Aprendizado Federado

Arduino e seu Papel na Privacidade em Redes Neurais Profundas

Kaylani Bochie

https://www.gta.ufrj.br/~kaylani/
https://github.com/kaylani2/minicursos

Prefácio

Arduino como:

- Produto final
- Plataforma de prototipagem
- Ferramenta de pesquisa
- **Ferramenta de ensino**

Prefácio

Arduino como:

- Produto final
- Plataforma de prototipagem
- Ferramenta de pesquisa
- **Ferramenta de ensino**

FAQ:

- Perguntas?
- Conhecimento prévio?

Conteúdo

O que é Aprendizado de Máquina?

O que é Aprendizado de Máquina?

"Machine learning is about extracting knowledge from data. It is a research field at the intersection of statistics, artificial intelligence, and computer science and is also known as predictive analytics or statistical learning."

Andreas C. Müller e Sarah Guido, "*Introduction to Machine Learning with Python*", página 1, 2016.

O que é Aprendizado de Máquina?

"Machine learning is about extracting knowledge from data. It is a research field at the intersection of statistics, artificial intelligence, and computer science and is also known as predictive analytics or statistical learning."

Andreas C. Müller e Sarah Guido, "*Introduction to Machine Learning with Python*", página 1, 2016.

"Machine learning is essentially a form of applied statistics with increased emphasis on the use of computers to statistically estimate complicated functions and a decreased emphasis on proving confidence intervals around these functions [...]"

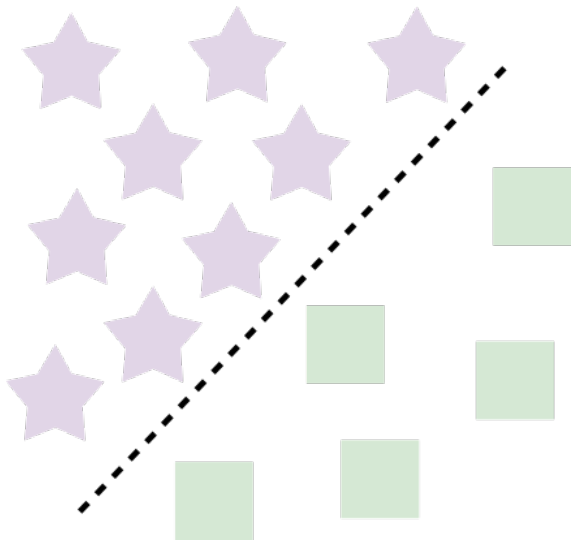
Ian Goodfellow, "*Deep Learning*", página 96, 2016.

Tipos de Aprendizado

- Supervisionado
- Não supervisionado
- Semissupervisionado
- Por reforço

Tipos de Aprendizado

- Supervisionado



Amostras rotuladas. $TS = \{\langle x_1, y_1 \rangle, \langle x_2, y_2 \rangle, ..., \langle x_n, y_n \rangle\}$

- Não supervisionado
- Semissupervisionado
- Por reforço

Tipos de Aprendizado

- Supervisionado
- Não supervisionado

Amostras não rotuladas. $TS = \{\langle x_1 \rangle, \langle x_2 \rangle, ..., \langle x_n \rangle\}$

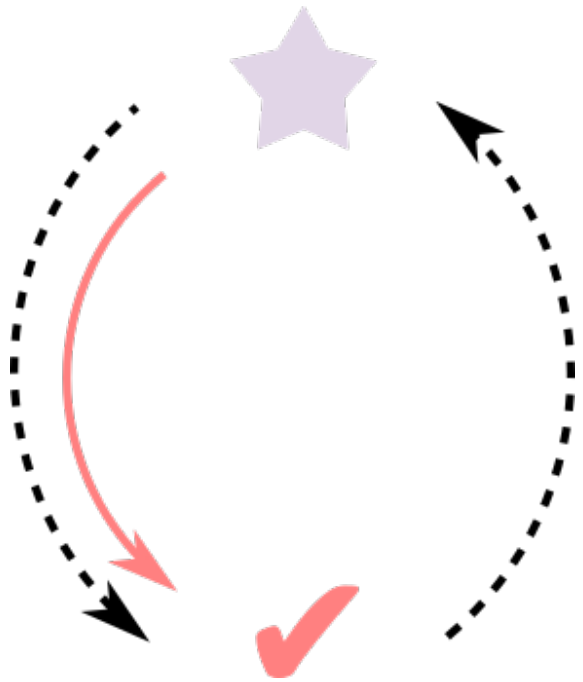
- Semissupervisionado
- Por reforço

Tipos de Aprendizado

- Supervisionado
- Não supervisionado
- Semissupervisionado
  Amostras rotuladas e não rotuladas
  $TS = \{\langle x_1, y_1 \rangle, \langle x_2 \rangle, ..., \langle x_n, y_n \rangle\}$
- Por reforço

Tipos de Aprendizado

- Supervisionado
- Não supervisionado
- Semissupervisionado
- Por reforço



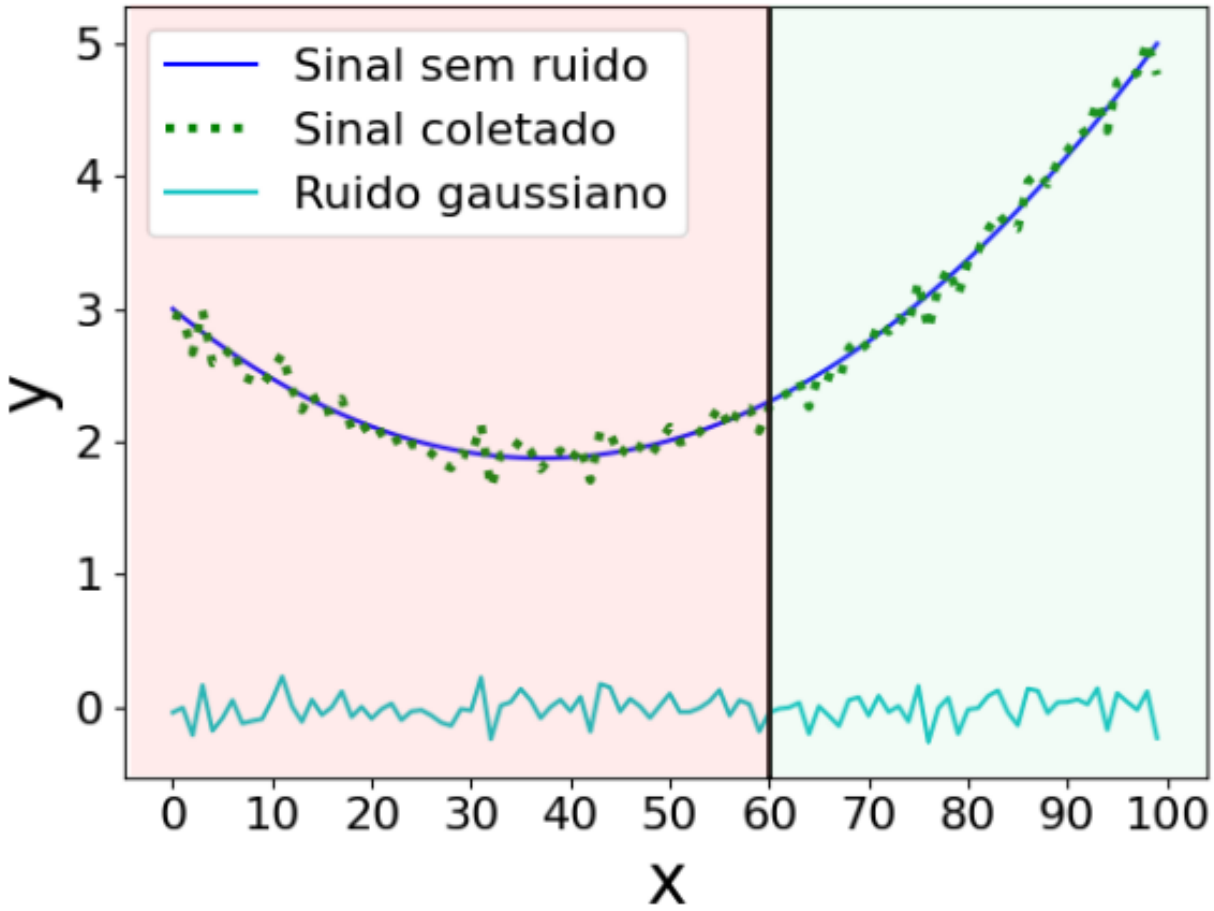
Aprendizado iterativo. Agente X ação X recompensa.

Divisão do Conjunto de Dados

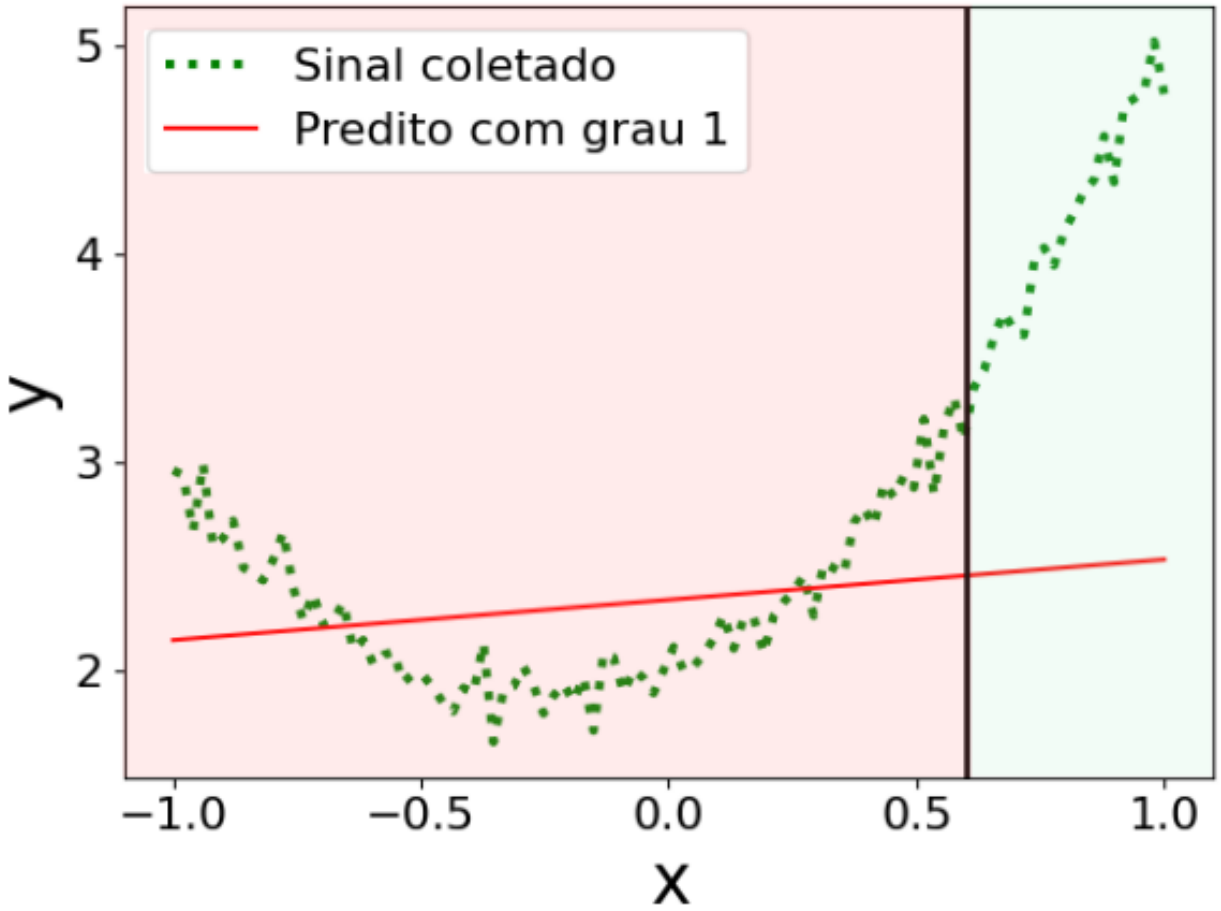
Como dividir os dados para treinamento?

- Treino, teste e validação
- Vazamento de dados
- *Overfitting* (sobreajuste) e *underfitting* (subajuste)
- Ruído

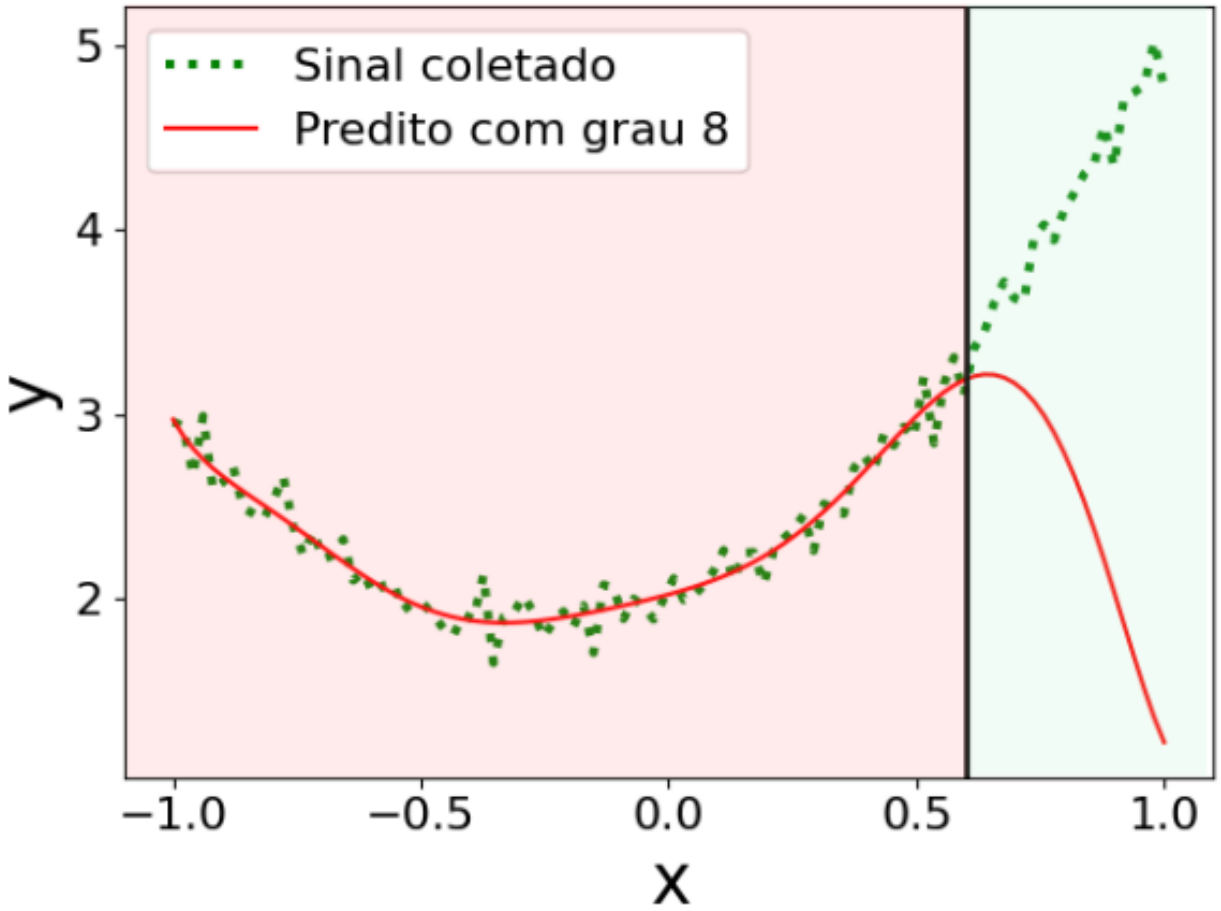
Intuição da Divisão do Conjunto de Dados



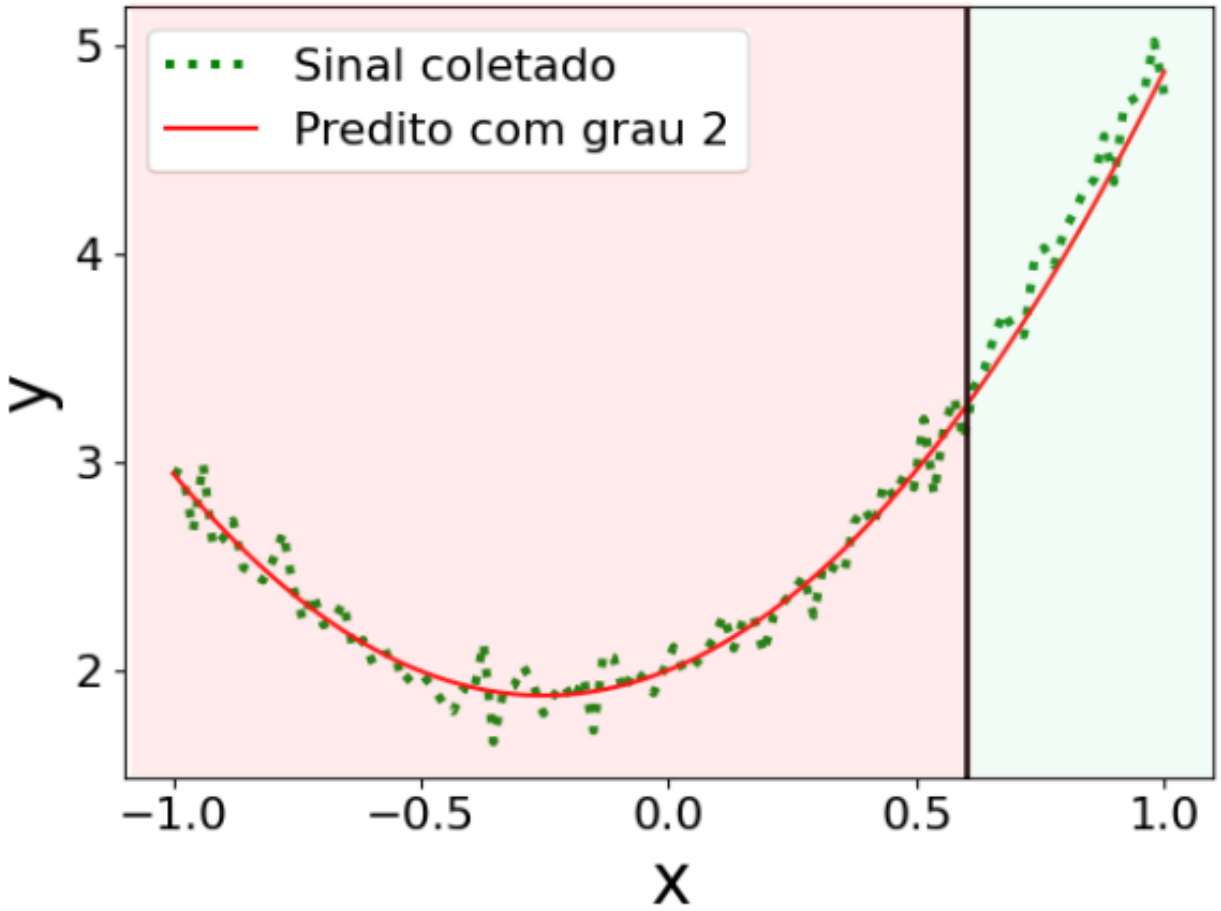
Intuição da Divisão do Conjunto de Dados



