Hacking, IA e Eu

Luiz Gastão de Lara Jr
gazstao@gmail.com

aztechtecnologia.com.br
https://bit.ly/recrutatech2025

Apresentação

aztechtecnologia.com.br

Técnico em Eletrônica (CEFET-PR) e Mecatrônica (Ensitec)
Tecnólogo em Informática (UTFPR)
Pós graduação em Gestão de Tecnologia da Informação e Comunicação (UTFPR)

OffTheMatrix: Guia de Hacking e Computação Forense
https://**bit.ly/recrutatech2025**

Quero compartilhar ferramentas poderosas

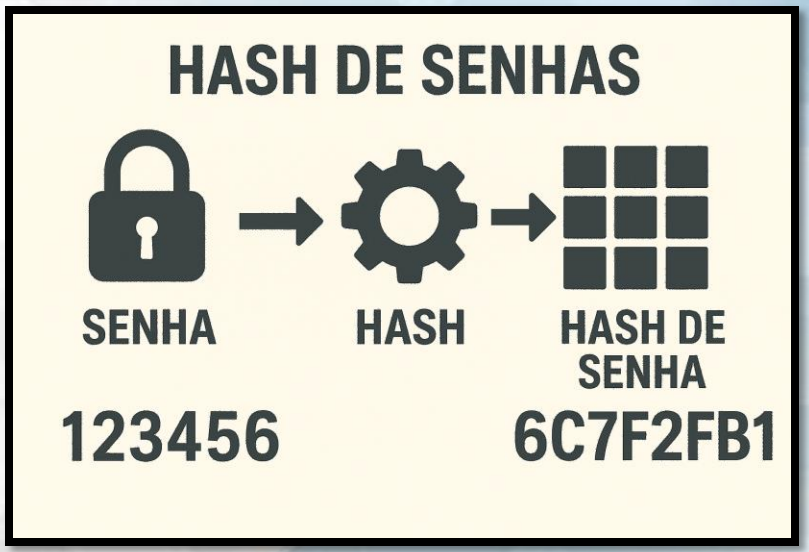
Segurança de Dispositivos Pessoais

- Bloqueio do SIM (senha no chip)

Senhas fortes: hashes desconhecidos

- A Função Hash

- Ataque de força bruta
- Ataque de Dicionário
- Ataque de Rainbow Tables
- Phishing e Engenharia Social
- Vazamento de dados
- Credential Stuffing



RecrutaTech

https://**bit.ly/recrutatech2025**

Segurança de Dispositivos Pessoais

- Ataques IoT

- S3nh4$Mu1t0F0rt3$ (cofre de senhas)
- Manter os sistemas atualizados
- Usar salt
- Usar autenticação multifator: MFA
- Educar usuários

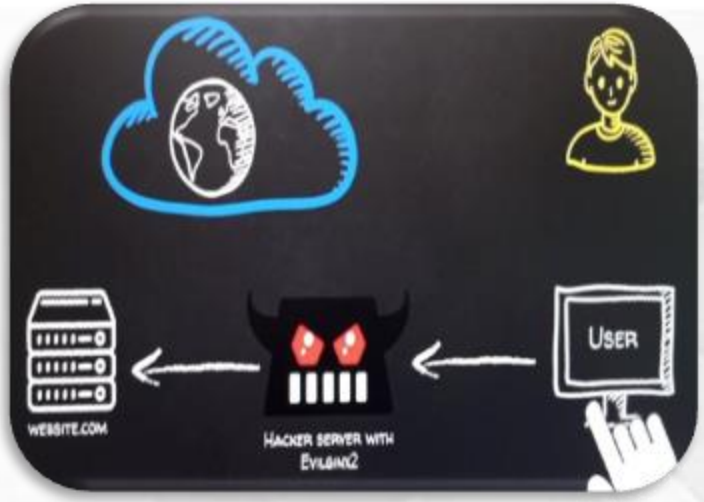
- Ferramentas: shodan.io, L0pthcrack, crackstation.net , john, aircrack

