1.Infraestrutura Cloud

A adoção de tecnologias em nuvem está cada vez mais presente nas organizações, abrangendo diferentes modelos como **Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS)**. Com essa mudança, surge a necessidade de definir claramente as **responsabilidades de segurança** entre o provedor de nuvem e o cliente.

Os provedores de nuvem geralmente oferecem uma **matriz de responsabilidades**, indicando quem é responsável por cada camada da infraestrutura. Em serviços SaaS, por exemplo, o provedor gerencia o sistema operacional, os servidores e a rede, enquanto o cliente cuida da **gestão de identidades e dados**. Já em IaaS, o cliente tem mais controle e, consequentemente, mais responsabilidades sobre a segurança do sistema operacional, aplicativos e configurações de rede.

Muitas empresas adotam uma abordagem **híbrida**, utilizando múltiplos provedores de nuvem (multi-cloud). Essa estratégia aumenta a flexibilidade, mas também adiciona **complexidade na gestão de segurança**, pois cada provedor possui **diferentes regras, configurações e formatos de logs**. O tráfego de dados entre provedores precisa ser protegido com criptografia para evitar a interceptação de informações sensíveis.

A segurança também deve ser estendida a **aplicações de terceiros** hospedadas na nuvem, como firewalls e balanceadores de carga (*load balancers*). Para isso, as empresas devem implementar um **gerenciamento de risco de fornecedores**, garantindo que serviços externos atendam aos padrões de segurança exigidos. Além disso, a **resposta a incidentes** deve incluir protocolos que envolvam provedores e terceiros, assegurando uma reação rápida a possíveis violações.

Um conceito fundamental na computação em nuvem é a **Infraestrutura como Código (IaC)**, **que permite definir servidores, configurações e aplicações por meio de scripts, garantindo padronização, automação e escalabilidade**. Dessa forma, sempre que uma nova instância da infraestrutura for criada, ela seguirá um conjunto específico de regras e políticas de segurança.

A arquitetura serverless é outra tendência na nuvem, onde as aplicações são executadas sem a necessidade de gerenciar servidores físicos ou virtuais. Em vez disso, funções específicas do sistema são executadas sob demanda, reduzindo custos e otimizando o desempenho. No entanto, essa abordagem exige um novo modelo de segurança, focado em **proteção de APIs, controle de identidade e monitoramento de acessos**.

O modelo **monolítico tradicional** de aplicações, onde todos os componentes rodam em um único sistema, está sendo substituído por **arquiteturas baseadas em microsserviços**. Cada funcionalidade da aplicação é executada separadamente e pode

ser dimensionada individualmente conforme a demanda. Essa abordagem permite **melhor controle de segurança**, pois diferentes partes da aplicação podem ter níveis distintos de proteção.

A segurança na nuvem depende de **boas práticas de gestão, configuração correta de permissões e monitoramento contínuo**. Empresas devem implementar **autenticação multifator (MFA), criptografia de dados em trânsito e em repouso, além de políticas rigorosas de controle de acesso**. Com a adoção dessas práticas, é possível garantir a integridade e a confidencialidade das informações na nuvem.