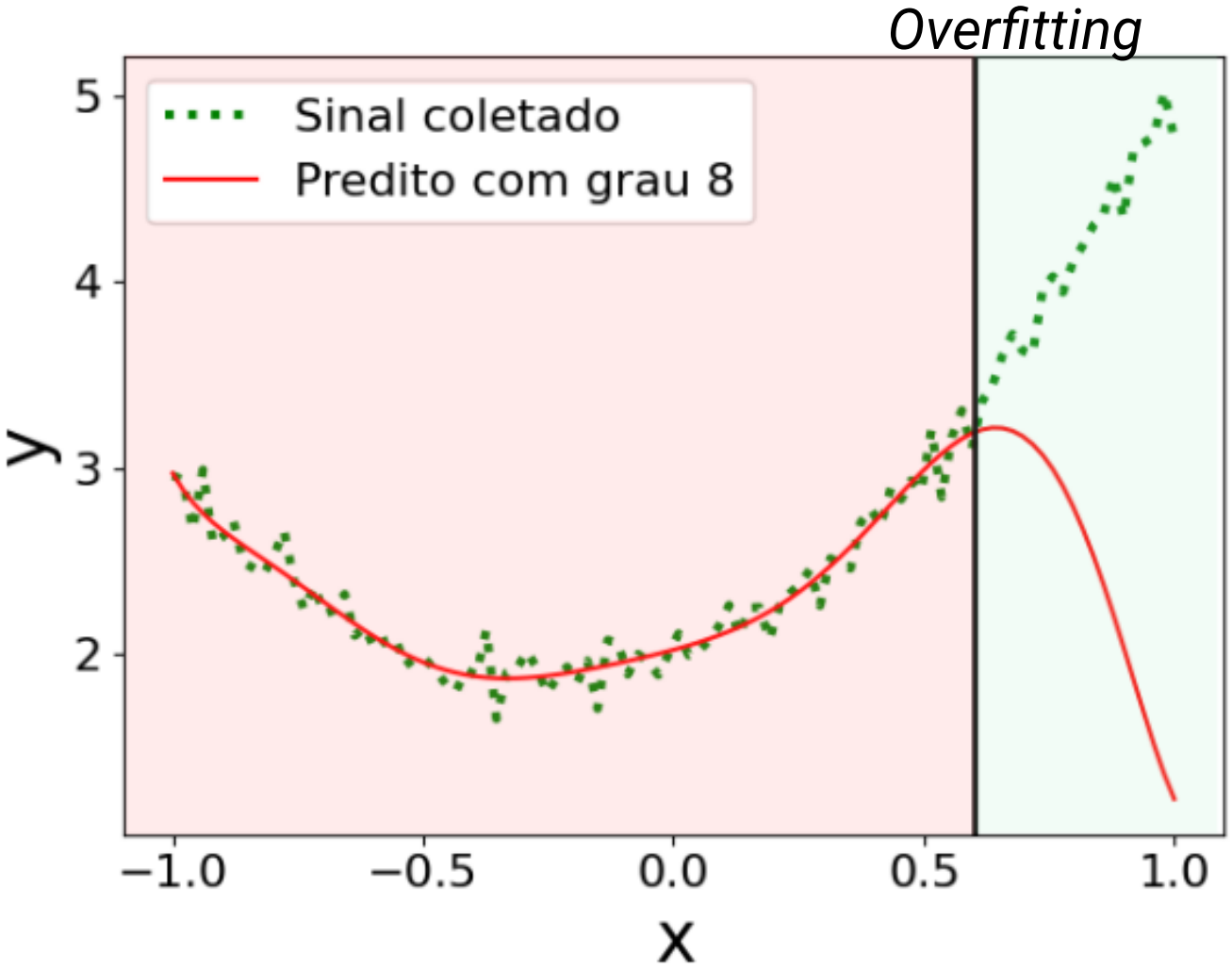
Intuição da Divisão do Conjunto de Dados



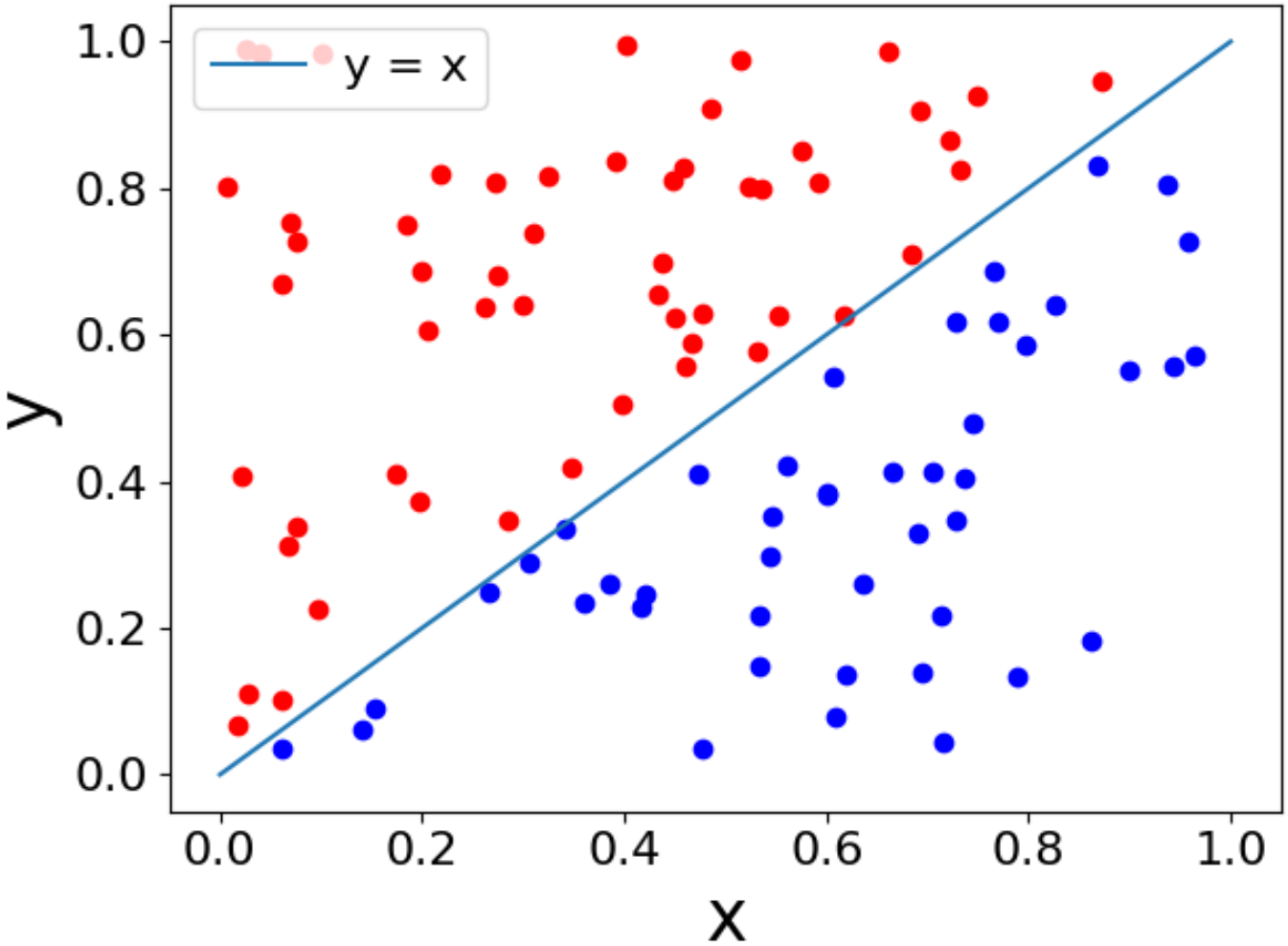
Intuição da Divisão do Conjunto de Dados



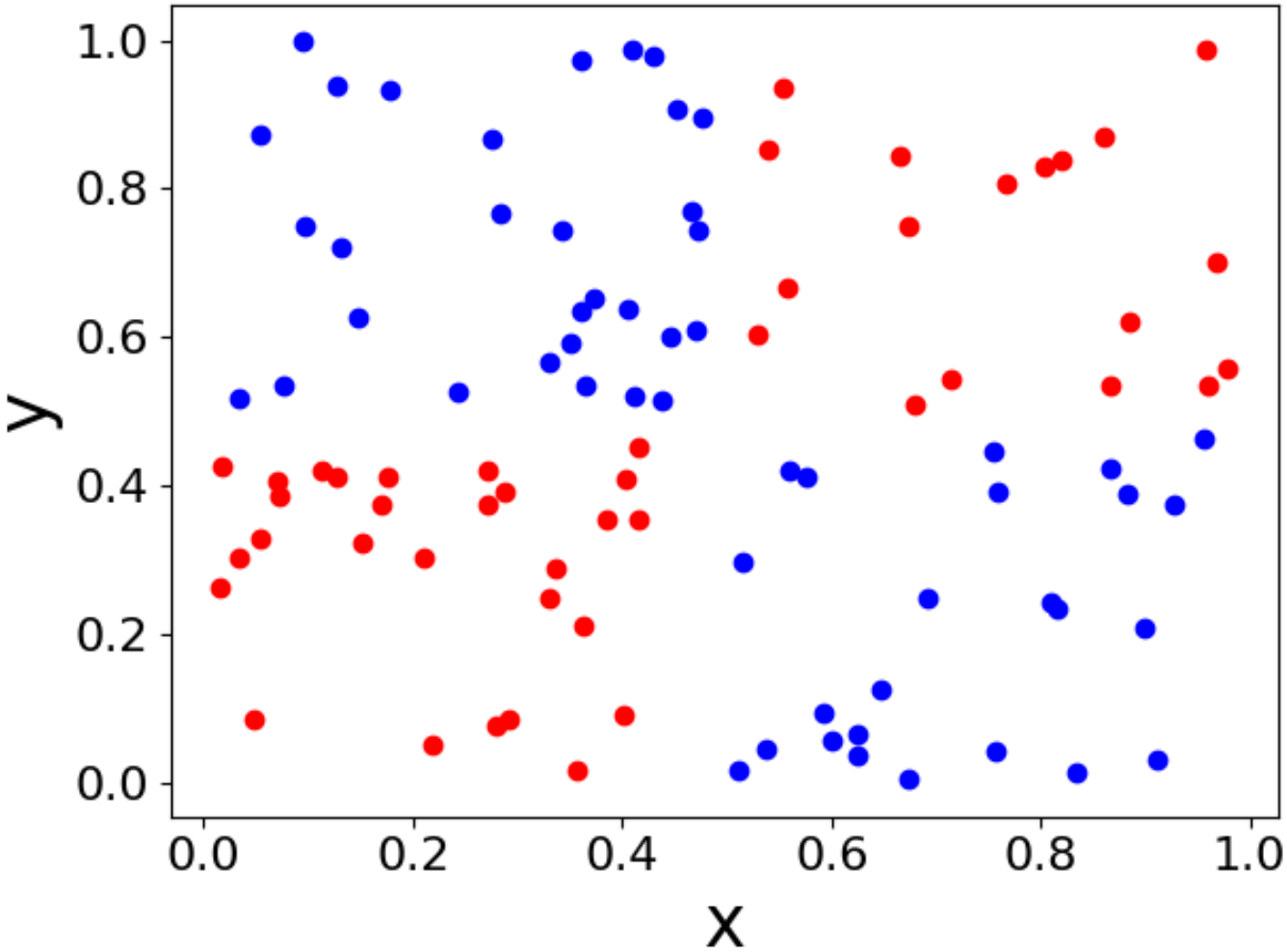
Exemplo de Sobreajuste

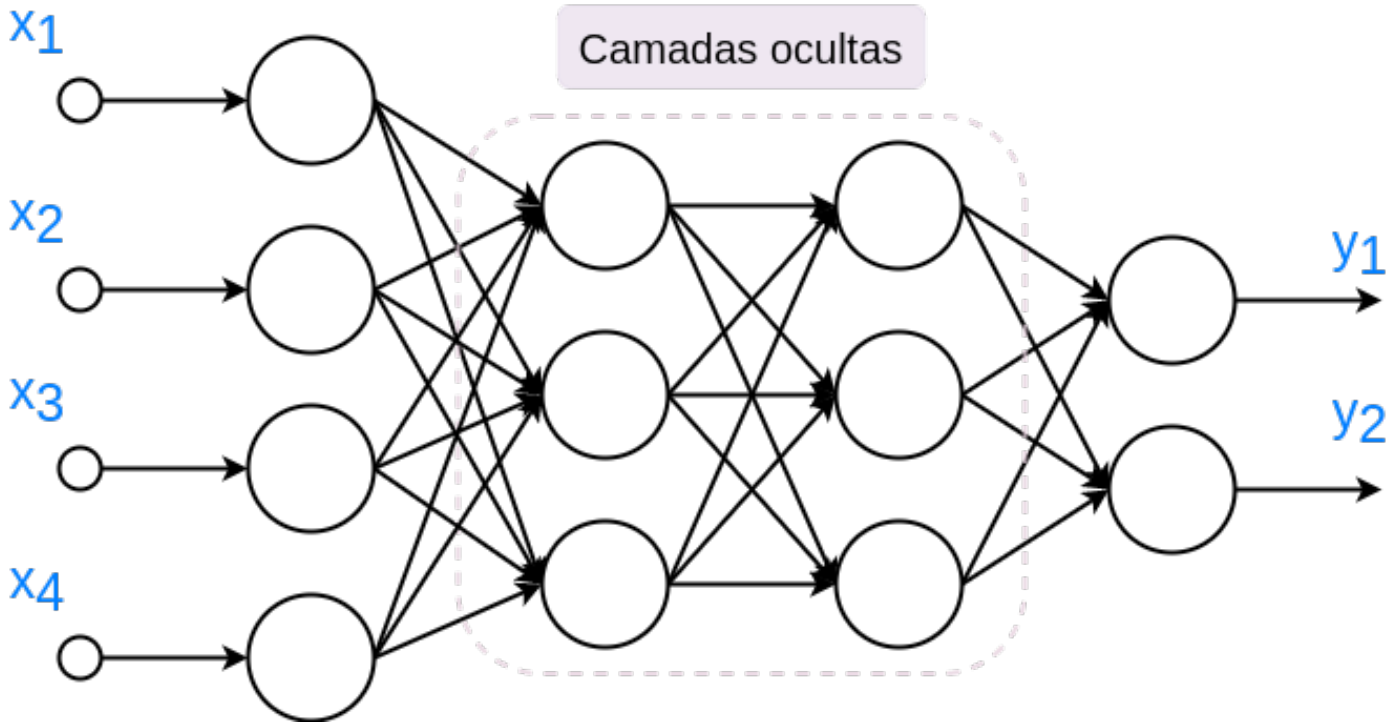


Separabilidade Linear

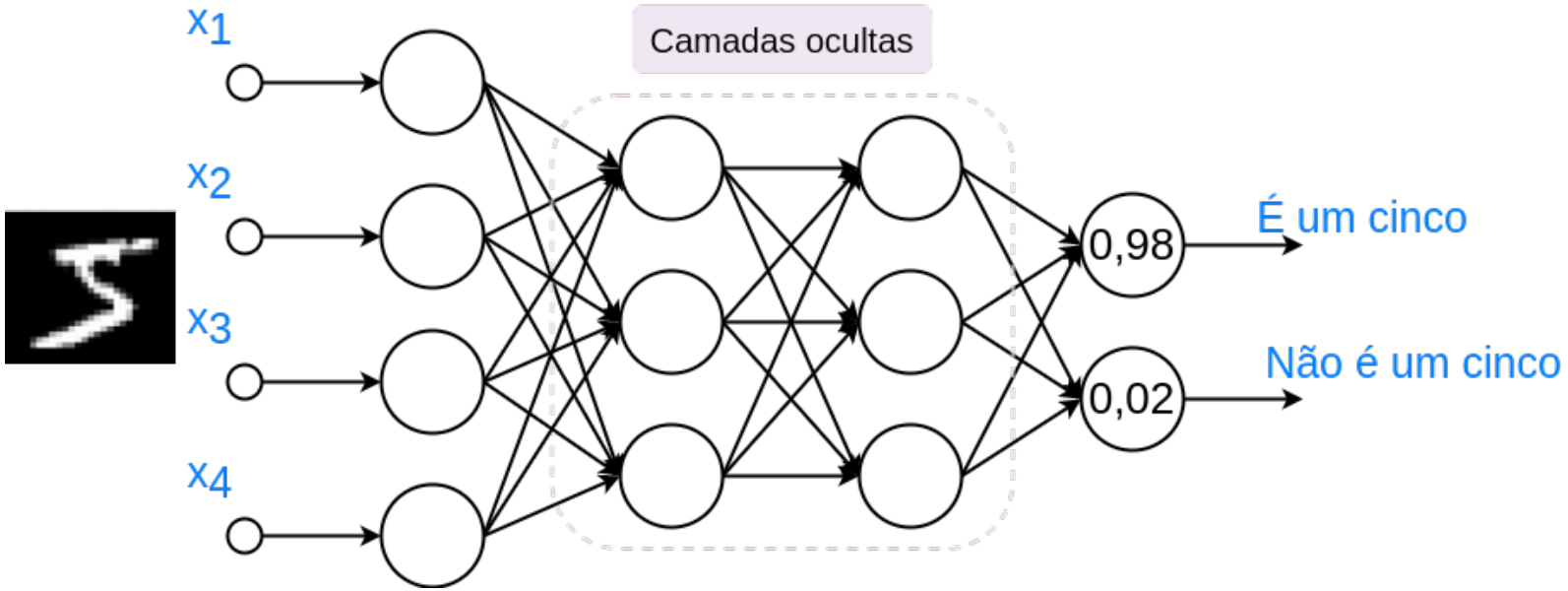


Função XOR



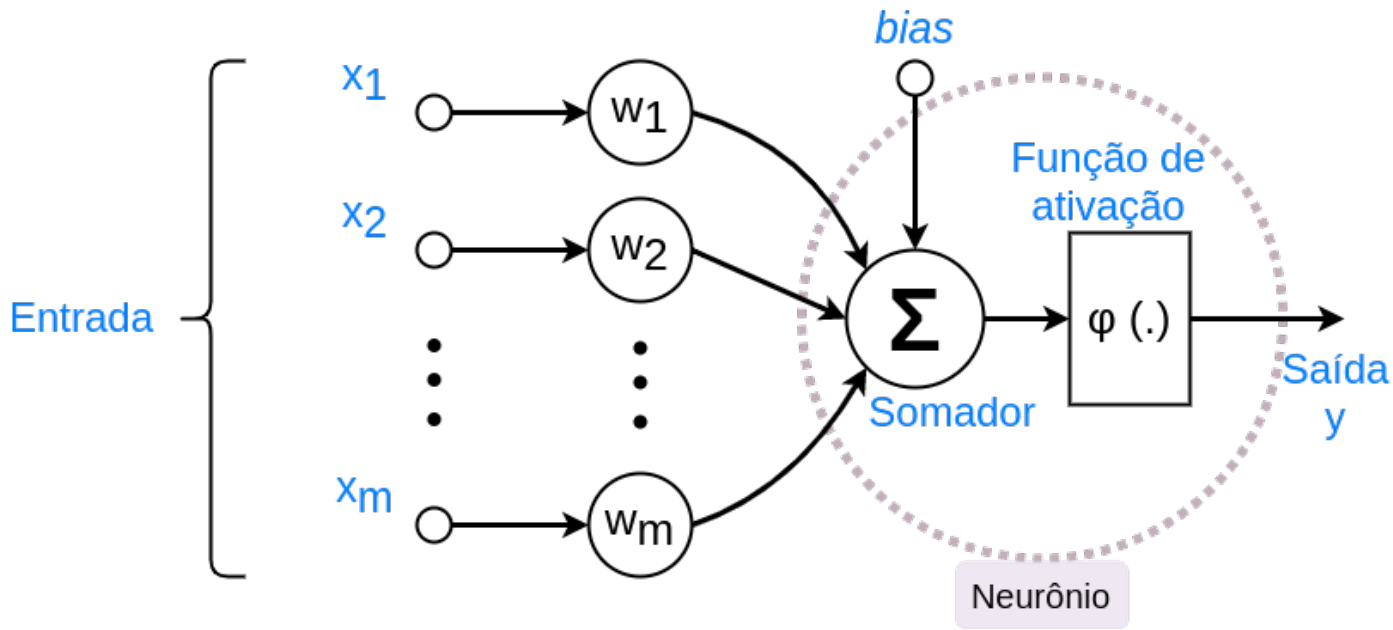


Exemplo de uma rede neural *feedforward*.

