1.Outros tipos de infraestrutura

A escolha entre armazenar dados localmente ou na nuvem envolve considerações de segurança, controle e custo. Infraestruturas locais garantem **controle total sobre os dados e a segurança**, permitindo que a organização defina todas as políticas e implemente suas próprias soluções de proteção. No entanto, esse modelo exige **alto investimento em hardware, manutenção e pessoal especializado**. Por outro lado, a nuvem oferece escalabilidade, atualizações automáticas e suporte especializado do provedor, mas exige **confiança na segurança e na conformidade do fornecedor**.

Ataques cibernéticos ocorrem independentemente do local de armazenamento dos dados, e os invasores buscam falhas tanto em ambientes locais quanto na nuvem. Manter um ambiente local seguro exige **profissionais treinados**, atualização constante e equipamentos modernos. Qualquer mudança na configuração pode ser feita imediatamente, sem depender de terceiros. No entanto, expansão e melhorias exigem novos investimentos em infraestrutura e podem levar tempo para serem implementadas.

A descentralização dos sistemas aumenta a complexidade da segurança. Empresas modernas utilizam **múltiplos provedores de nuvem, servidores em várias localizações e diferentes sistemas operacionais**, dificultando a gestão centralizada. Para resolver esse problema, muitas organizações adotam **painéis de controle unificados**, que permitem monitoramento contínuo de dispositivos, usuários e aplicações. Esse modelo melhora a visibilidade, mas cria um **ponto único de falha**: se o console de monitoramento for comprometido, toda a visão de segurança da empresa pode ser perdida.

A virtualização revolucionou o gerenciamento de servidores, permitindo rodar múltiplos sistemas operacionais em uma única máquina física. No entanto, cada **máquina virtual (VM)** precisa de seu próprio sistema operacional, o que pode gerar redundâncias e desperdício de recursos. Para aumentar a eficiência, empresas adotam **containers**, que compartilham o mesmo sistema operacional, mas rodam aplicações isoladas. Essa abordagem reduz o consumo de memória e processamento, além de facilitar a implantação de novas aplicações.

Os dispositivos **Internet das Coisas (IoT)** trouxeram automação para casas, escritórios e indústrias, mas também criaram novos riscos de segurança. Muitos dispositivos IoT, como câmeras de segurança, sensores e assistentes virtuais, **não foram projetados com segurança robusta**, tornando-se alvos fáceis para hackers. Um único dispositivo comprometido pode expor toda a rede, exigindo segmentação e monitoramento rigoroso para reduzir riscos.

Indústrias críticas, como **energia, petróleo e manufatura**, utilizam **SCADA (Supervisory Control and Data Acquisition)** para monitorar e controlar

equipamentos remotamente. Como um ataque a esses sistemas pode causar impactos catastróficos, a segurança é extremamente rígida, muitas vezes isolando redes SCADA do restante da infraestrutura corporativa.

Sistemas embarcados, como **automóveis, semáforos e dispositivos médicos**, operam de forma altamente específica e segura. Muitos deles utilizam **sistemas operacionais em tempo real (RTOS)**, que priorizam processos críticos, como **freios ABS ou marcapassos**, garantindo respostas imediatas sem interferência de outras funções. Esses sistemas são projetados para serem isolados e difíceis de manipular, reduzindo riscos de invasão.

A **alta disponibilidade (HA - High Availability)** é essencial para empresas que não podem tolerar falhas em seus serviços. Essa abordagem envolve redundância de servidores, infraestrutura de rede e energia, garantindo continuidade das operações mesmo em caso de falhas. No entanto, implementar HA gera **altos custos**, e as empresas precisam decidir até que ponto vale a pena investir para minimizar o risco de interrupções.

A segurança e a disponibilidade dos sistemas dependem de uma combinação equilibrada de tecnologias, práticas de monitoramento e políticas bem definidas. Empresas precisam avaliar riscos, custos e benefícios para adotar as melhores soluções de armazenamento, gerenciamento e proteção de dados.