1.Tipos de dados

A gestão de dados em uma organização envolve diferentes níveis de segurança e acesso, dependendo do tipo e da sensibilidade das informações armazenadas. Dados podem ser classificados de diversas formas, como **regulados, sigilosos, proprietários, financeiros ou pessoais**, cada um exigindo políticas específicas de proteção.

Dados regulados são aqueles cujo armazenamento e uso são controlados por regulamentações externas. Um exemplo é o **PCI DSS (Payment Card Industry Data Security Standard)**, que estabelece regras para a proteção de informações de cartões de crédito. Além disso, leis governamentais podem definir como os dados devem ser armazenados e por quanto tempo.

As organizações também possuem **segredos comerciais**, que incluem processos, fórmulas ou estratégias que oferecem vantagem competitiva. Esses dados precisam ser protegidos contra acessos indevidos, pois sua divulgação pode comprometer a posição da empresa no mercado. Da mesma forma, **propriedade intelectual** pode ser resguardada por **patentes, direitos autorais e marcas registradas**, garantindo que terceiros não utilizem informações exclusivas sem permissão.

Os dados legais apresentam um desafio adicional, pois muitas informações judiciais são públicas, mas certos detalhes precisam ser mantidos em sigilo. Elementos como **informações pessoais identificáveis (PII)** e dados financeiros exigem níveis elevados de segurança para evitar acessos não autorizados.

A acessibilidade dos dados pode variar entre formatos **legíveis por humanos** (como documentos e planilhas) e **não legíveis por humanos** (como códigos de barras e informações codificadas). Algumas informações combinam ambos os formatos para facilitar a leitura por máquinas e pessoas.

Para garantir a proteção dos dados, eles são classificados em diferentes níveis de sensibilidade. Algumas organizações estabelecem camadas como:

- **Dados públicos**: acessíveis a qualquer pessoa.
- **Dados privados**: restritos a usuários autorizados.
- **Dados confidenciais**: exigem níveis mais altos de permissão e podem ser protegidos por **termos de confidencialidade (NDA)**.
- **Dados críticos**: devem estar sempre disponíveis, exigindo redundância e sistemas de alta disponibilidade.

Além disso, **dados proprietários** são exclusivos da organização e podem incluir metodologias, relatórios internos e bancos de dados estratégicos. Já **informações pessoais identificáveis (PII)** englobam dados como **nome, endereço, número de identidade e informações biométricas**, que podem ser usados para

identificar uma pessoa. Quando essas informações estão relacionadas à saúde, são classificadas como **PHI (Protected Health Information)** e exigem conformidade com leis de privacidade, como a **HIPAA** nos Estados Unidos.

Ao definir políticas de classificação e controle de acesso, as organizações garantem que apenas usuários autorizados possam visualizar e modificar informações sensíveis, reduzindo o risco de vazamento e uso indevido de dados.