1.Proteção de dados

A proteção de dados envolve diversas estratégias para garantir segurança e controle sobre onde e como as informações podem ser acessadas. Uma das abordagens é a implementação de **restrições geográficas**, conhecidas como **geofencing**, que limitam o acesso aos dados com base na localização do usuário. Isso pode ser feito analisando **endereços IP, redes Wi-Fi e sinais de GPS** para determinar se um usuário está dentro de uma área permitida. Empresas podem, por exemplo, restringir o acesso a determinados arquivos apenas para usuários dentro de instalações corporativas.

A perda ou comprometimento de dados pode ser desastroso para qualquer organização, tornando essencial a aplicação de **medidas de segurança em diferentes estágios do ciclo de vida da informação**. Os dados podem estar **armazenados em dispositivos físicos, sendo transmitidos pela rede ou em processamento na memória de um sistema**. Qualquer um desses estados pode ser explorado por atacantes, exigindo o uso de **criptografia, políticas de acesso restrito e monitoramento contínuo**.

A criptografia transforma **dados legíveis (plaintext)** em **dados ilegíveis (ciphertext)**, protegendo as informações contra acessos não autorizados. O processo de reversão, conhecido como **decriptação**, só pode ser realizado por usuários que possuam a chave correta. A eficácia da criptografia depende da **qualidade do algoritmo utilizado** e da segurança no armazenamento das chaves de decriptação.

Outro método de proteção é o uso de **hashing**, que gera um código único baseado no conteúdo de um arquivo ou senha. Hashes são frequentemente utilizados para armazenar **credenciais de usuários e verificar a integridade de arquivos baixados da internet**. Um bom algoritmo de hash deve garantir que até mesmo pequenas mudanças nos dados originais resultem em um hash completamente diferente, evitando colisões que possam comprometer a segurança.

Além da criptografia e hashing, a **ofuscação de dados** é uma técnica que torna informações mais difíceis de serem interpretadas. Isso pode ser aplicado a códigos-fonte de programas, ocultando sua lógica para impedir engenharia reversa, ou a dados sensíveis, mascarando parte das informações. Um exemplo prático é a exibição parcial de números de cartão de crédito em recibos de compras.

A **tokenização** substitui dados sensíveis por identificadores únicos (tokens), que não possuem relação direta com a informação original. Essa técnica é amplamente usada em pagamentos móveis, garantindo que **números de cartão de crédito reais nunca sejam transmitidos pela rede**. Como os tokens são gerados para uso único, mesmo que um atacante intercepte os dados, eles não poderão ser reutilizados.

A segmentação de dados reduz os riscos ao armazenar informações em **bancos de dados separados**, dificultando o acesso completo em caso de invasão. Além disso,

diferentes níveis de segurança podem ser aplicados conforme a sensibilidade dos dados, garantindo proteção reforçada para informações financeiras ou de saúde.

As permissões de acesso desempenham um papel crítico na segurança de dados. Usuários só devem ter acesso às informações necessárias para suas funções, seguindo o princípio do **menor privilégio**. Além disso, políticas de **autenticação forte e autenticação multifator (MFA)** ajudam a evitar acessos não autorizados.

A combinação dessas estratégias fortalece a segurança das informações, minimizando riscos de vazamento, fraude e ataques cibernéticos.