1.Estados de dados

Os dados podem existir em três estados principais: **dados em repouso, dados em trânsito e dados em uso**. Cada um desses estados exige medidas específicas de segurança para proteger a integridade e a confidencialidade das informações.

Os **dados em repouso** são aqueles armazenados em dispositivos como **discos rígidos, SSDs, pen drives e bancos de dados**. Mesmo quando não estão sendo acessados ativamente, esses dados podem ser vulneráveis a ataques, tornando a **criptografia** uma medida essencial para protegê-los. Métodos como **criptografia de disco inteiro (Full Disk Encryption - FDE)** e criptografia de arquivos individuais ajudam a impedir o acesso não autorizado. Além disso, **permissões de acesso** podem ser configuradas para garantir que apenas usuários autorizados possam visualizar ou modificar essas informações.

Os **dados em trânsito**, também chamados de **dados em movimento**, referem-se às informações transferidas através de redes, como e-mails, downloads e transmissões de vídeo. Sem criptografia, esses dados podem ser interceptados e lidos por terceiros. Tecnologias como **TLS (Transport Layer Security)** e **VPNs com IPsec** são amplamente usadas para proteger dados enquanto estão sendo transmitidos, garantindo que apenas os destinatários autorizados possam acessá-los. Firewalls e **sistemas de prevenção de intrusão (IPS)** também ajudam a monitorar e bloquear tráfego suspeito.

Os **dados em uso** são aqueles que estão sendo processados na memória RAM ou manipulados por um sistema. Diferente dos outros estados, esses dados geralmente não estão criptografados, pois precisam ser acessíveis para operações computacionais. Isso os torna um alvo valioso para ataques, como o caso da violação da **Target Corporation em 2013**, onde hackers instalaram malware em terminais de ponto de venda (POS) e capturaram **110 milhões de números de cartões de crédito** diretamente da memória dos dispositivos. Esse tipo de ataque explora vulnerabilidades antes que a criptografia possa ser aplicada novamente.

Outro conceito importante na segurança de dados é a **soberania dos dados**, que determina que informações armazenadas dentro de um país estão sujeitas às suas leis locais. Regulamentos como o **GDPR (General Data Protection Regulation)** da União Europeia exigem que os dados de cidadãos europeus sejam armazenados dentro da UE, garantindo conformidade com os padrões de privacidade. Empresas que operam globalmente precisam estar atentas às diferenças legais entre regiões para evitar violações.

A **geolocalização** também desempenha um papel na proteção de dados, ajudando a controlar o acesso com base na localização do usuário. Alguns serviços restringem o acesso a conteúdos dependendo do país, como ocorre com plataformas de streaming. Empresas podem implementar políticas de segurança que concedem

diferentes níveis de acesso com base na posição geográfica do usuário, permitindo maior permissividade dentro de prédios corporativos e restringindo acessos remotos.

Garantir a proteção dos dados em seus diferentes estados exige uma combinação de **criptografia, controle de acesso, monitoramento contínuo e conformidade com regulamentações locais**. Medidas proativas são essenciais para minimizar riscos e evitar o comprometimento de informações sensíveis.