INOVAÇÃO E TECNOLOGIA

# COMPUTAÇÃO CONFIDENCIAL E PRIVACIDADE POR DESIGN

Gabrieli Oliveira, Guilherme Barbosa,
Neife Junior, Raika Sousa - 3ºH

# SUMÁRIO



# DEFINIÇÃO

## COMPUTAÇÃO CONFIDENCIAL

- Tecnologia que protege dados sensíveis durante o processamento.
- Garante que informações permaneçam protegidas contra acesso não autorizado, mesmo na nuvem.

---

### Como funciona?

- Uso de enclaves seguros de hardware.
- Permite processamento de dados criptografados.
- Apenas partes autorizadas podem acessar os dados originais.

# DEFINIÇÃO

## PRIVACIDADE POR DESIGN

- Abordagem que integra proteção de dados desde o início do desenvolvimento de produtos ou serviços.

---

### Como funciona?

1. **Proativo, não reativo**: Prevenir invasões antes que ocorram.
2. **Privacidade como padrão**: Proteção automática dos dados pessoais.
3. **Privacidade incorporada ao design**: Segurança integrada na arquitetura e processos.
4. **Funcionalidade total**: Conciliar interesses legítimos sem comprometer a privacidade.
5. **Proteção de ponta a ponta**: Garantia de segurança durante todo o ciclo de vida dos dados.
6. **Visibilidade e transparência**: Práticas claras e verificáveis.
7. **Respeito pelo usuário**: Foco na experiência e controle do usuário.

# IMPORTÂNCIA DO CENÁRIO ATUAL

01 Crescimento de ataques cibernéticos e vazamentos de dados

02 Conformidade com legislações como LGPD e GDPR

03 Necessidade de confiança em serviços digitais

# COMPUTAÇÃO HOMOMÓRFICA


- A criptografia homomórfica permite que operações complexas sejam realizadas em dados criptografados sem compromete-los
- Já na computação, permite que cálculos matemáticos sejam realizados diretamente nos dados criptografados
- Na matemática, homomórfica significa transformação de um conjunto de dados em outro, preservando suas características
- Pode ser dividida em Criptografia Parcialmene Homomórfica, Um Tanto Homomorfica e Totalmente Homomórfica

# COMPUTAÇÃO HOMOMÓRFICA

Uma operação definida pode ser realizada infinitas vezes no texto cifrado. Esses esquemas de criptografia são relativamente fáceis de projetar.


Um número limitado de operações de adição ou multiplicação são permitidas, em oposição a um número infinito de uma operação

Um número infinito de adições ou multiplicações para textos cifrados é habilitado

# FEDERATED LEARNING

## O que é?

O Aprendizado Federado é uma abordagem descentralizada de IA que treina modelos diretamente nos dispositivos dos usuários, sem transferir os dados brutos para um servidor central. Apenas os ajustes do modelo são enviados, garantindo a privacidade e segurança das informações pessoais.

## Como funciona?

Cada dispositivo coleta dados localmente e realiza pequenos ajustes no modelo de IA. Em seguida, esses ajustes são enviados para um servidor central, onde são combinados com ajustes de outros dispositivos para atualizar o modelo global. Esse processo se repete de forma iterativa, garantindo que o aprendizado ocorra de maneira distribuída e segura.

# FEDERATED LEARNING

## VANTAGENS

- Maior Privacidade e Segurança
- Eficiência na Transferência de Dados
- Aprendizado Descentralizado
- Melhoria Contínua e Personalização
- Compatibilidade com Dispositivos Móveis e IoT

## DESVANTAGENS

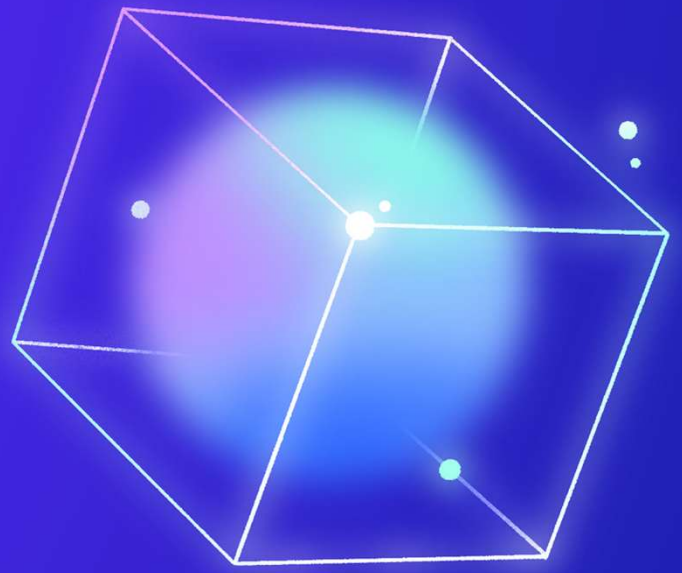
- Consumo de Recursos Locais
- Sincronização e Comunicação
- Segurança dos Modelos Treinados
- Desigualdade na Qualidade dos Dados
- Complexidade de Implementação

# DIFFERENTIAL PRIVACY

- Método matemático para proteger dados individuais
- Adiciona ruído controlado às respostas das consultas
- Mantém padrões e estatísticas úteis sem revelar informações pessoais
- Usado por empresas e governos para garantir privacidade em análises de dados

# BENEFÍCIOS

- **Proteção da privacidade:** A privacidade diferencial protege as informações individuais, mesmo que um invasor tenha acesso ao conjunto de dados e a outras informações sobre as pessoas.
- **Análise de dados útil:** Apesar da adição de ruído, a privacidade diferencial ainda permite obter resultados precisos e úteis para a análise de dados.
- **Aplicações:** A privacidade diferencial pode ser usada em diversas áreas, como saúde, pesquisa social e análise de dados governamentais.



# AGRADECEMOS A ATENÇÃO!