RecrutaTech

https://**bit.ly/recrutatech2025**

Bypass de MFA com Evilginx

Real	Homoglyph
facebook.com	facebook.com
twitter.com	twitter.com
microsoft.com	microsoft.com
amazon.com	amazon.com




```
 id           : 1
 phishlet     : github
 username     : z00z
 password     : M^K)j~5xuDVLkq@{"\`
 tokens       : captured
 landing url  : https://zshacks.com/github
 user-agent   : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, li
) Chrome/107.0.0.0 Safari/537.36
 remote ip    : 37.228.253.233
 create time  : 2022-11-30 19:09
 update time  : 2022-11-30 19:12

[{"path":"/","domain":"github.com","expirationDate":1701371624,"value":"z00z","name":"dotcom_
ttpOnly":true},{"path":"/","domain":"github.com","expirationDate":1701371624,"value":"yes","n
gged_in","httpOnly":true},{"path":"/","domain":"github.com","expirationDate":1701371624,"valu
a7JGrMpJSTayKddqF2DJ2RXkrIou8umarxGKv01ZN5a3vptOdyuFx9jRzwKt4AutdB6sxVswDB2PeRhjC7bX0aoiQgERR
f34%2BEs2aftjFSh3qfyH%2F39zDFvS%2FUrnelf5S4UUlGgQsOVjBAahRLD302gVyjwza4B9%2Fyqh%2FaHI8tR%2BbB
OGAoUkJ7TgvQarKYFE8t4yLGlgEkkRdim6G6tF9PHzyVnD%2FSqxSFyIRZMUeZYGNR4ecdt8YwoCiSGRQUtHvoHjqJyja
3fOcEdkJbn48X8xMdliHQtcyWRnkGkVj7kyC0Z9qDHwoKnKjIJQRUl7jkjoF3BpgjKjuLYXqnnY8zcgcCuc4sx6LxX0%2
2BlpKHipwbpgy2UgrZWvmpBqJwG%2FN8P90n99hYsQu7%2BFkVLKwYy8aiap6z4Wcy1dJjKl1DZau%2FwslyWz%2F5vCU
0XvPiLZZUBhIEOuSHW6O23lEF8cftimQGBIGphMKOklzt2fVspnnKKITоJkgcHfPhkZeKtAPT1WvLZ0ocQYYBUNCtFMnX
1OG0%2BMCSvKciumn8vGliwyeSn5KLrubuUQZ8QecUptxLWQMrLKb9x5SdtWc7pZIcXqVop4hCykSmdz3ykMYNI2PyuQh
F5rju1eo0vGOTidNM7Qc8SuHr542YUYrjz4EHCLaBUxMVenLKqSHGvcLk81tKZjbW1hktDUPi4cPprdYtTxo%3D--0W6O
fun3--0VoqdWOkK2WShR0dUkxr4g%3D%3D","name":"_gh_sess","httpOnly":true,"hostOnly":true},{"path"
```

RecrutaTech

https://**bit.ly/recrutatech2025**

Segurança de Informações Pessoais

- Cuidado com a confiança.
- Dados podem vazar. Cópias infinitas.
- Internet não tem delete.
- WiFi: Canal público.
- VPN: reduzindo riscos em redes públicas
- TOR
- Criptografia de dispositivos
- Descarte de discos, documentos e dispositivos de forma segura (placas tesla)

- Ferramentas: WiFi Analyzer, WireShark, VPN, pesquisa reversa de imagens, OSINT Framework, Registrato BACEN

RecrutaTech

https://**bit.ly/recrutatech2025**

Como os Sistemas São Invadidos?

