Princípios de Segurança na Nuvem e Responsabilidade Compartilhada

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

Segurança na Nuvem

A segurança na nuvem envolve práticas, controles e políticas para proteger dados, sistemas e infraestrutura. Esse conceito é essencial para garantir a confidencialidade, integridade e disponibilidade dos dados em um ambiente de nuvem.

Quer se aprofundar mais?

Conheça mais sobre Segurança da Informação e o CID:
https://www.linkedin.com/pulse/import%C3%A2ncia-da-tr%C3%ADade-c-i-d-para-seguran%C3%A7a-informa%C3%A7%C3%A3o/

Segurança

Modelo de Responsabilidade Compartilhada

No modelo de responsabilidade compartilhada, provedores e clientes dividem responsabilidades para garantir a segurança na nuvem:

Responsabilidade do Provedor	Responsabilidade do Cliente
Segurança da infraestrutura física e da rede	Segurança das aplicações, dados e acesso
Gestão de hardware e segurança de rede	Controle de configuração e permissões
Cumprimento de conformidades gerais	Gestão de usuários e monitoramento de atividades

Segurança

Riscos e Ameaças na Nuvem

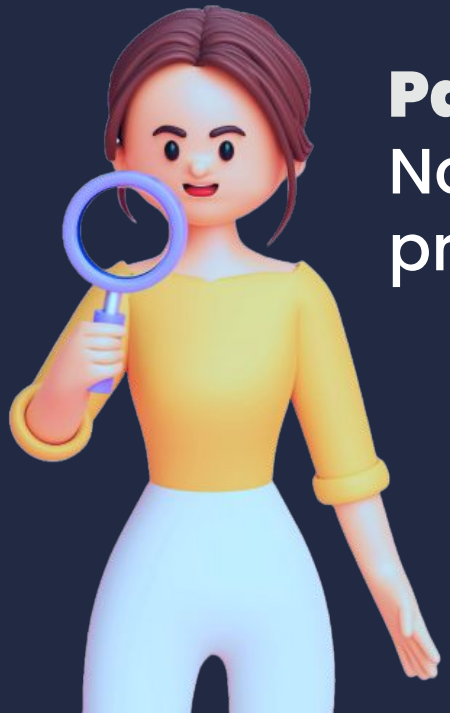
Embora o provedor seja responsável pela segurança da infraestrutura física, cabe ao cliente gerenciar os riscos específicos de configuração e acesso aos dados:

- **Configurações incorretas**: Erros de configuração, como permissões excessivas ou falha em proteger dados, podem expor informações sensíveis.
- **Gestão de acessos e credenciais**: Contas sem autenticação multifator ou senhas fracas aumentam o risco de acessos não autorizados.
- **Armazenamento público inadvertido**: Buckets e contêineres mal configurados podem deixar dados expostos ao público.
- **Falta de conformidade**: Ignorar normas regulatórias (como GDPR, LGPD) pode gerar multas e prejudicar a reputação da empresa.
- **Falta de visibilidade e controle contínuo**: A ausência de monitoramento e auditorias frequentes dificulta a identificação e resposta a atividades suspeitas.

Resumo da ópera

Para uma segurança eficaz na nuvem, é essencial:

- **Entender o modelo de responsabilidade compartilhada**
  - Conheça o que é sua responsabilidade e o que é do provedor.
- **Gerenciar configurações e acessos**
  - Evite falhas de segurança por meio de boas práticas de configuração.
- **Monitorar continuamente os riscos**
  - Identifique e responda rapidamente a potenciais ameaças.



Parabéns!
Nos vemos na próxima etapa!