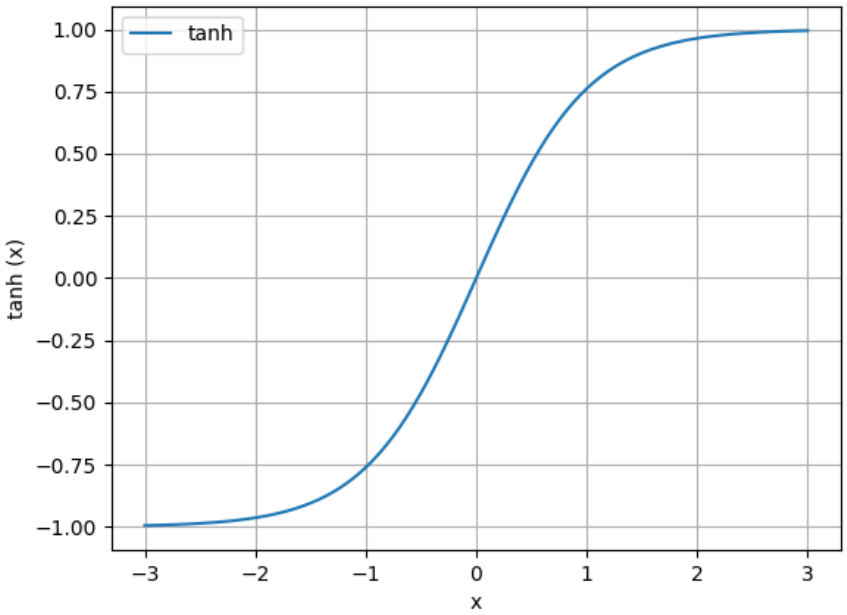


Exemplo de uma rede neural *feedforward*.

Neurônio

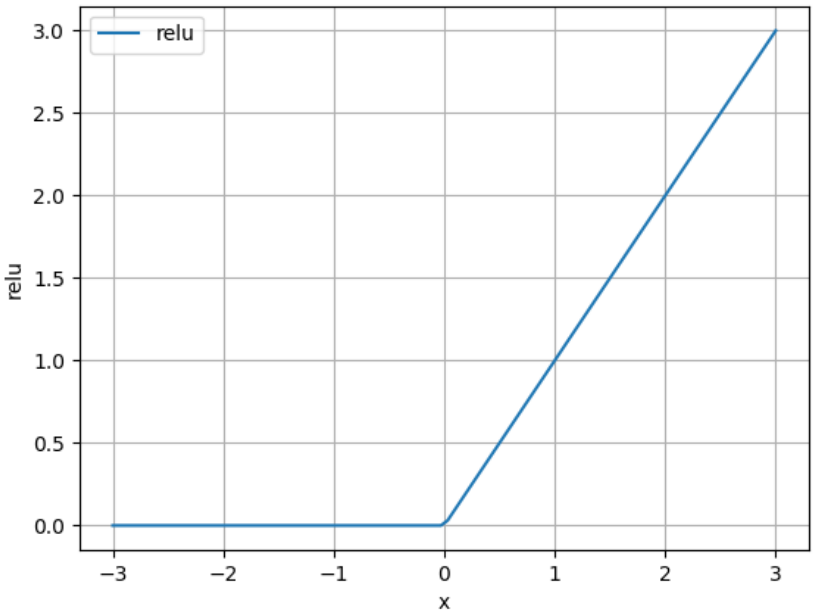

bias
x1
x2
xm
Entrada
w1
w2
wm
Σ
Somador
Função de ativação
φ (.)
Saída y
Neurônio

Tangente Hiperbólica



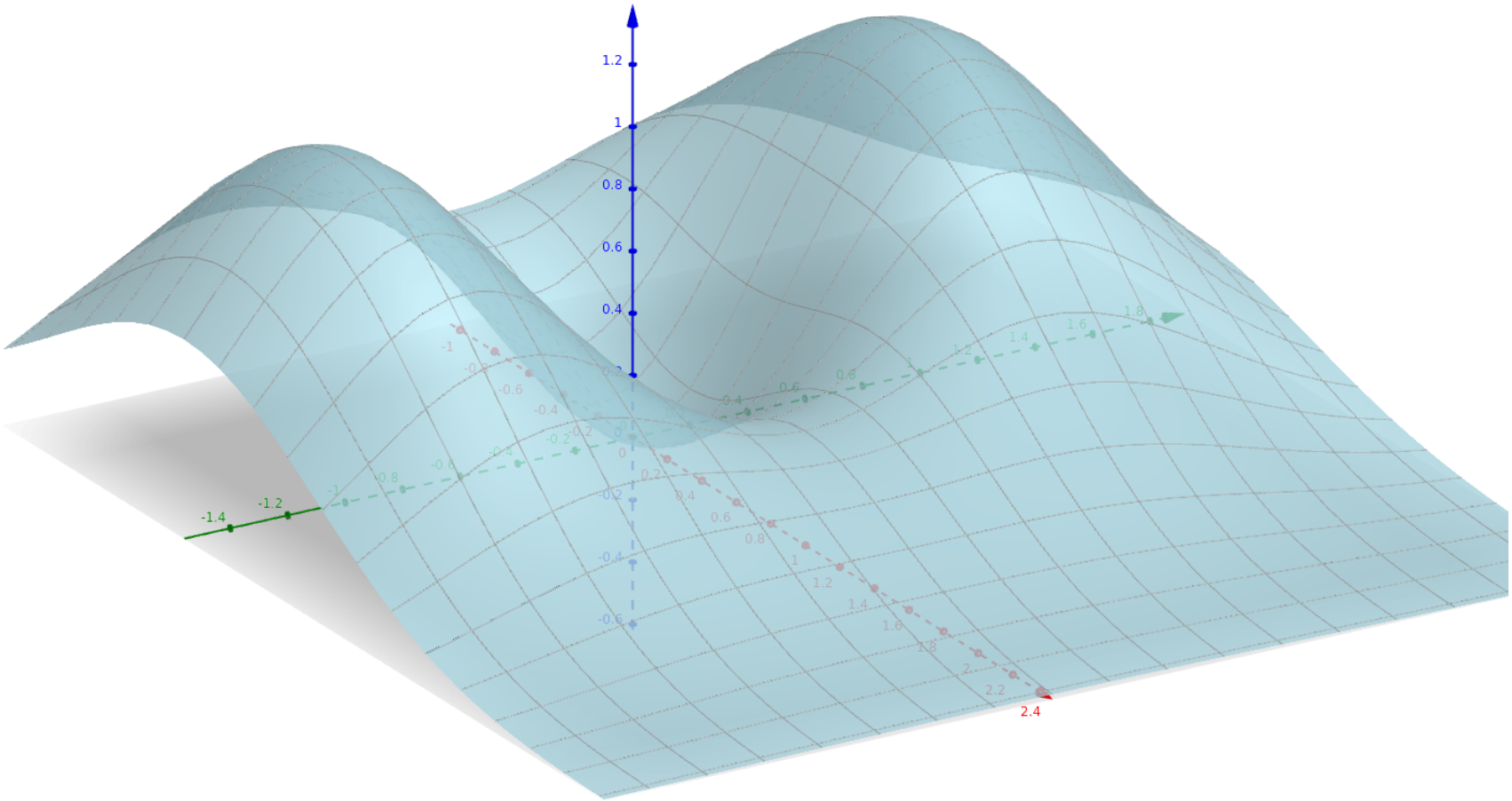
- Neurônios podem saturar

ReLU (Rectified Linear Unit)

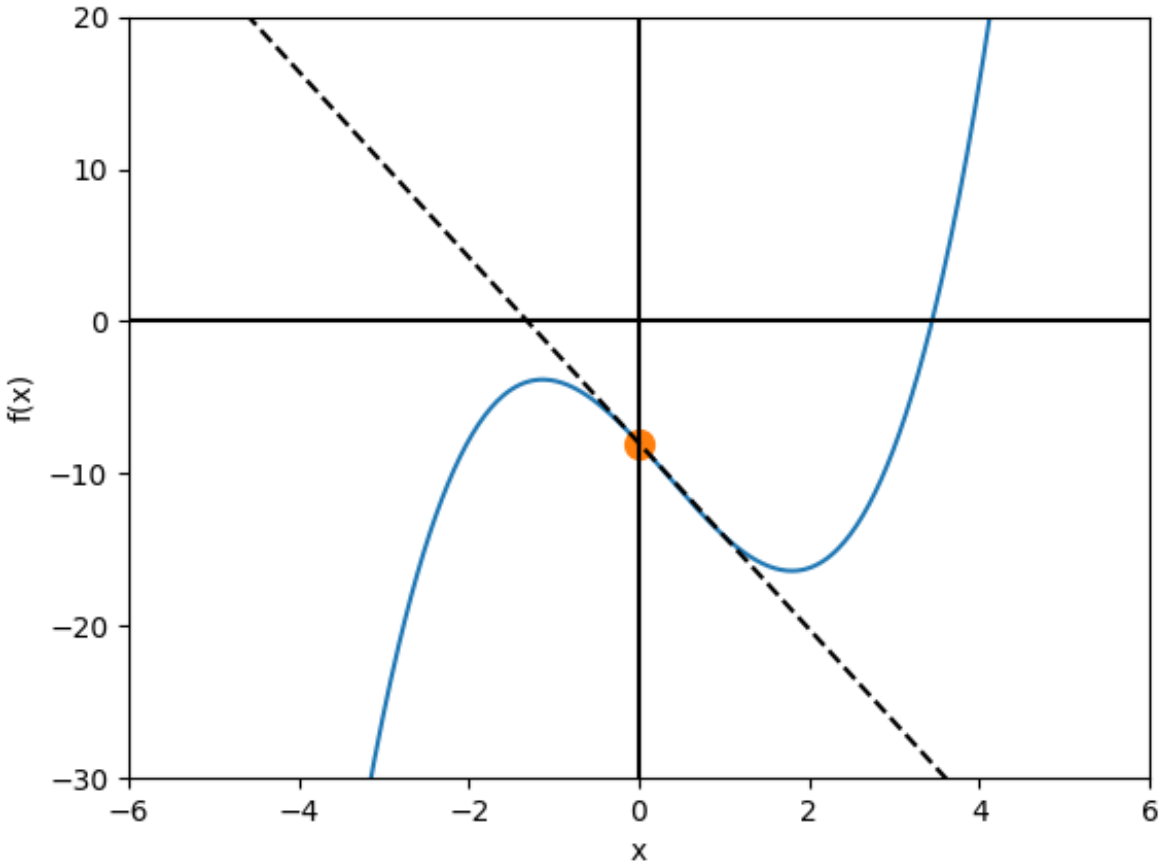


- $max\ (0, x)$
- Computacionalmente eficiente
- Não satura na região positiva
- Converge mais rapidamente que a *sigmoid* e a tangente hiperbólica
- Saída não é centrada em zero
- Há saturação na região negativa

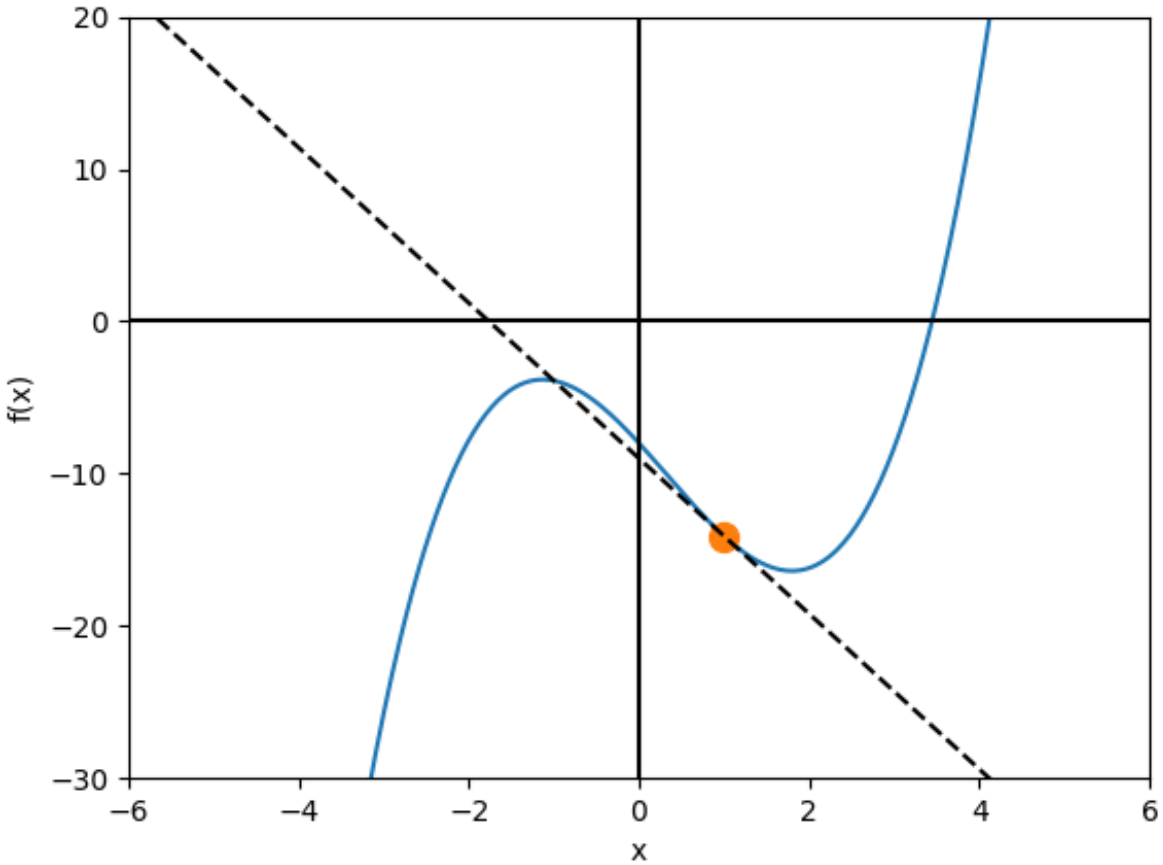
Stochastic Gradient Descent (SGD)