- Sistemas inseguros podem ser acessados sem que o usuário perceba
- Sistemas seguros podem ser acessados induzindo usuários a executar ações
- Gatilhos mentais (Urgência, Escassez, Autoridade, Intimidação, Confiança, Reciprocidade, Curiosidade, Prova social, Familiaridade, Recompensa, Ganância)
- Frameworks ataque: Metasploit, Cobalt Strike, Brute Ratel, Havoc
- Ferramentas: Antivírus, virustotal.com, Netcraft Anti Phishing Toolbar, Nessus Essentials

RecrutaTech

bit.ly/recrutatech2025

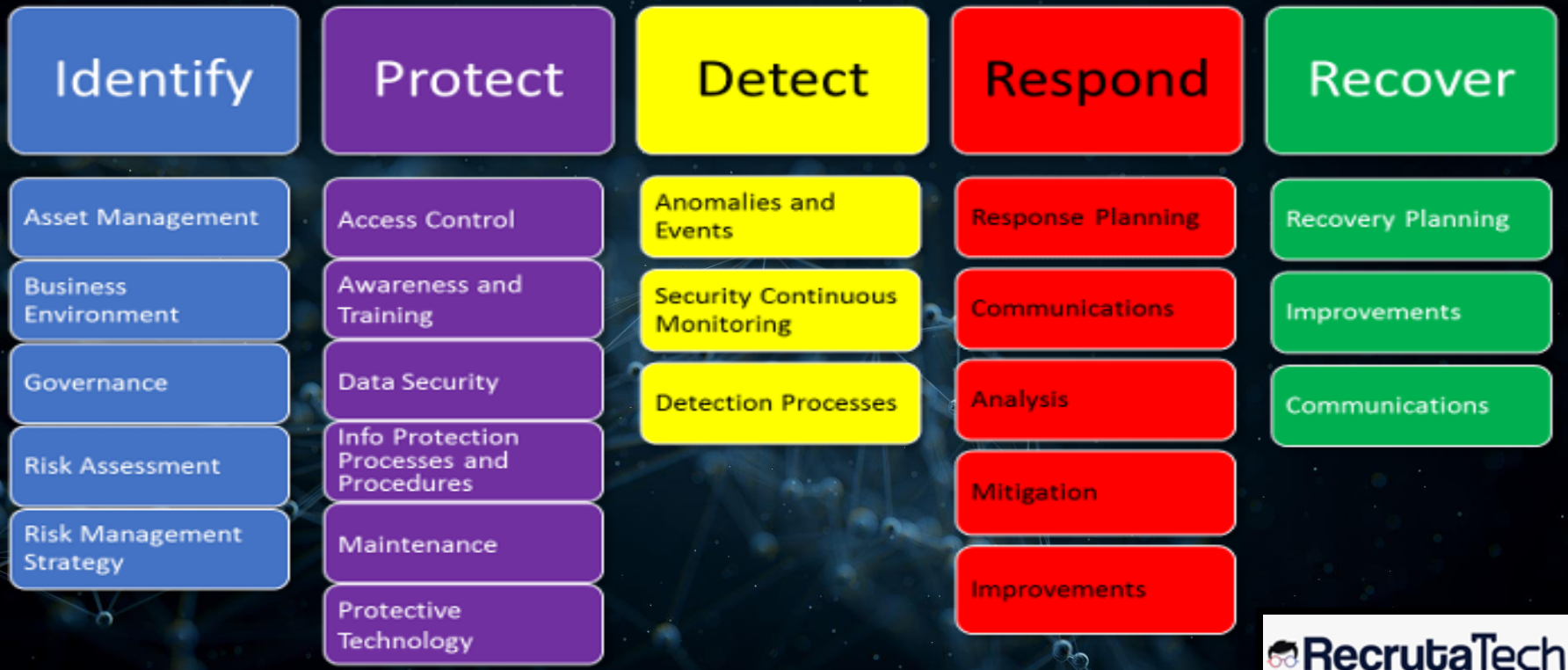
Frameworks de Cibersegurança

- Nist (National Institute of Standards and Technology)
- ISO/IEC 27001 - Padrão internacional para Sistemas de Gestão de Segurança da Informação
- CIS Controls – 18 controles de segurança focados em práticas contra ameaças comuns.
- Mitre Att&ck – Base de conhecimento de táticas e técnicas
- Específicos: Saúde (HIPAA), Finanças (PCI-DSS)

