.

- **Por que usar criptografia?**
  - **Confidencialidade**: Garante que somente pessoas autorizadas possam acessar informações sensíveis.
  - **Integridade**: Protege os dados contra alterações não autorizadas.
  - **Autenticidade**: Permite verificar a identidade de quem envia ou acessa os dados.
- **Onde a criptografia é usada?**
  - Em transações bancárias e e-commerce, para proteger informações financeiras.
  - Em mensagens e e-mails, para garantir que só o destinatário tenha acesso ao conteúdo.
  - Em ambientes de nuvem, para proteger dados armazenados e em trânsito.

Segurança

Como Funciona a Criptografia com Chaves?

A criptografia usa **chaves** para proteger e acessar dados:

- **Chave de Criptografia**: Código que "tranca" ou "destranca" os dados.
- **Criptografia Simétrica**: Usa a mesma chave para codificar e decodificar.
- **Criptografia Assimétrica**: Usa um par de chaves – uma pública para codificar e uma privada para decodificar.

Segurança

Criptografia em Trânsito e em Repouso

Na nuvem, a criptografia protege dados em diferentes momentos:

- **Em Trânsito**: Protege os dados enquanto são transmitidos pela rede, por exemplo, durante a comunicação entre usuário e aplicação.
- **Em Repouso**: Protege os dados armazenados, como em armazenamento de objetos e bancos de dados.

Exemplos:

- **Em trânsito**: Dados que transitam entre cliente e servidor, protegidos para evitar interceptação.
- **Em repouso**: Dados sensíveis armazenados em bancos de dados e sistemas de arquivos na nuvem.

Segurança

Ferramentas de Criptografia em Provedores de Nuvem

Cada provedor oferece ferramentas para gerenciar e aplicar criptografia:

- **AWS**: Amazon Key Management Service (KMS) – Gerenciamento de chaves e criptografia integrada.
- **Azure**: Azure Key Vault – Armazenamento e controle centralizado de chaves de criptografia.
- **Google Cloud**: Cloud Key Management Service (Cloud KMS) – Criptografia e gerenciamento de chaves para serviços Google.

Segurança

Boas Práticas para Gerenciar Chaves de Criptografia

Para garantir a segurança, é essencial seguir práticas eficazes de gerenciamento de chaves:

- **Use políticas de controle de acesso rigorosas**: Limite o acesso às chaves de criptografia a usuários autorizados.
- **Habilite a rotação regular de chaves**: Renove as chaves periodicamente para reduzir o risco de comprometimento.
- **Monitore e registre o uso das chaves**: Acompanhe quem acessou as chaves e quando, para auditoria e segurança.
- **Use criptografia gerenciada sempre que possível**: Simplifica o processo e reduz a complexidade da gestão.

Resumo da ópera

Introdução à Criptografia: Técnica essencial para proteger dados, garantindo confidencialidade, integridade e autenticidade.

Criptografia com Chaves: Uso de chaves simétricas (mesma chave para codificar e decodificar) e assimétricas (par de chaves pública e privada).

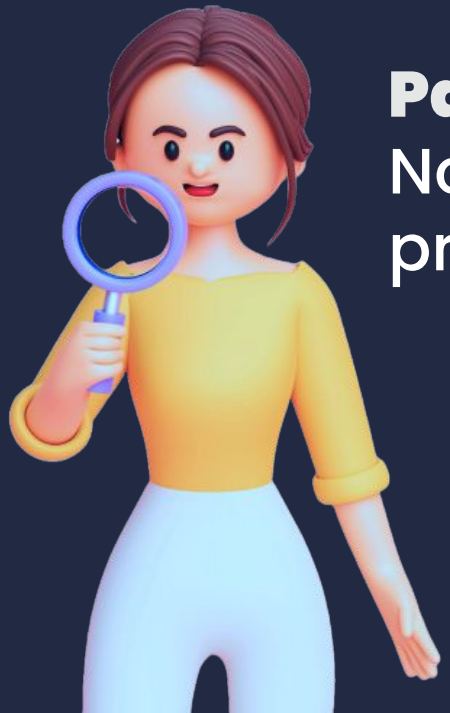
Tipos de Criptografia na Nuvem:

- **Em Trânsito**: Protege os dados enquanto são transmitidos.
- **Em Repouso**: Protege dados armazenados, como em bancos de dados e armazenamento de objetos.

Ferramentas de Criptografia por Provedor:

- AWS KMS, Azure Key Vault e Google Cloud KMS, que oferecem gerenciamento de chaves e criptografia integrada.

Boas Práticas para Gerenciar Chaves: Controle de acesso, rotação de chaves, monitoramento de uso e preferência por criptografia gerenciada.



Parabéns!
Nos vemos na próxima etapa!