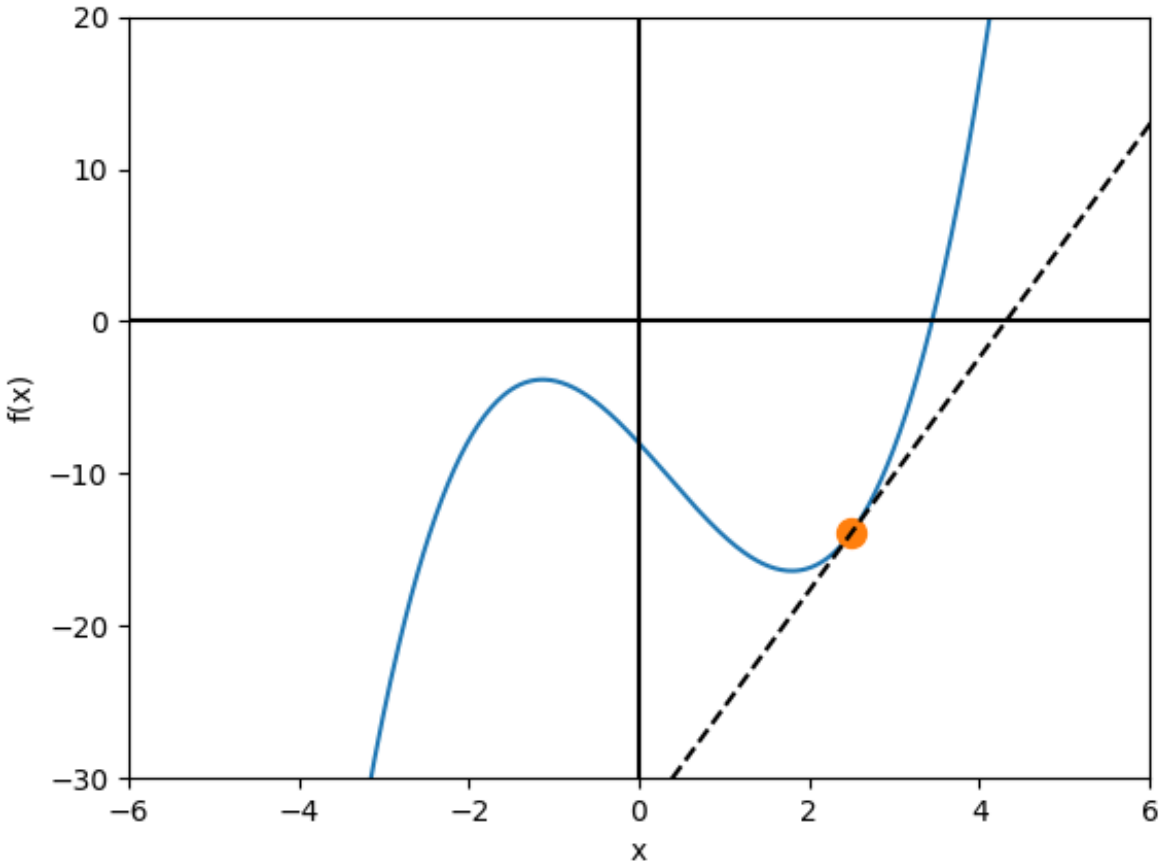
Intuição para o SGD



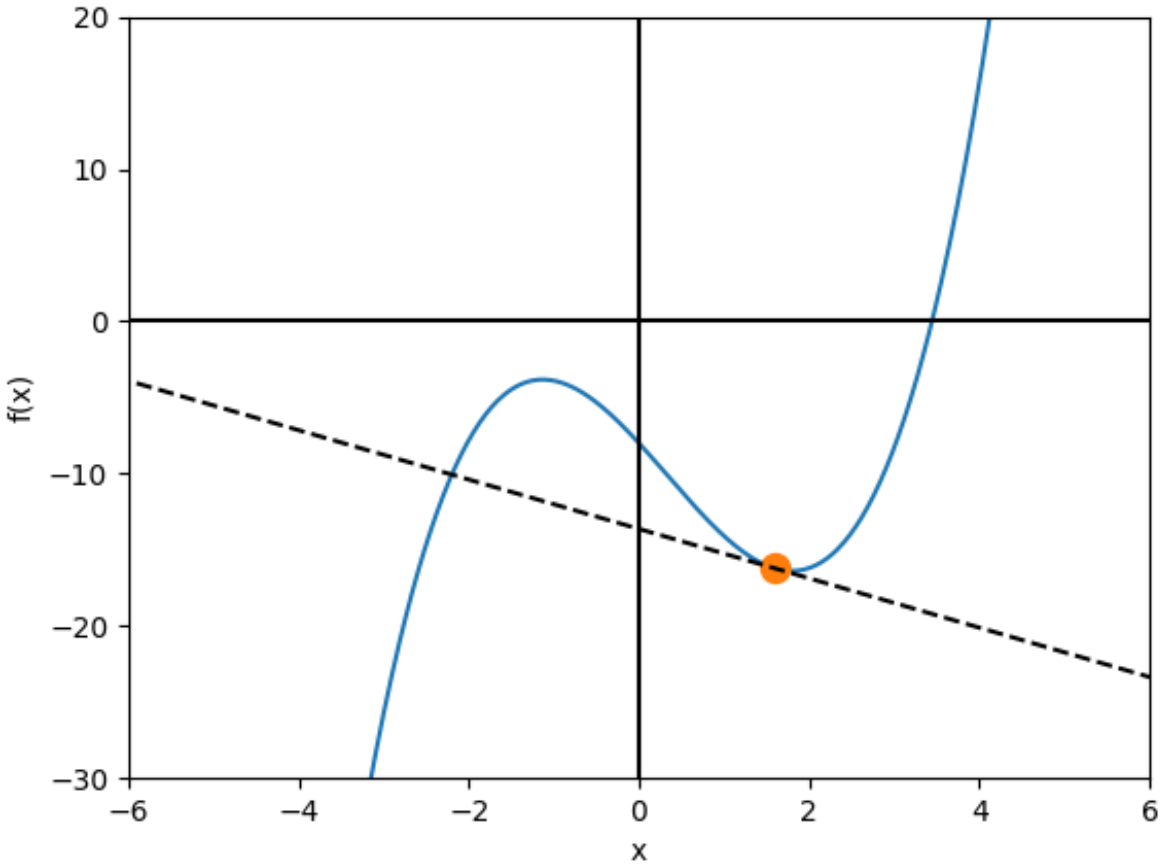
Intuição para o SGD



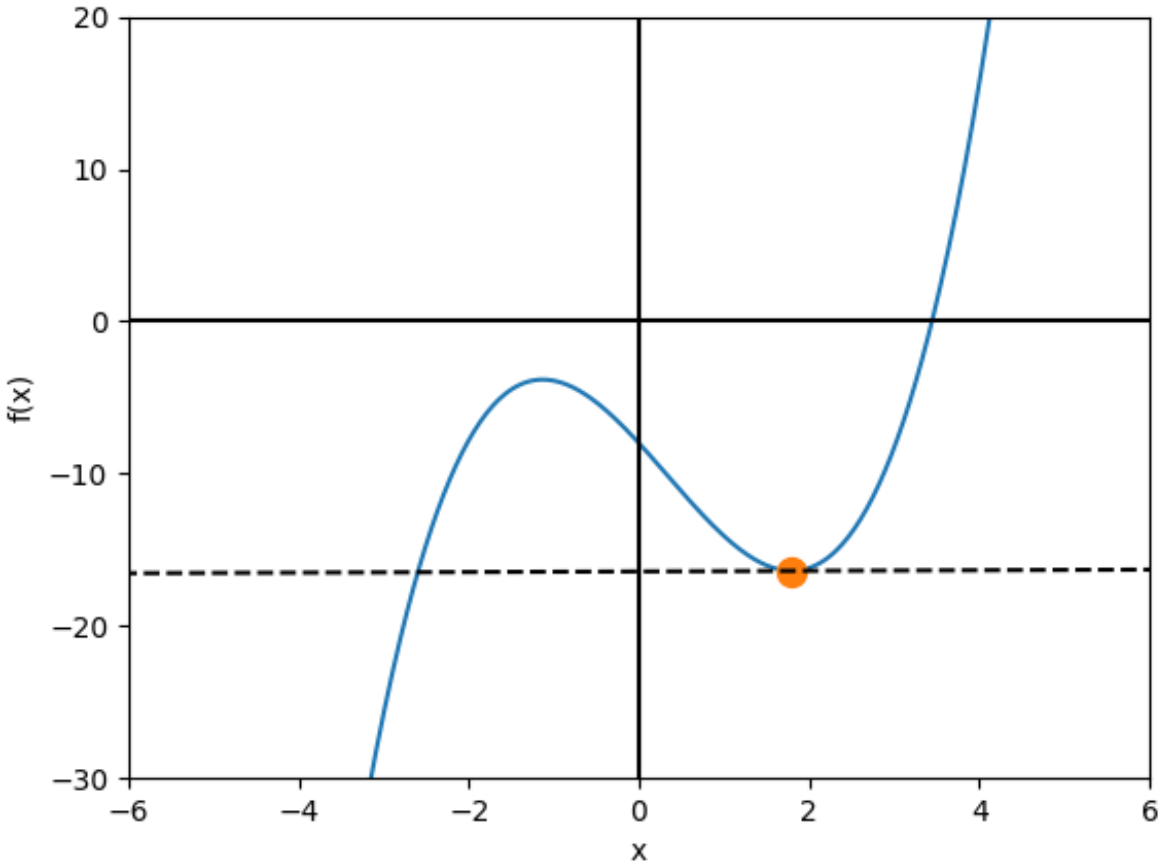
Intuição para o SGD



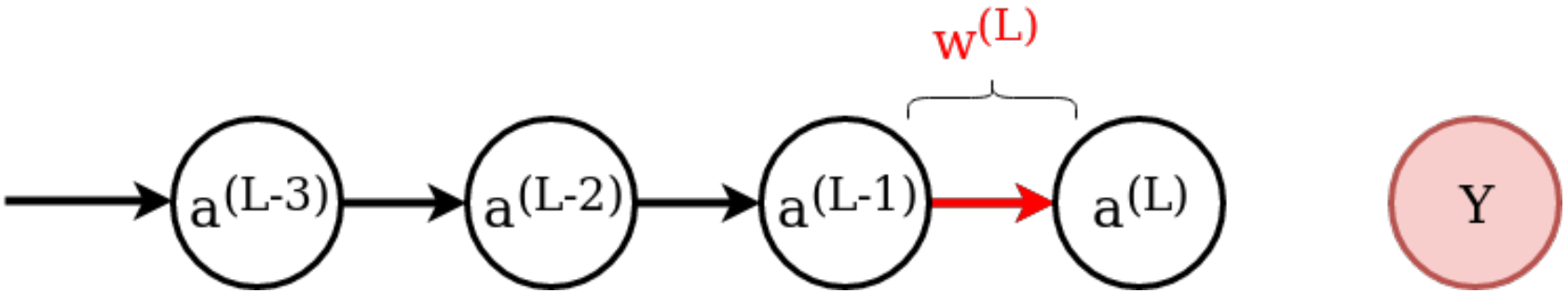
Intuição para o SGD

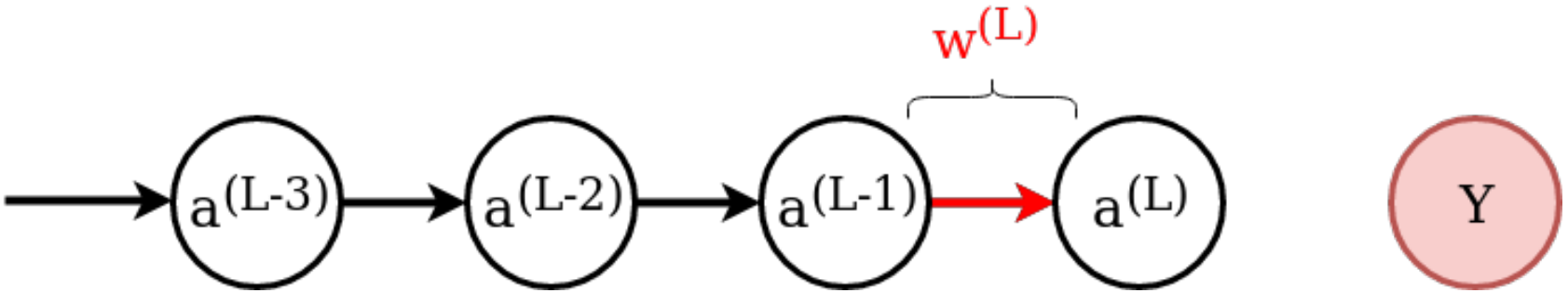


Intuição para o SGD



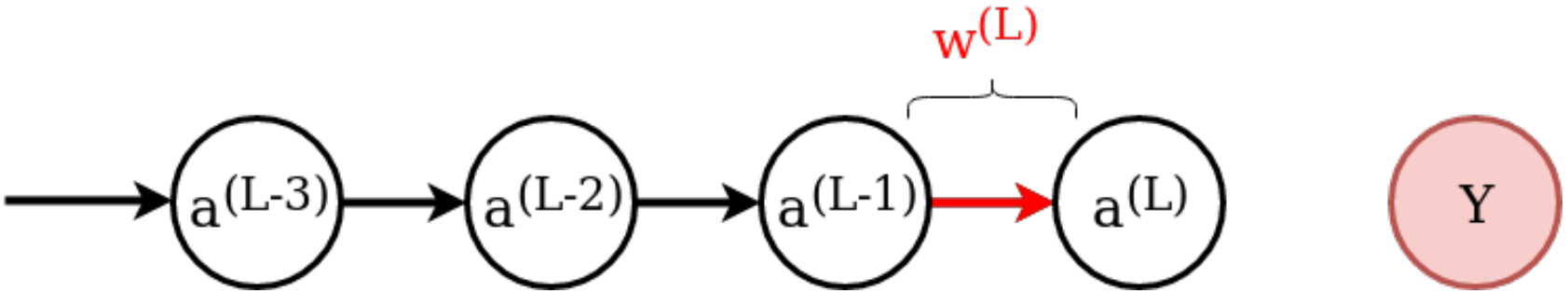
Backpropagation





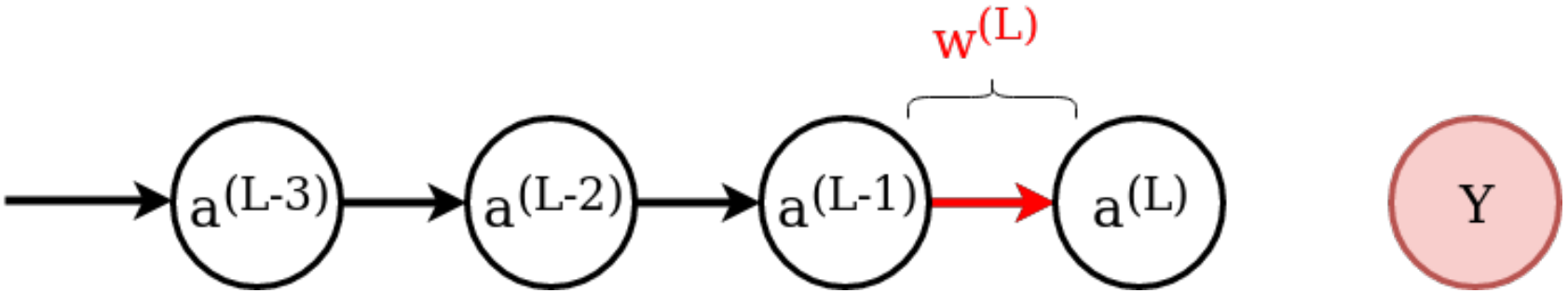
- Saída desejada $\rightarrow Y$, ou seja, é desejado que $a^{(L)} = Y$
- Custo $\rightarrow C_0(...) = (a^{(L)} - Y)^2$, C_0 deve ser minimizado

Backpropagation

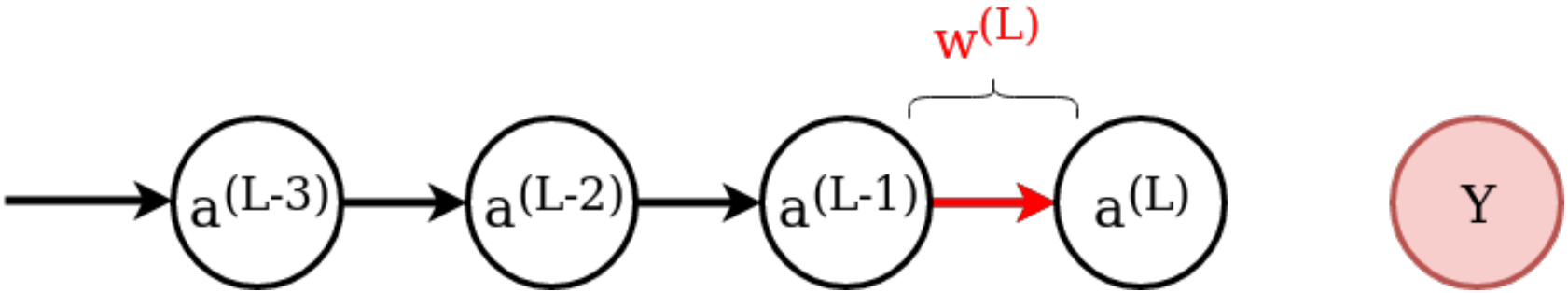


- Saída desejada $\rightarrow Y$, ou seja, é desejado que $a^{(L)} = Y$
- Custo $\rightarrow C_0(...) = (a^{(L)} - Y)^2$, C_0 deve ser minimizado
- $a^{(L)} = \sigma(w^{(L)} * a^{(L-1)} + b^{(L)}) = \sigma(z^{(L)})$

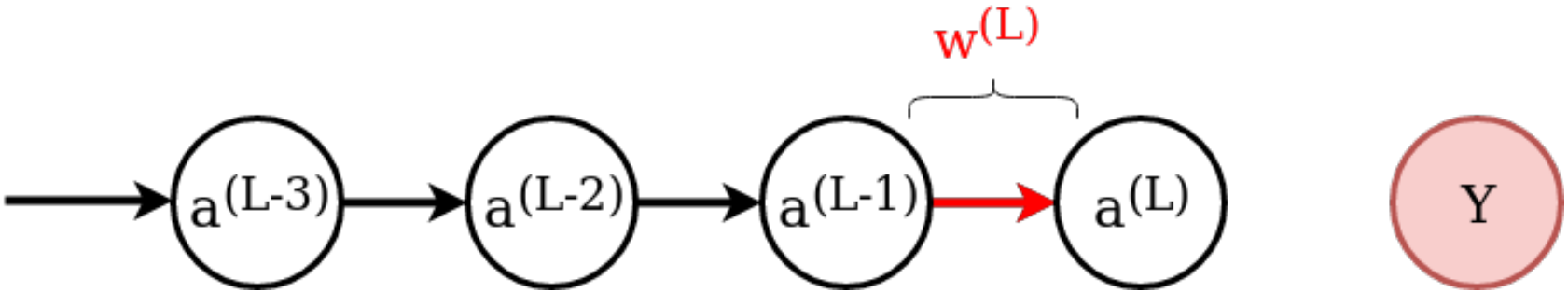
Backpropagation



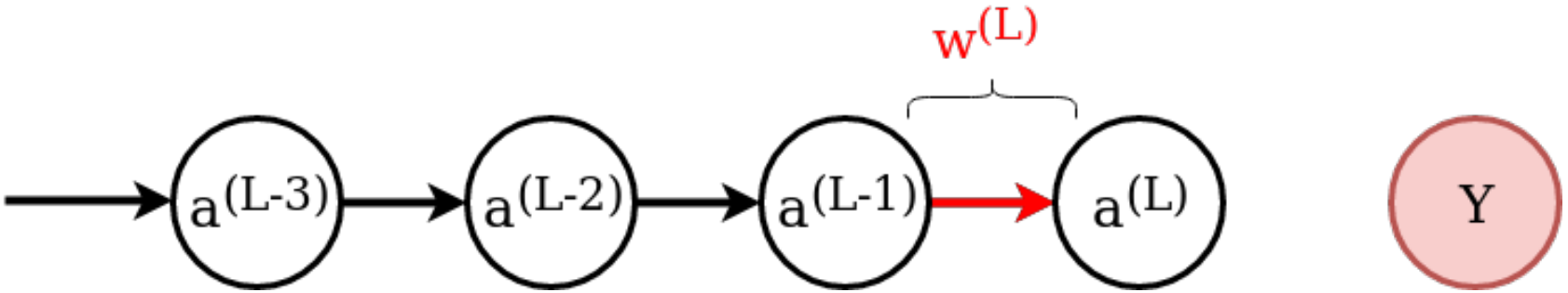
- Saída desejada $\rightarrow Y$, ou seja, é desejado que $a^{(L)} = Y$
- Custo $\rightarrow C_0(...) = (a^{(L)} - Y)^2$, C_0 deve ser minimizado
- $a^{(L)} = \sigma(w^{(L)} * a^{(L-1)} + b^{(L)}) = \sigma(z^{(L)})$
- $a^{(L)} = \sigma(z^{(L)})$



- Saída desejada $\rightarrow Y$, ou seja, é desejado que $a^{(L)} = Y$
- Custo $\rightarrow C_0(...) = (a^{(L)} - Y)^2$, C_0 deve ser minimizado
- $a^{(L)} = \sigma(w^{(L)} * a^{(L-1)} + b^{(L)}) = \sigma(z^{(L)})$
- $a^{(L)} = \sigma(z^{(L)})$
- $a^{(L-1)} = \sigma(w^{(L-1)} * a^{(L-2)} + b^{(L-1)}) = \sigma(z^{(L-1)})$

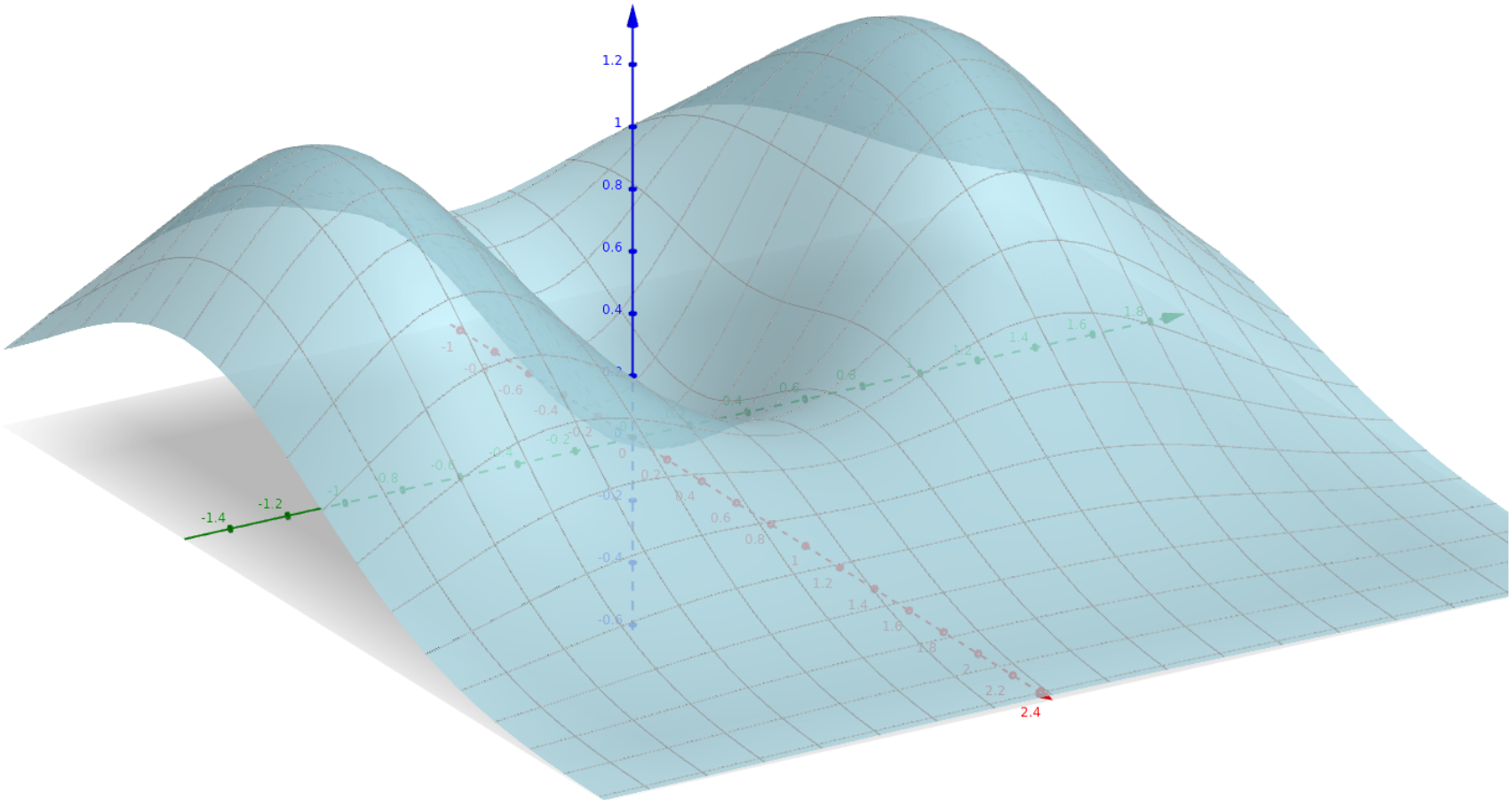


- Saída desejada $\rightarrow Y$, ou seja, é desejado que $a^{(L)} = Y$
- Custo $\rightarrow C_0(...) = (a^{(L)} - Y)^2$, C_0 deve ser minimizado
- $a^{(L)} = \sigma(w^{(L)} * a^{(L-1)} + b^{(L)}) = \sigma(z^{(L)})$
- $a^{(L)} = \sigma(z^{(L)})$
- $a^{(L-1)} = \sigma(w^{(L-1)} * a^{(L-2)} + b^{(L-1)}) = \sigma(z^{(L-1)})$
- $C_0 = f(Y, a_{(L)})$