RecrutaTech

bit.ly/recrutatech2025

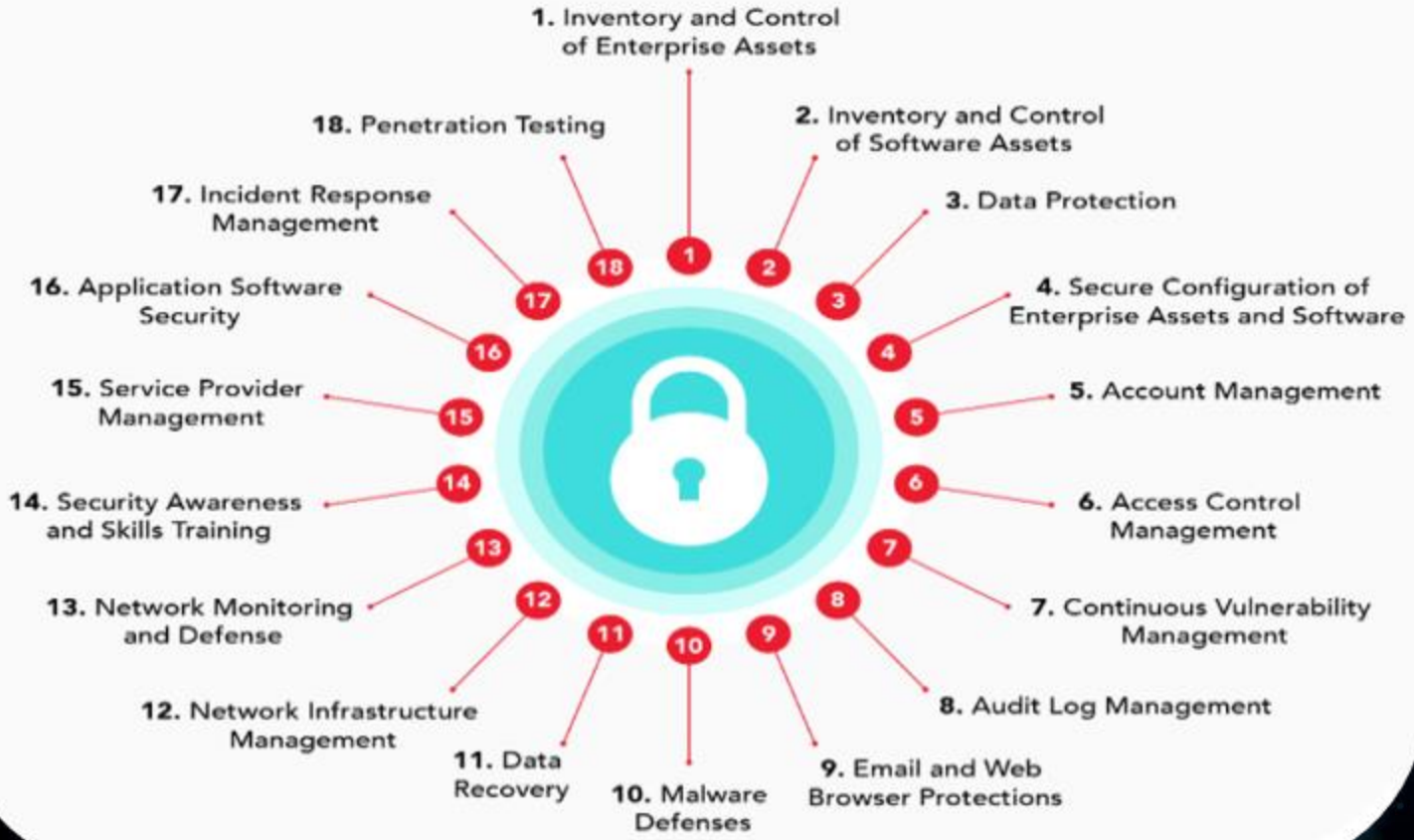
NIST Cyber Security Framework



RecrutaTech

bit.ly/recrutatech202

THE 18 CIS CONTROLS



bit.ly/recrutatech202

RecrutaTech

CONTROLE 01

Inventário e controle de ativos corporativos

SAFEGUARDS TOTAL	IG1	IG2	IG3
5	2/5	4/5	5/5

Visão geral

Gestão ativa (inventariar, rastrear e corrigir) de todos os ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais; Internet das Coisas (IoT); e servidores) conectados fisicamente à infraestrutura, virtualmente, remotamente, e aqueles em ambientes de nuvem, para saber com precisão a totalidade dos ativos que precisam ser monitorados e protegidos dentro da empresa. Isso também ajudará na identificação de ativos não autorizados e não gerenciados para removê-los ou remediá-los.

CONTROLE 02

Inventário e controle de ativos de software

SAFEGUARDS TOTAL	IG1	IG2	IG3
7	3/7	6/7	7/7

Visão geral

Gestão ativa (inventariar, rastrear e corrigir) de todos os softwares (sistemas operacionais e aplicações) na rede para que apenas o software autorizado seja instalado e possa ser executado, e que o software não autorizado e não gerenciado seja encontrado e impedido de ser instalado ou executado.

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
Inventário e controle de ativos corporativos						
	Gestão ativa (inventariar, rastrear e corrigir) de todos os ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais; Internet das Coisas (IoT); e servidores) conectados fisicamente à infraestrutura, virtualmente, remotamente, e aqueles em ambientes de nuvem, para saber com precisão a totalidade dos ativos que precisam ser monitorados e protegidos dentro da empresa. Isso também ajudará na identificação de ativos não autorizados e não gerenciados para removê-los ou remediá-los.					
1.1	**Estabelecer e manter um inventário detalhado de ativos corporativos**	Dispositivo	Identificar	●	●	●