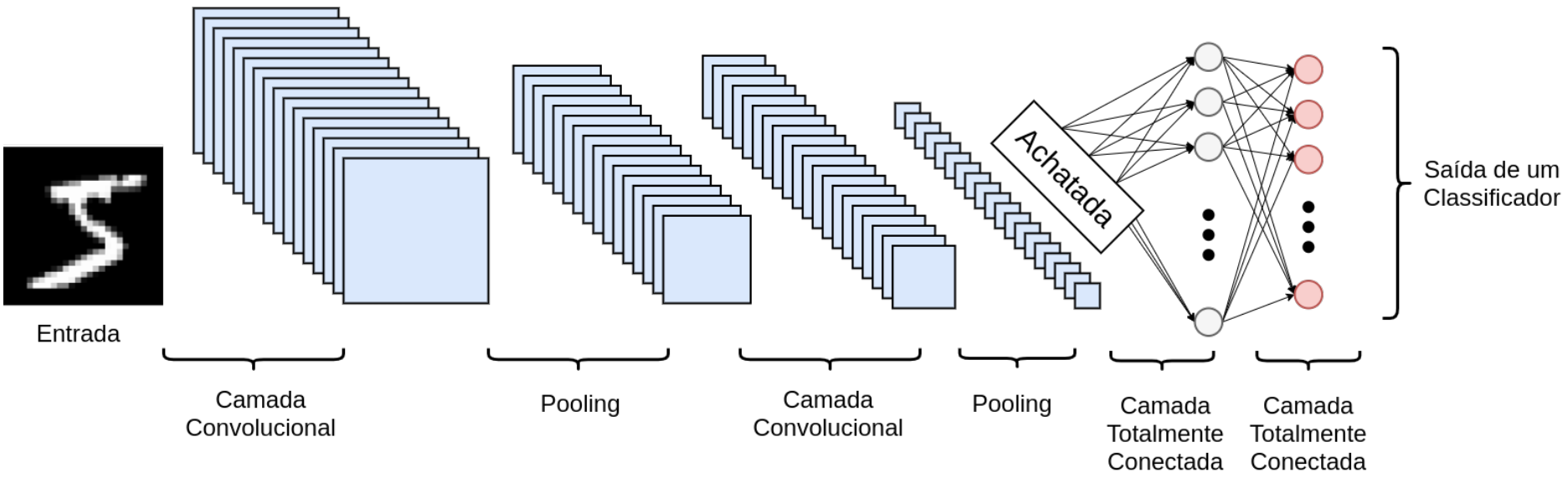


- Saída desejada $\rightarrow Y$, ou seja, é desejado que $a^{(L)} = Y$
- Custo $\rightarrow C_0(...) = (a^{(L)} - Y)^2$, C_0 deve ser minimizado
- $a^{(L)} = \sigma(w^{(L)} * a^{(L-1)} + b^{(L)}) = \sigma(z^{(L)})$
- $a^{(L)} = \sigma(z^{(L)})$
- $a^{(L-1)} = \sigma(w^{(L-1)} * a^{(L-2)} + b^{(L-1)}) = \sigma(z^{(L-1)})$
- $C_0 = f(Y, a_{(L)})$
- $a_{(L)} = f(w^{(L)}, a^{(L-1)}, b^{(L)})$

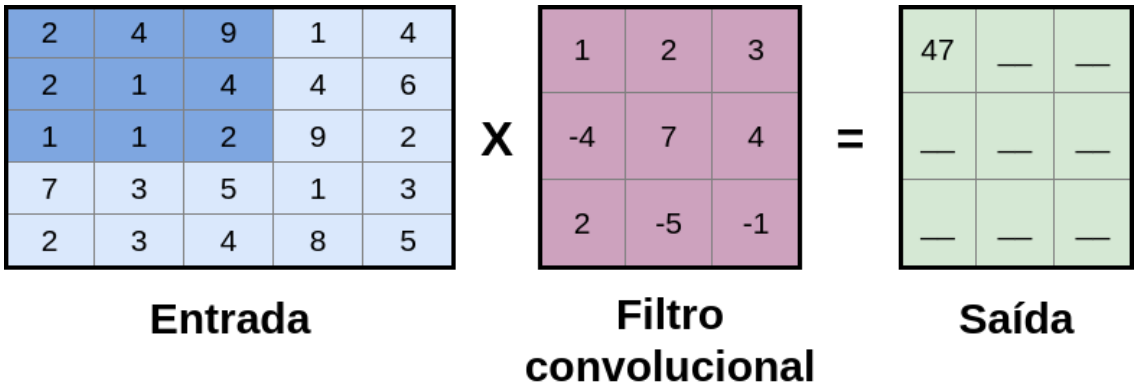
Stochastic Gradient Descent (SGD)



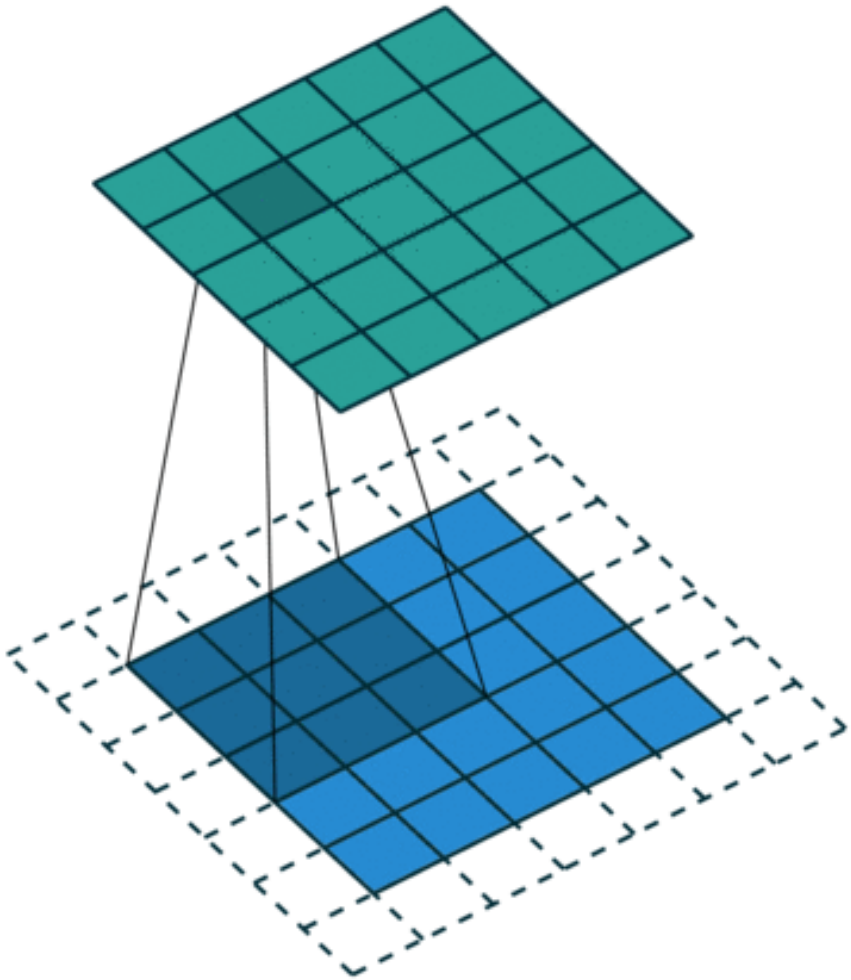
Redes Neurais Convolucionais



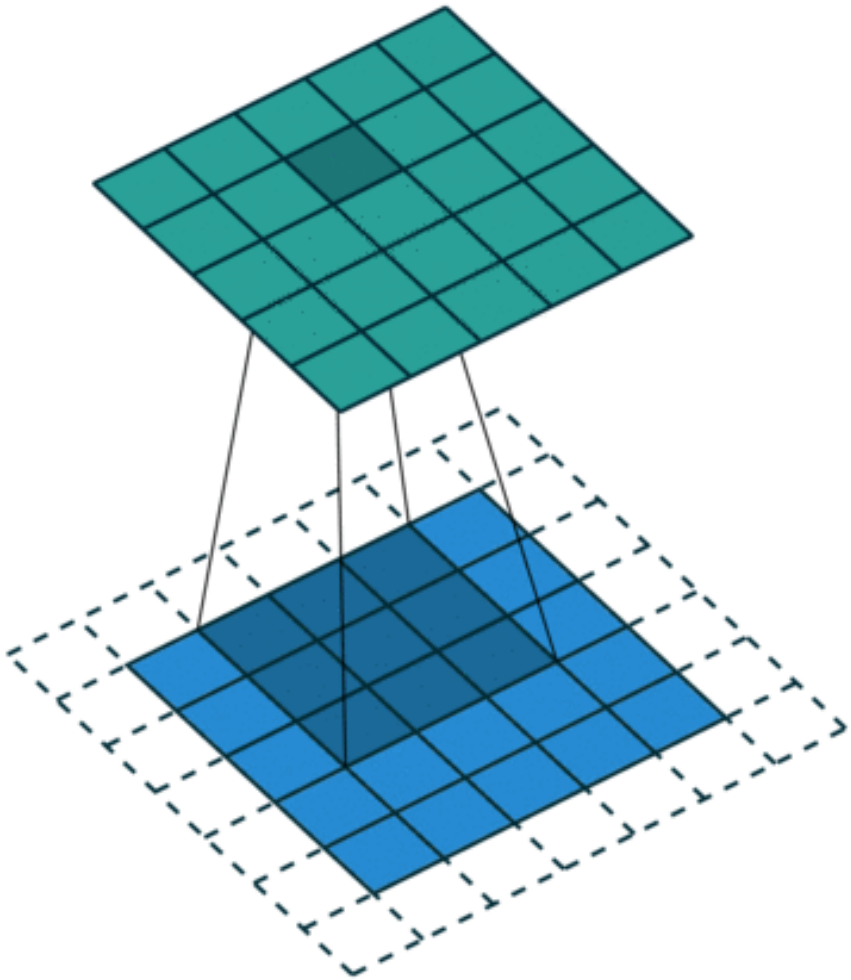
Filtros Convolucionais



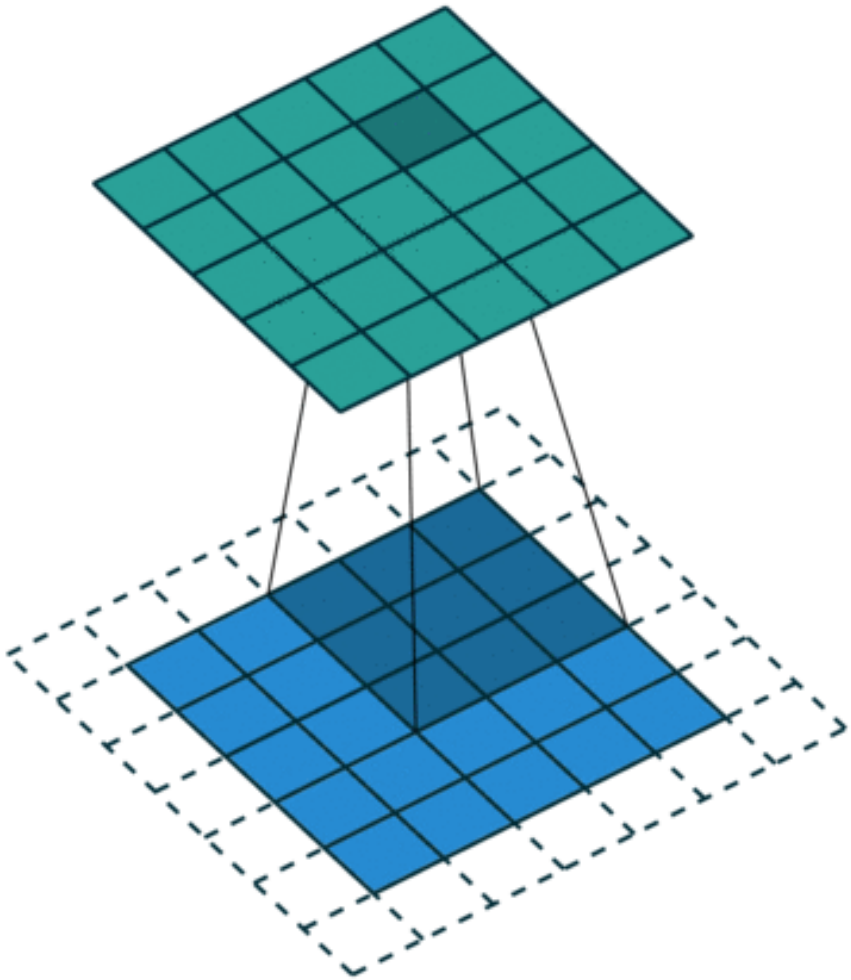
Convolução



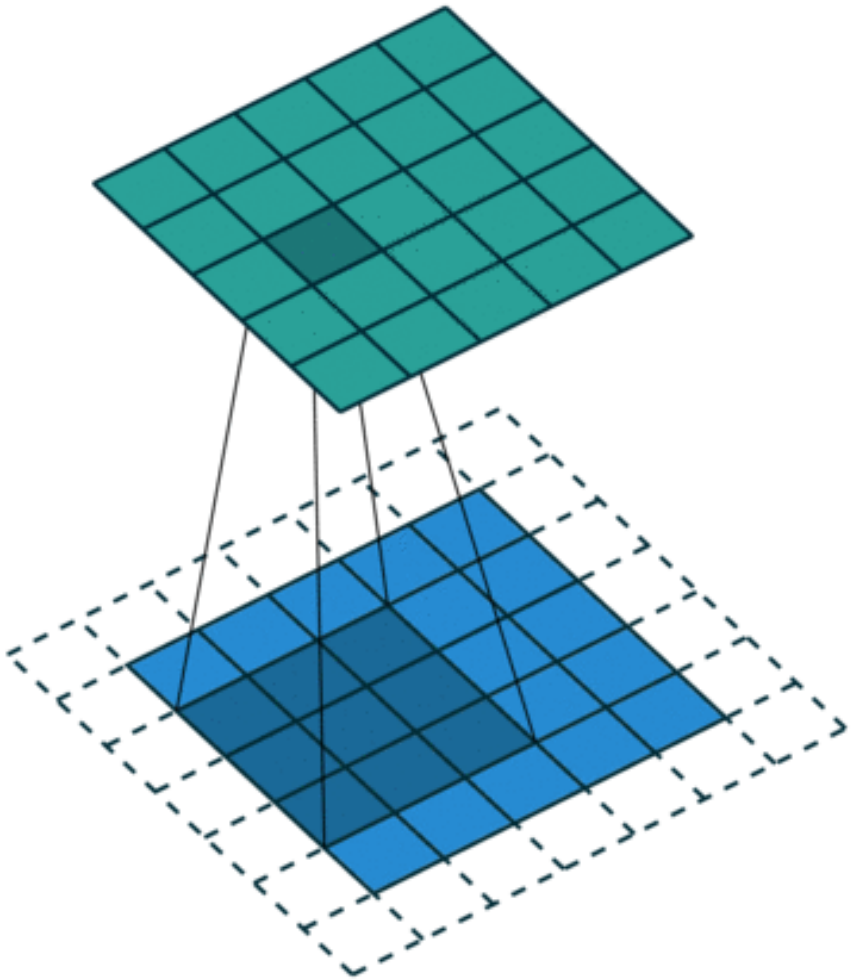
Convolução



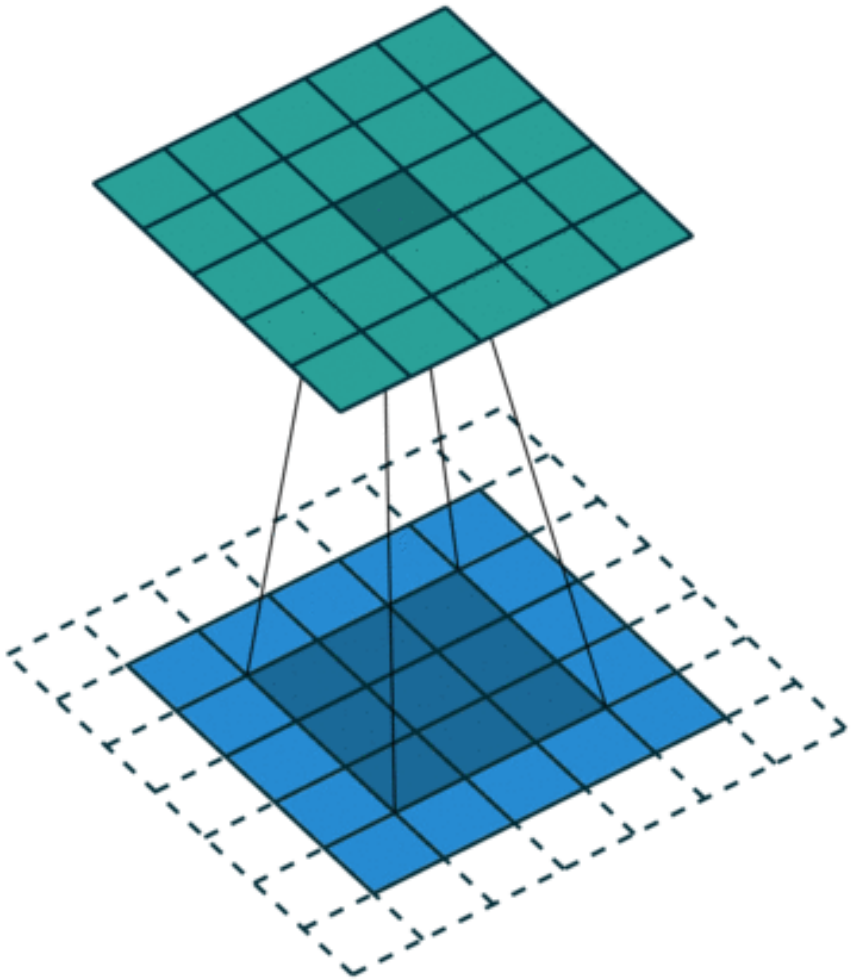
Convolução



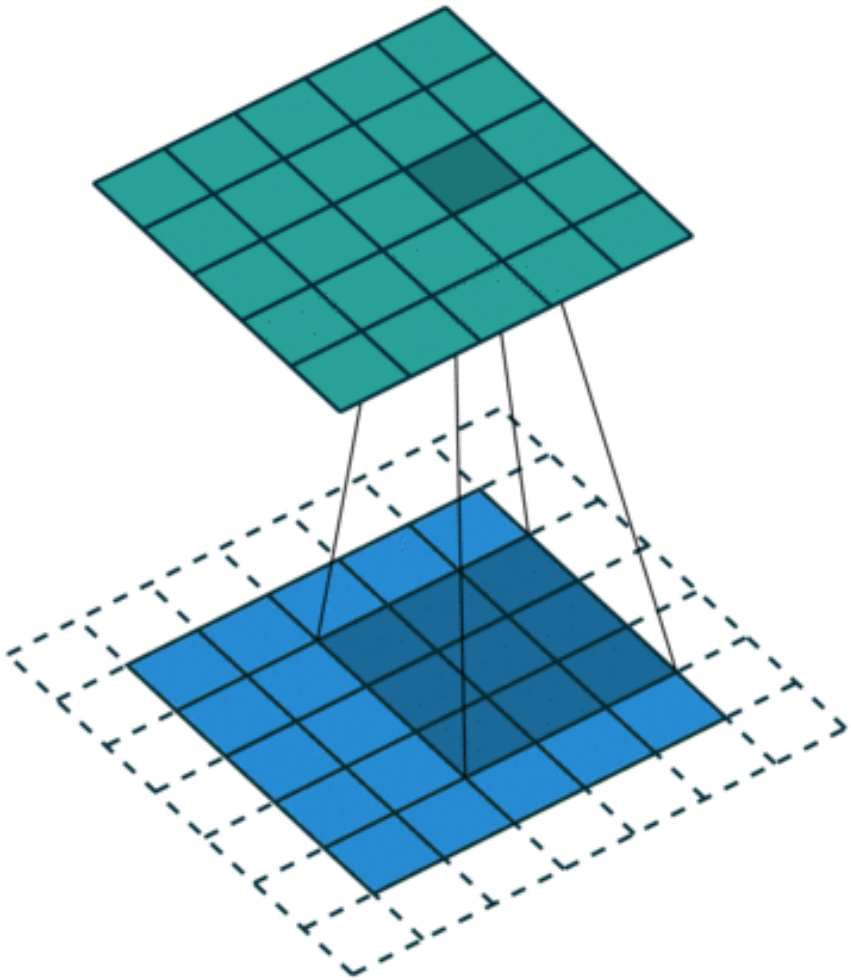
Convolução



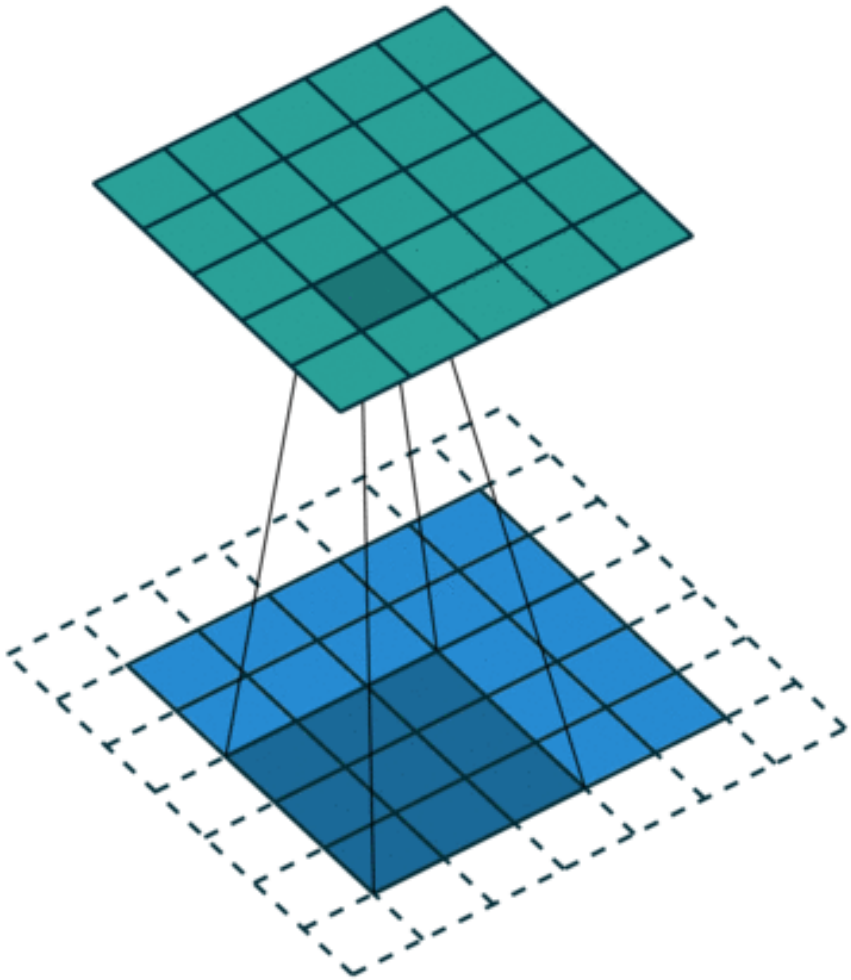
Convolução



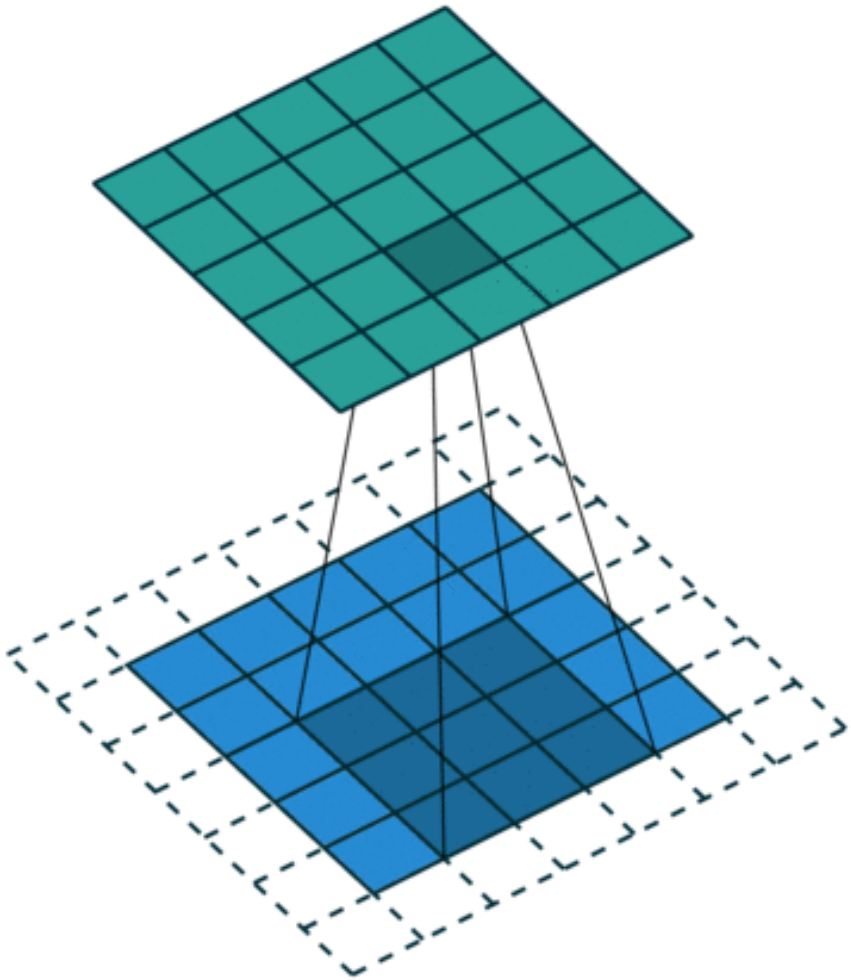
Convolução



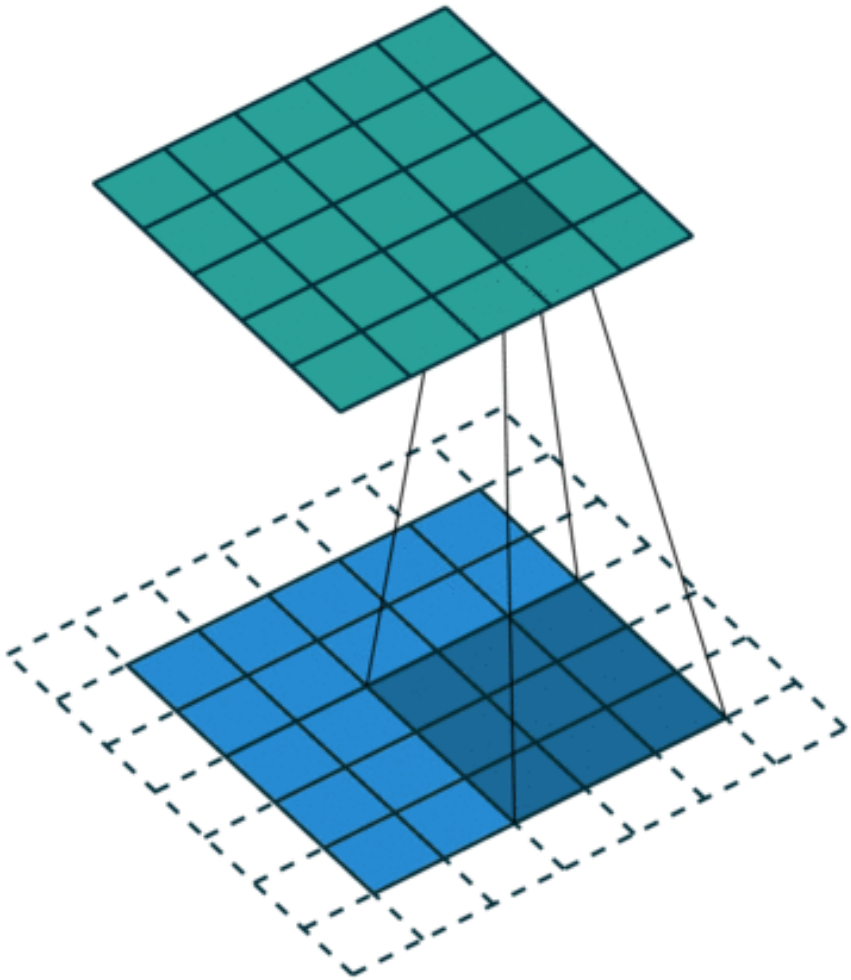
Convolução



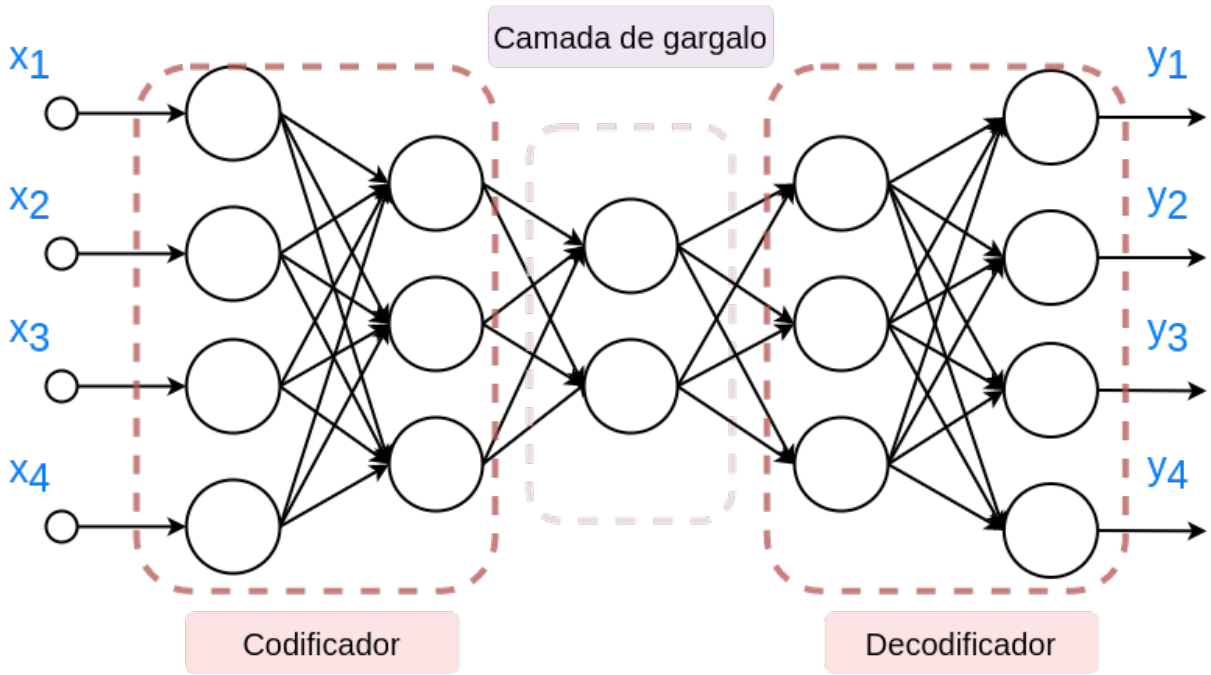
Convolução



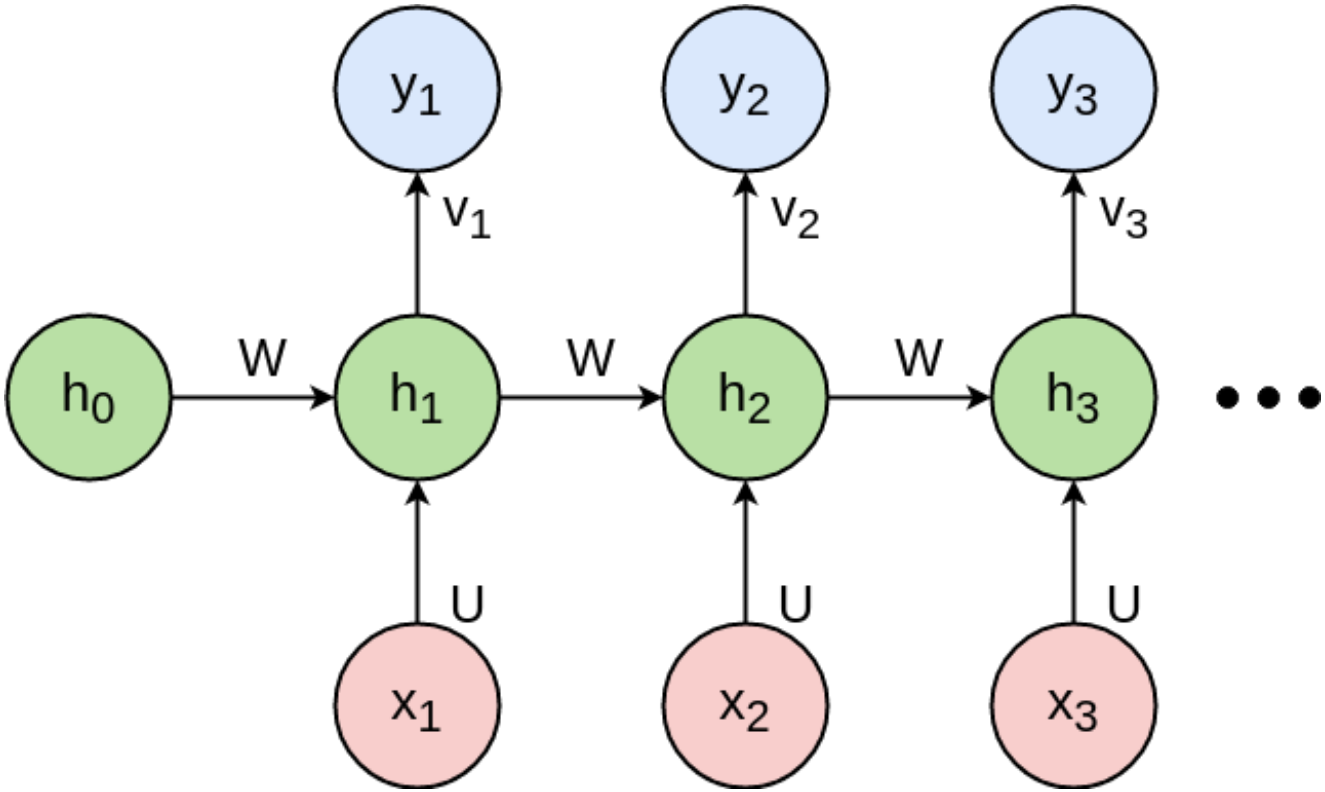
Convolução



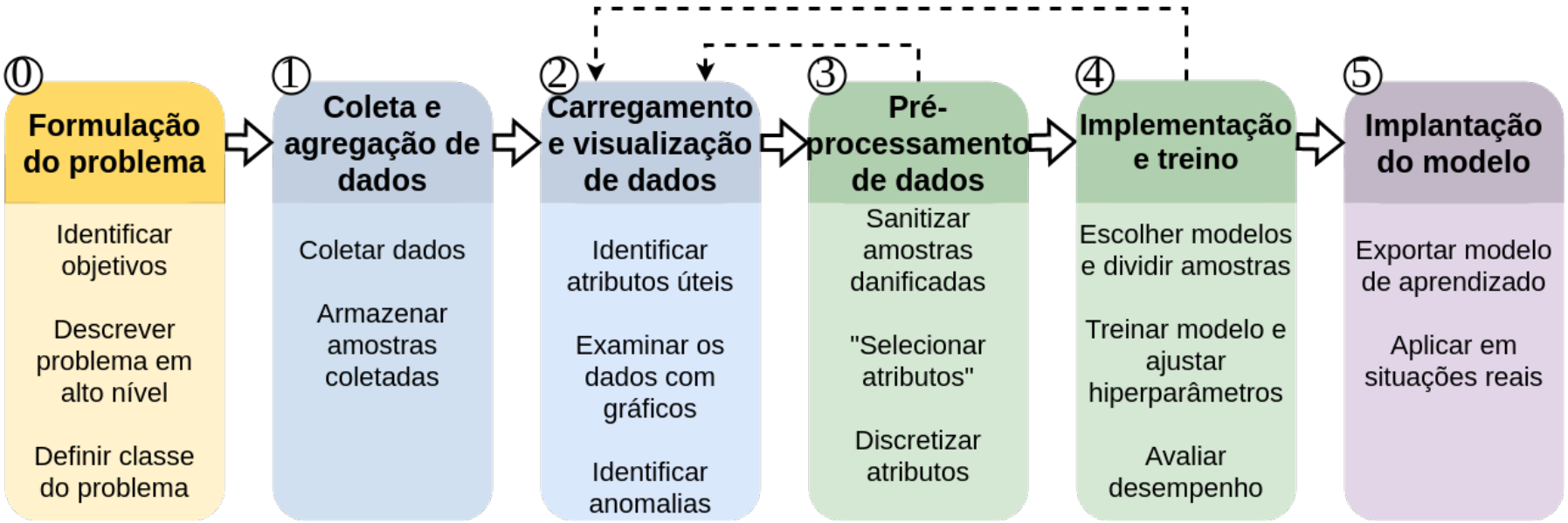
Redes Neurais Autoassociativas



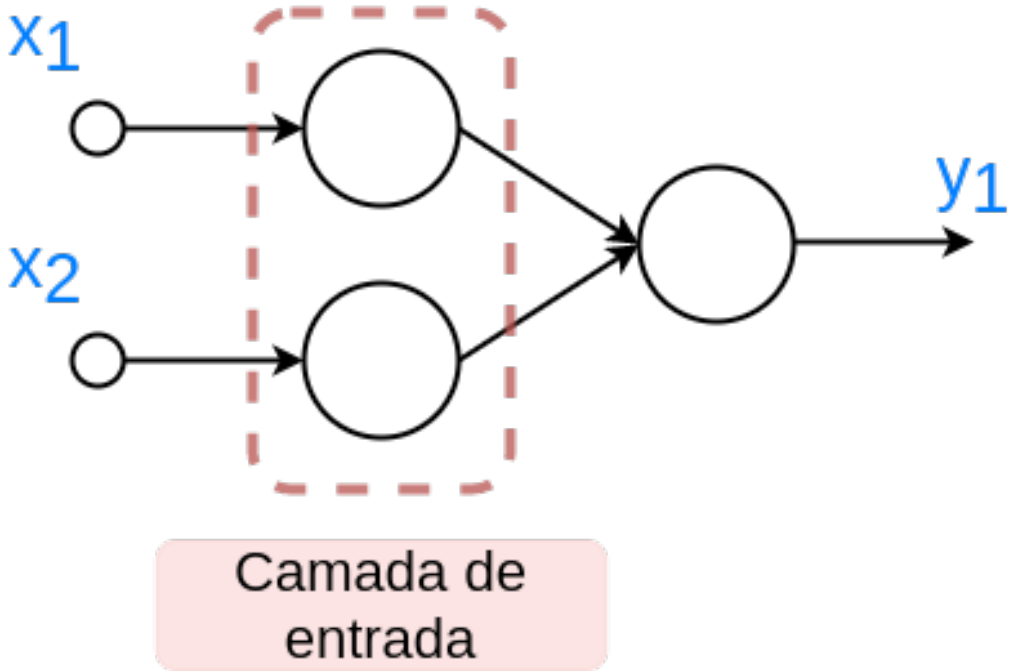
Redes Neurais Recorrentes



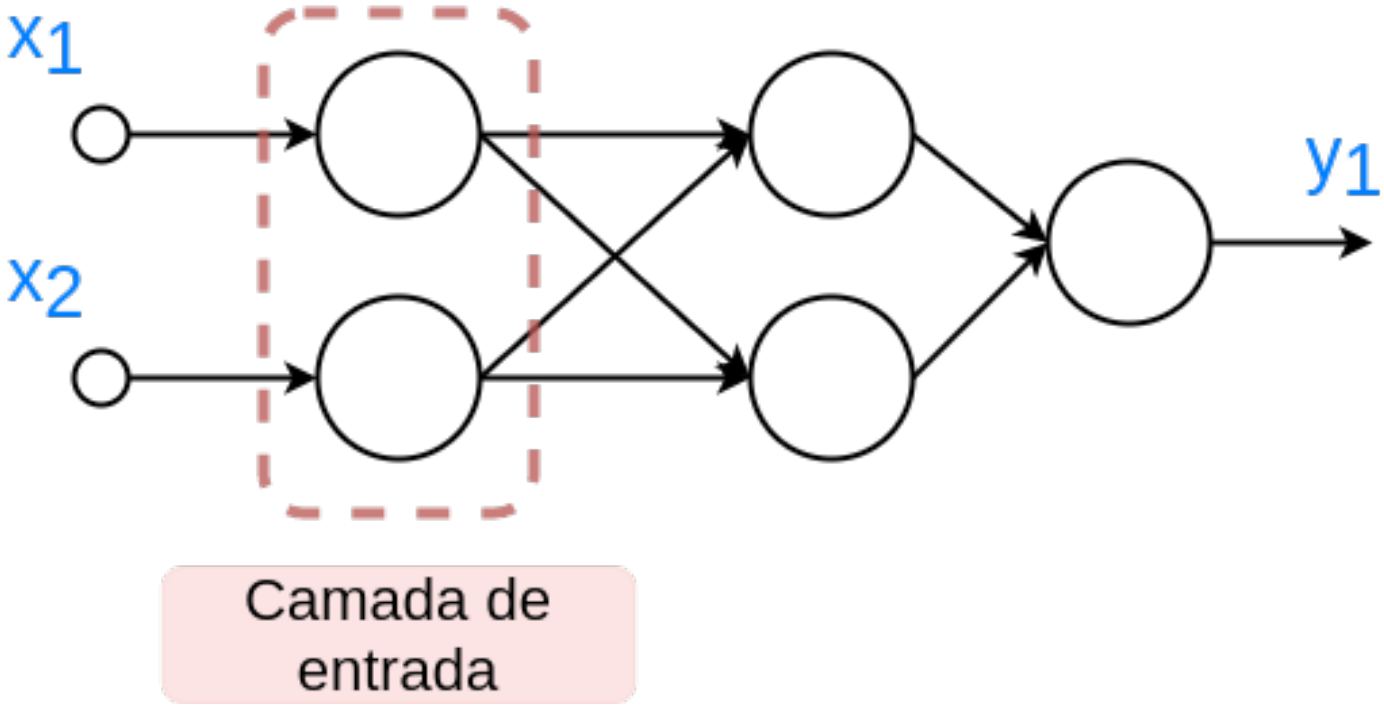
Fluxo de Trabalho Típico



Rede Neural Rasa



Rede Neural “Profunda”



1. Introdução ao Aprendizado Profundo
   - Aprendizado de Máquina
   - Redes Neurais e Aprendizado Profundo
2. Circuito de uma "Rede Neural" com Arduino
3. Aprendizado Federado
   - Definindo Privacidade
   - Distribuindo Aprendizado
   - Aplicações Atuais
4. Discussão: Como Arduino Contribui para o Aprendizado Federado?

Brechas e Comportamento

- Desafio Netflix
- Dados no formato `<user, movie, date of grade, grade>`
- Pesquisadores da *University of Texas at Austin* identificaram usuários cruzando informações com a base de dados do IMDb em 2007
- Em 2010 Netflix fez um acordo com usuários que iniciaram um processo em 2019

Brechas e Comportamento

- Desafio Netflix
- Dados no formato `<user, movie, date of grade, grade>`
- Pesquisadores da *University of Texas at Austin* identificaram usuários cruzando informações com a base de dados do IMDb em 2007
- Em 2010 Netflix fez um acordo com usuários que iniciaram um processo em 2019
- Paradoxo da privacidade

Brechas e Comportamento

- Desafio Netflix
- Dados no formato `<user, movie, date of grade, grade>`
- Pesquisadores da *University of Texas at Austin* identificaram usuários cruzando informações com a base de dados do IMDb em 2007
- Em 2010 Netflix fez um acordo com usuários que iniciaram um processo em 2019
- Paradoxo da privacidade

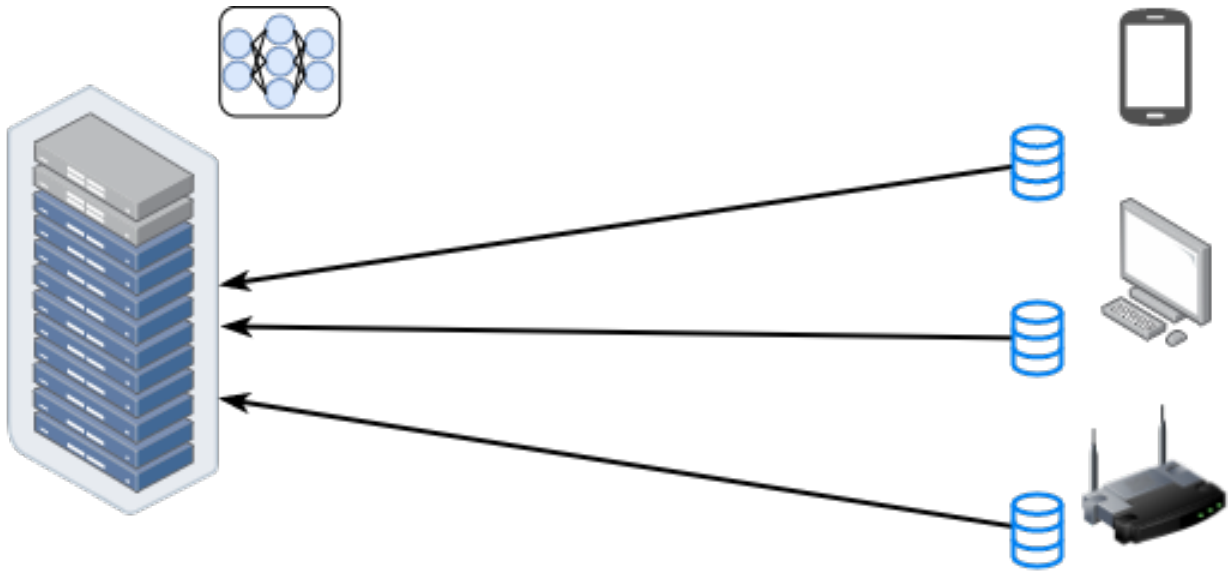
Privacidade diferencial:

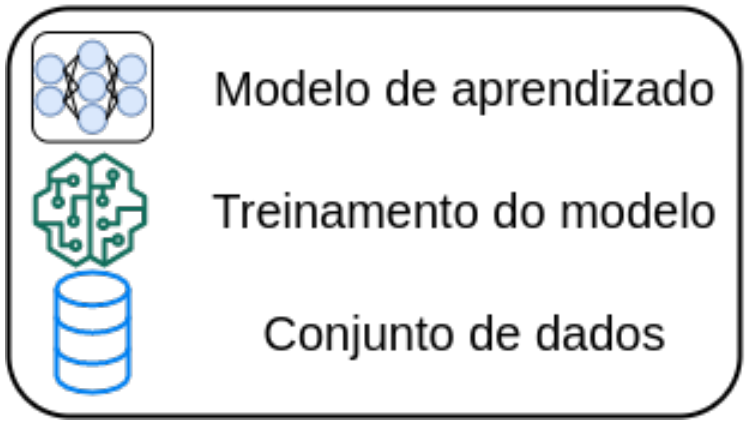
- Baseada no conceito de bases de dados adjacentes
- Dependente de aplicação
- Mecanismo de ruído aditivo
- “Dados + ruído = privacidade”

Cenário no Brasil

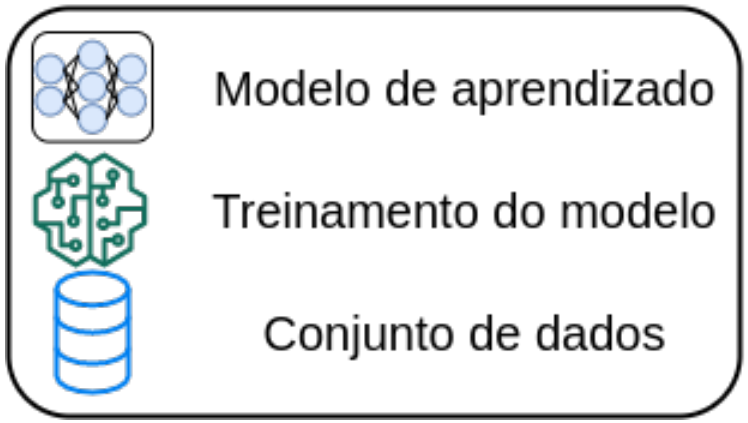
- Marco Civil da Internet de 2014 é um pouco vago sobre proteção de dados
- Lei nº 13.709/18 (Lei de Proteção de Dados – LGPD) de 2018, inspirada na *General Data Protection Regulation* (GDPR) Europeia de 2018
- Reflexo cotidiano da LGPD: confirmação para uso de *cookies*

Aprendizado Tradicional

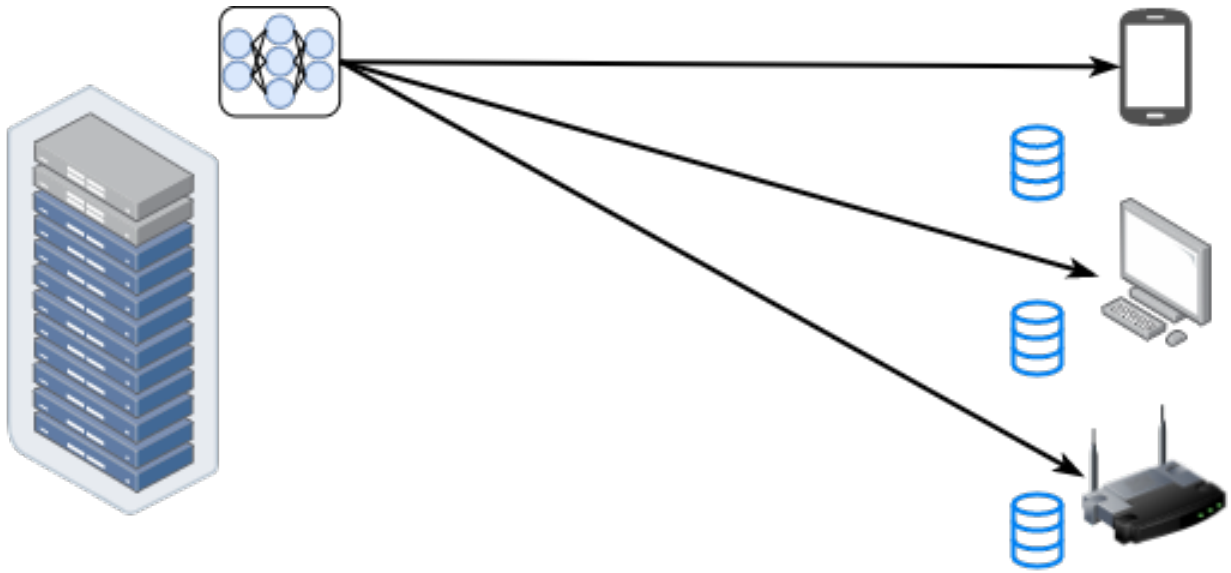


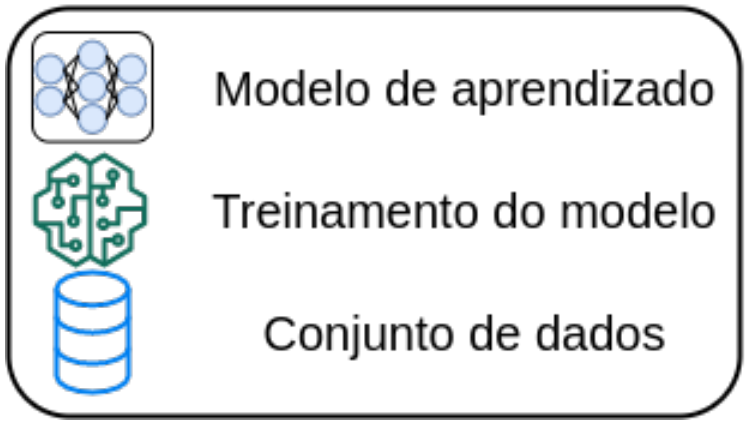


Aprendizado Tradicional

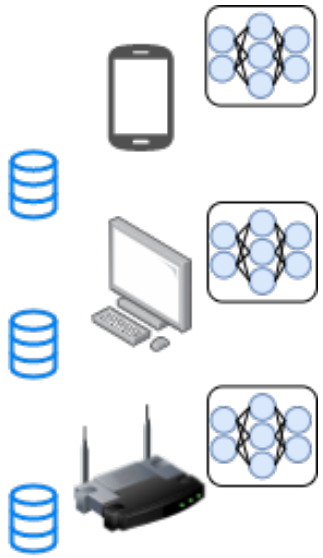


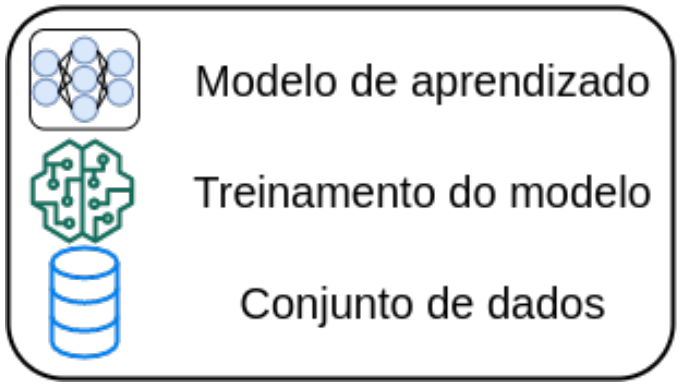
Aprendizado Tradicional





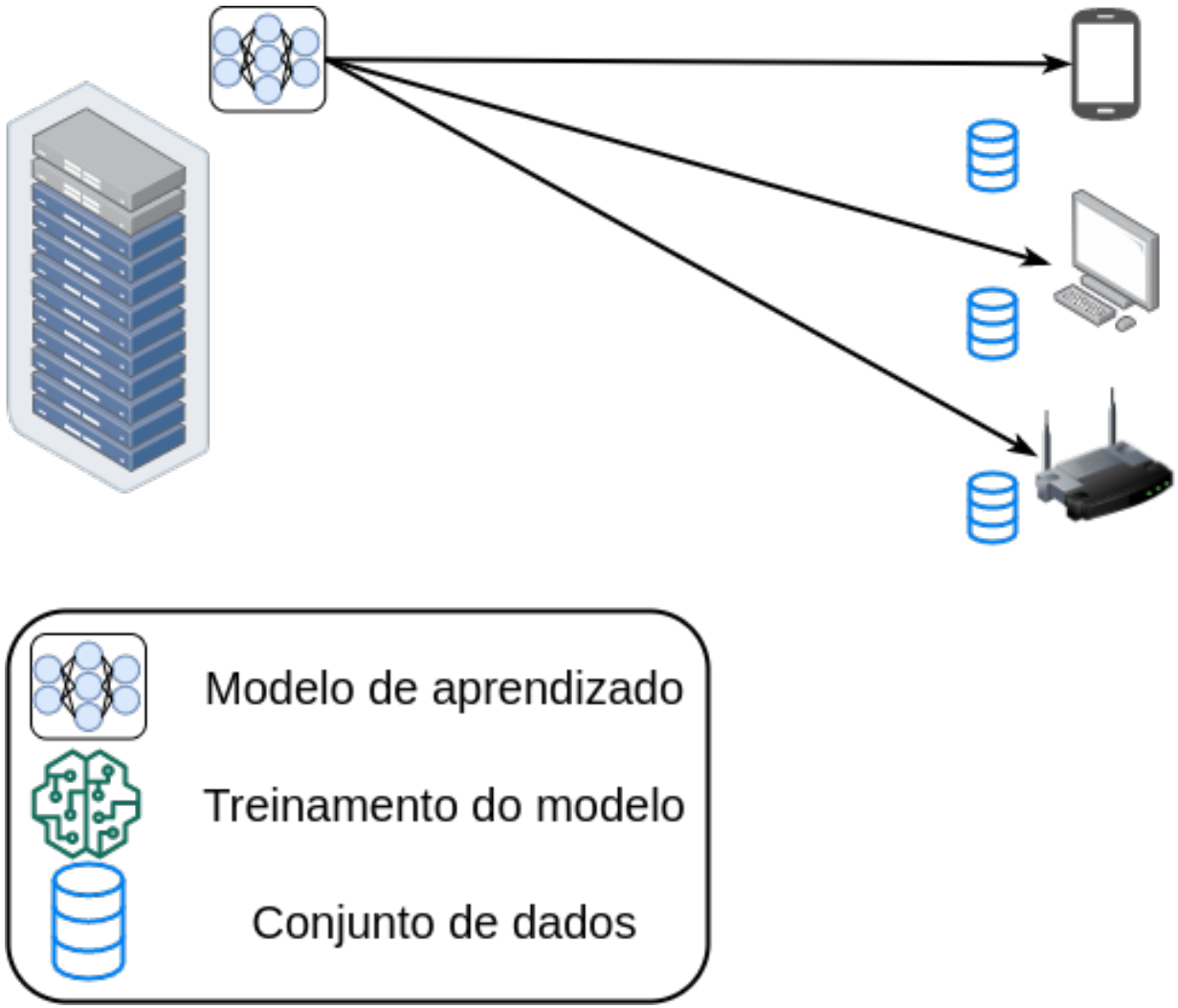
Aprendizado Tradicional



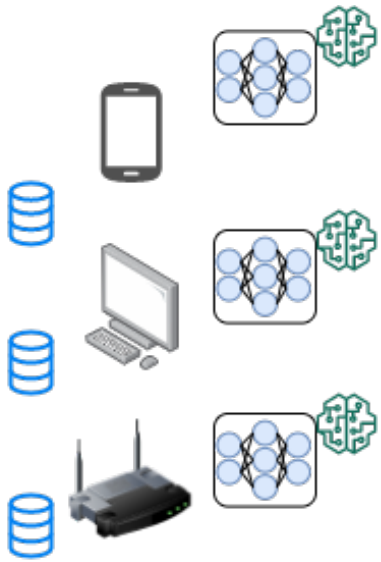


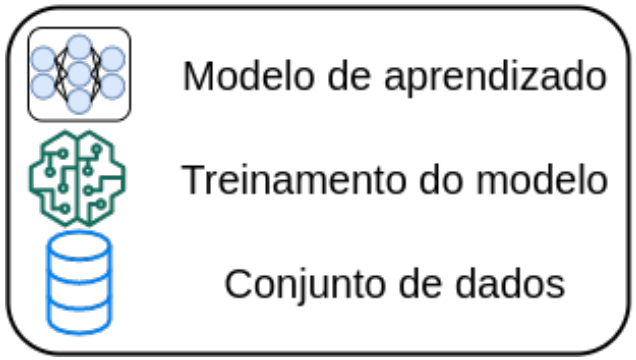
Aprendizado Federado

Aprendizado Federado

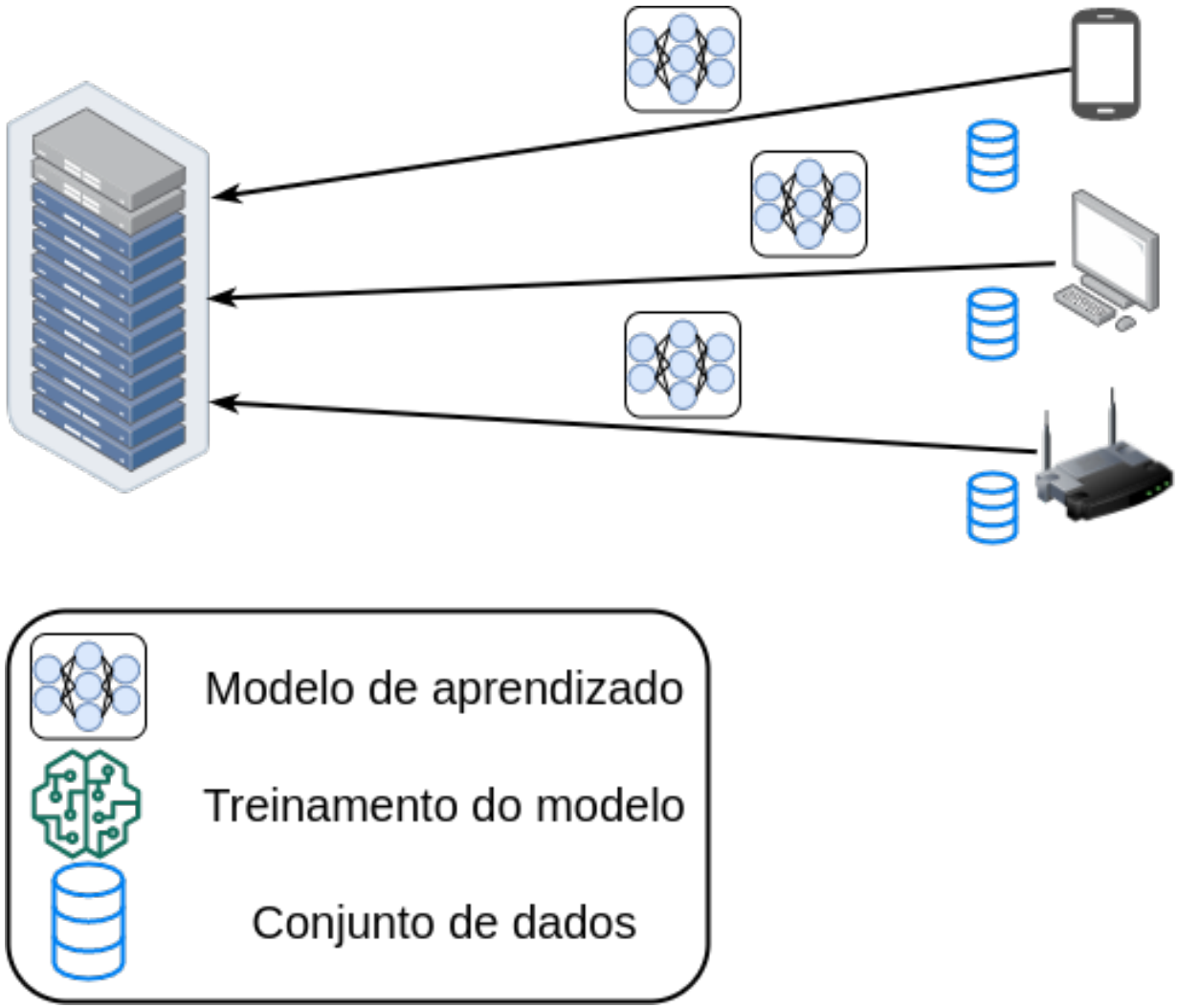


Aprendizado Federado

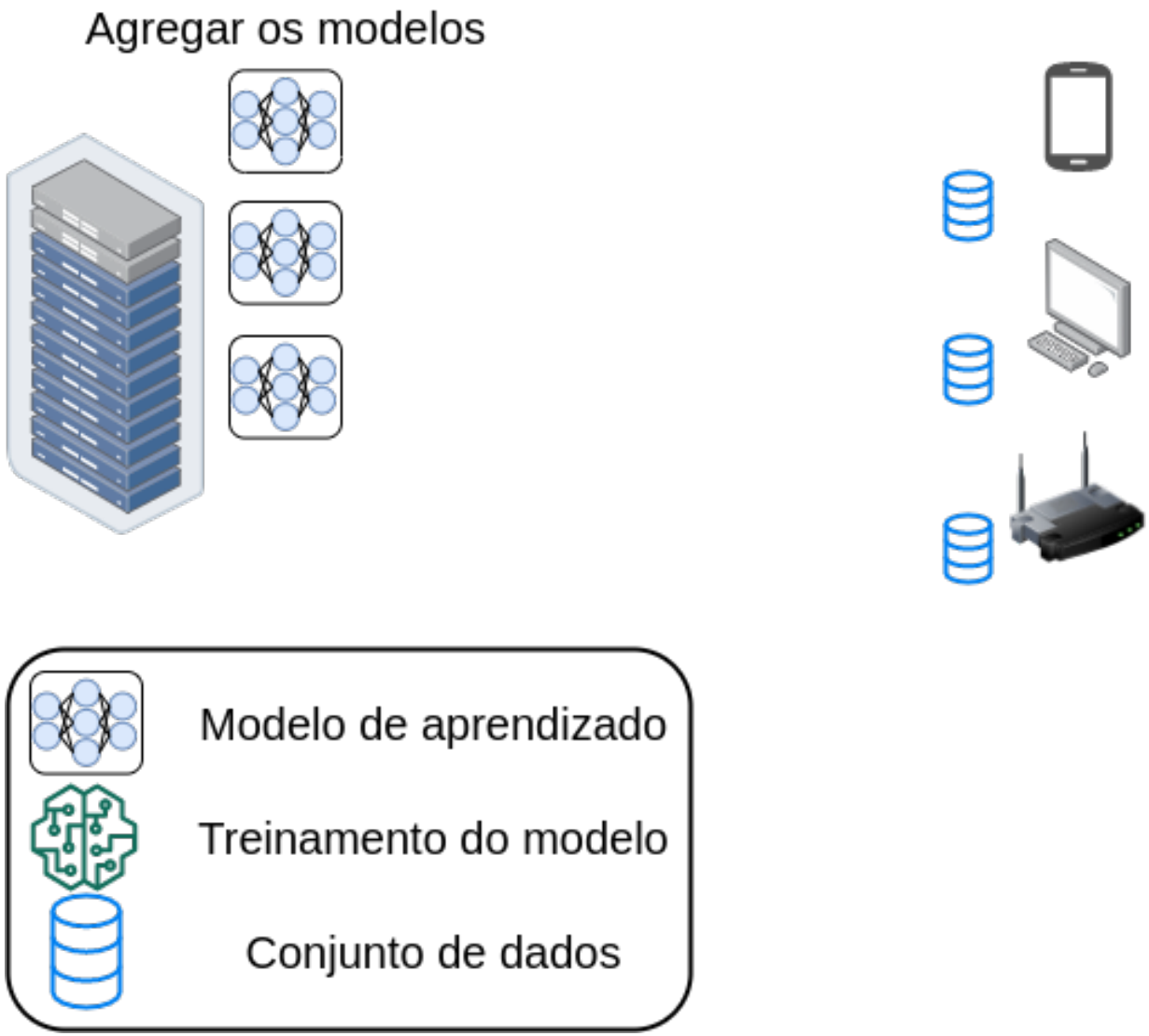




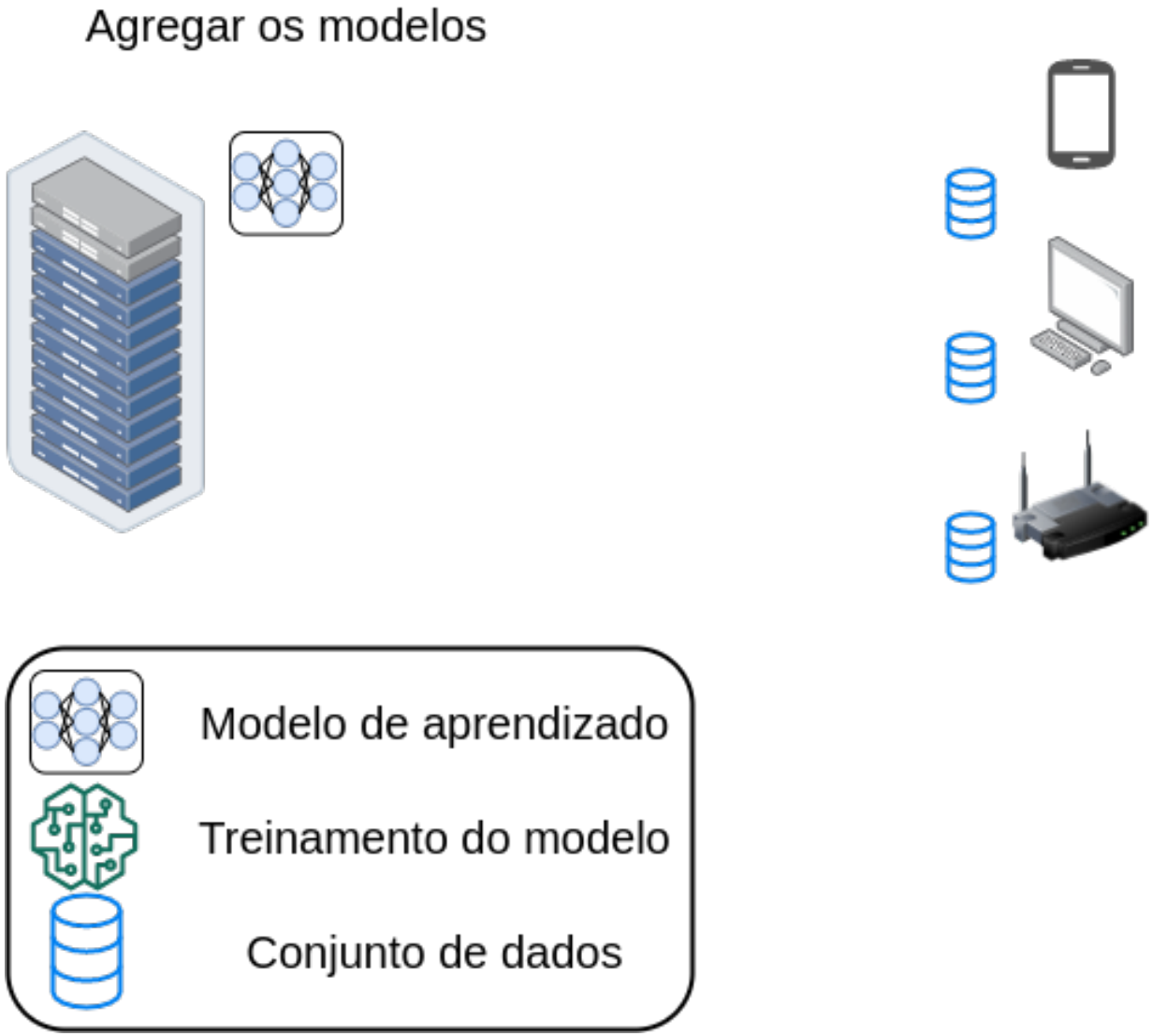
Aprendizado Federado



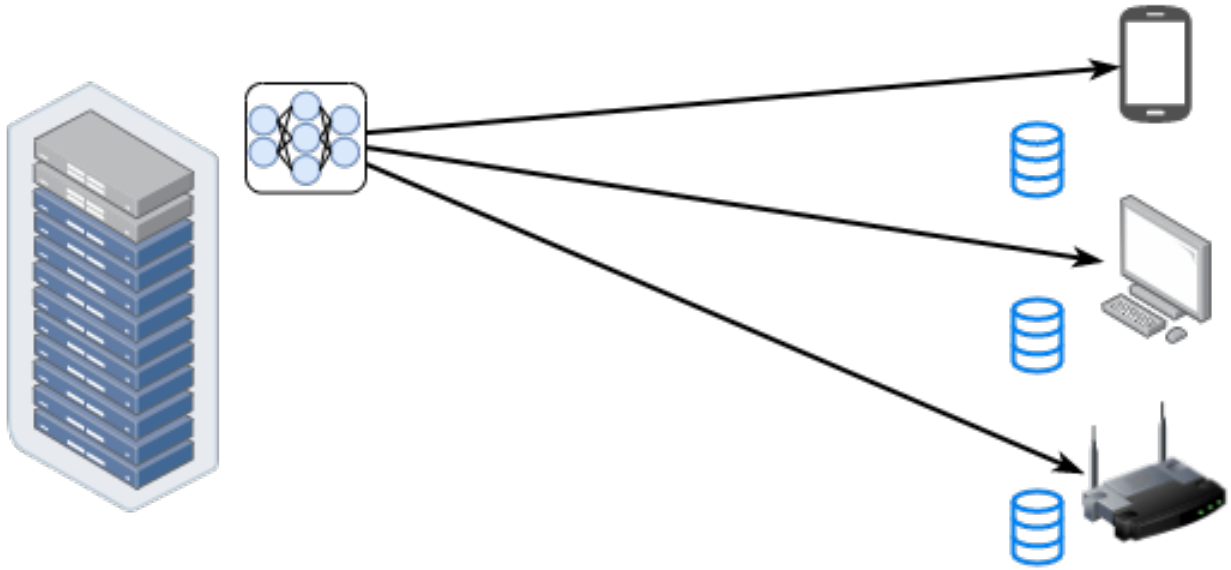
Aprendizado Federado

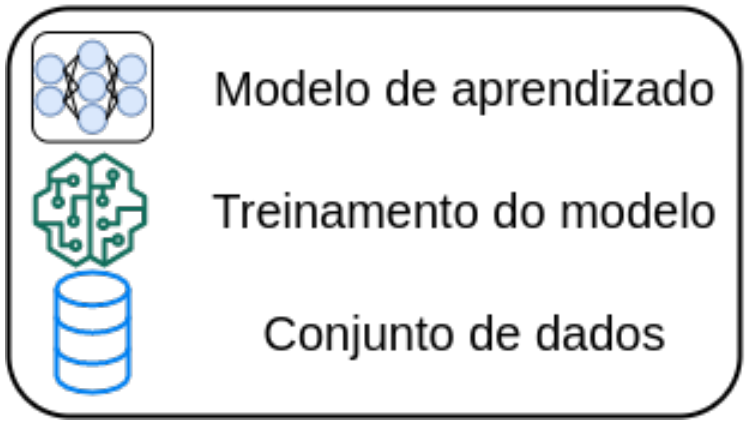


Aprendizado Federado

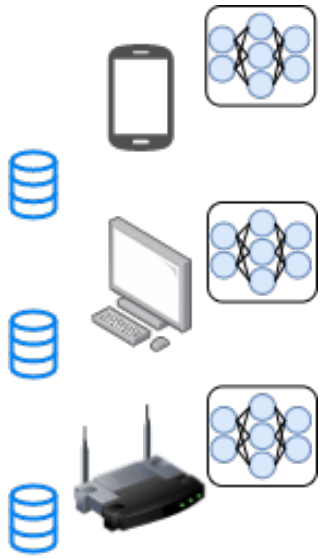


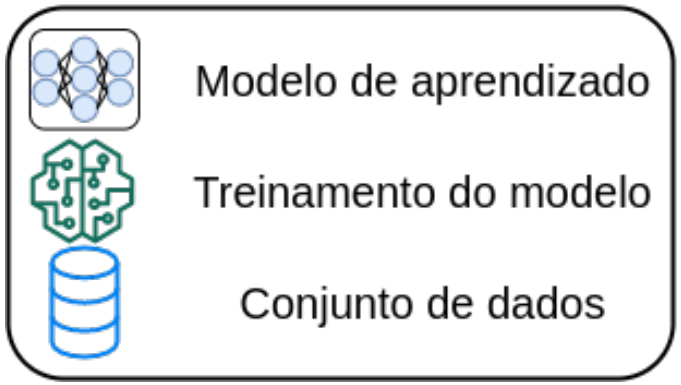
Aprendizado Federado





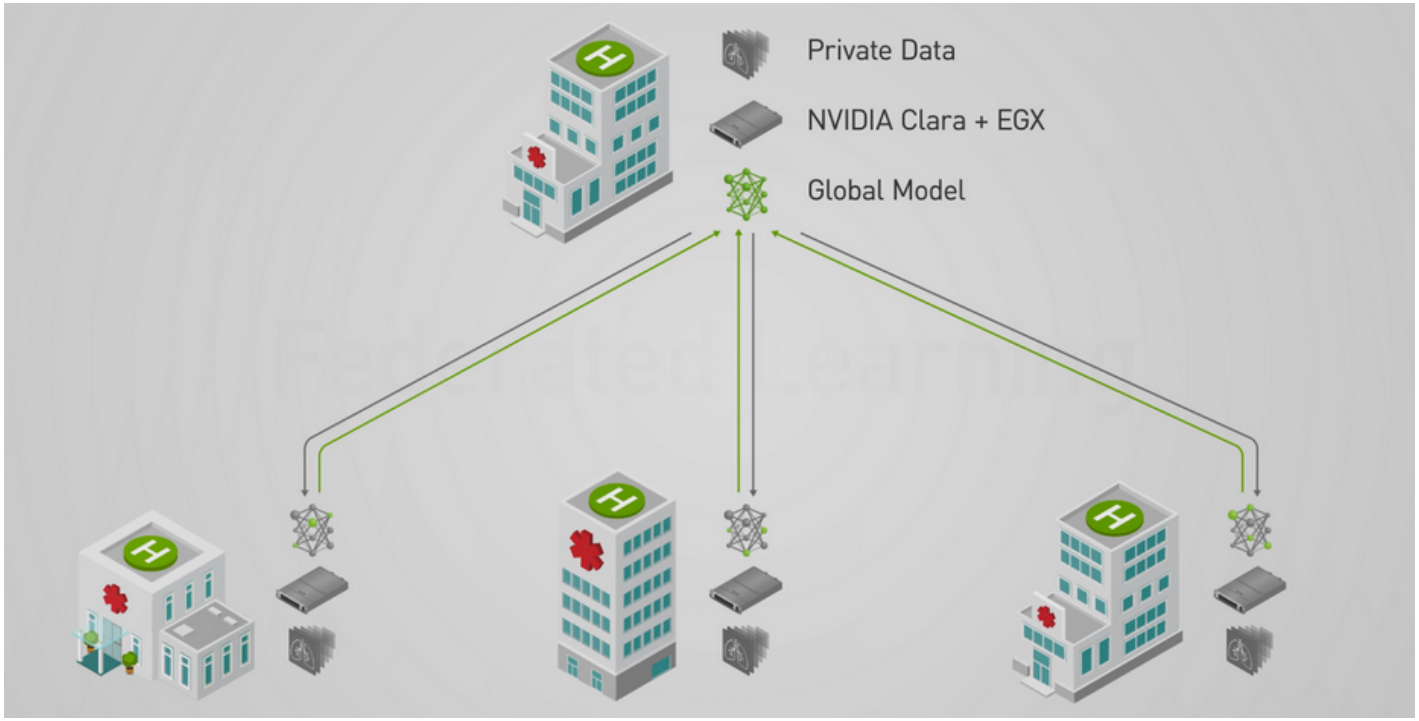
Aprendizado Federado





GBoard

NVIDIA *Healthcare*



Extraído de `https://developer.nvidia.com/blog/federated-learning-clara/`.

Etapas Típicas em Pesquisas Científicas

1. Estudar a literatura
2. Construir hipóteses
3. Simular e analisar
4. Publicar resultados e conclusões
5. Implementar e analisar
6. Publicar resultados e conclusões

Perguntas