	Estabeleça e mantenha um inventário preciso, detalhado e atualizado de todos os ativos corporativos com potencial para armazenar ou processar dados, incluindo: dispositivos de usuário final (incluindo portáteis e móveis), dispositivos de rede, dispositivos não computacionais/IoT e servidores. Certifique-se de que o inventário registre o endereço de rede (se estático), endereço de hardware, nome da máquina, proprietário do ativo de dados, departamento para cada ativo e se o ativo foi aprovado para se conectar à rede. Para dispositivos móveis de usuário final, as ferramentas do tipo MDM podem oferecer suporte a esse processo, quando apropriado. Este inventário inclui ativos conectados à infraestrutura fisicamente, virtualmente, remotamente e aqueles dentro dos ambientes de nuvem. Além disso, inclui ativos que são regularmente conectados à infraestrutura de rede corporativa, mesmo que não estejam sob o controle da empresa. Revise e atualize o inventário de todos os ativos corporativos semestralmente ou com mais frequência.					
1.2	**Endereçar ativos não autorizados**	Dispositivo	Responder	●	●	●
	Assegure que exista um processo para lidar com ativos não autorizados semanalmente. A empresa pode escolher remover o ativo da rede, negar que o ativo se conecte remotamente à rede ou colocar o ativo em quarentena.					
1.3	**Usar uma ferramenta de descoberta ativa**	Dispositivo	Detectar		●	●
	Utilize uma ferramenta de descoberta ativa para identificar ativos conectados à rede corporativa. Configure a ferramenta de descoberta ativa para executar diariamente ou com mais frequência.					
1.4	**Usar o Dynamic Host Configuration Protocol (DHCP) para atualizar o inventário de ativos corporativos**	Dispositivo	Identificar		●	●
	Use o log do DHCP em todos os servidores DHCP ou ferramentas de gestão de endereço Internet Protocol (IP) para atualizar o inventário de ativos corporativos. Revise e use logs para atualizar o inventário de ativos corporativos semanalmente ou com mais frequência.					
1.5	**Usar uma ferramenta de descoberta passiva**	Dispositivo	Detectar			●
	Use uma ferramenta de descoberta passiva para identificar ativos conectados à rede corporativa. Revise e use varreduras para atualizar o inventário de ativos corporativos pelo menos semanalmente ou com mais frequência.					

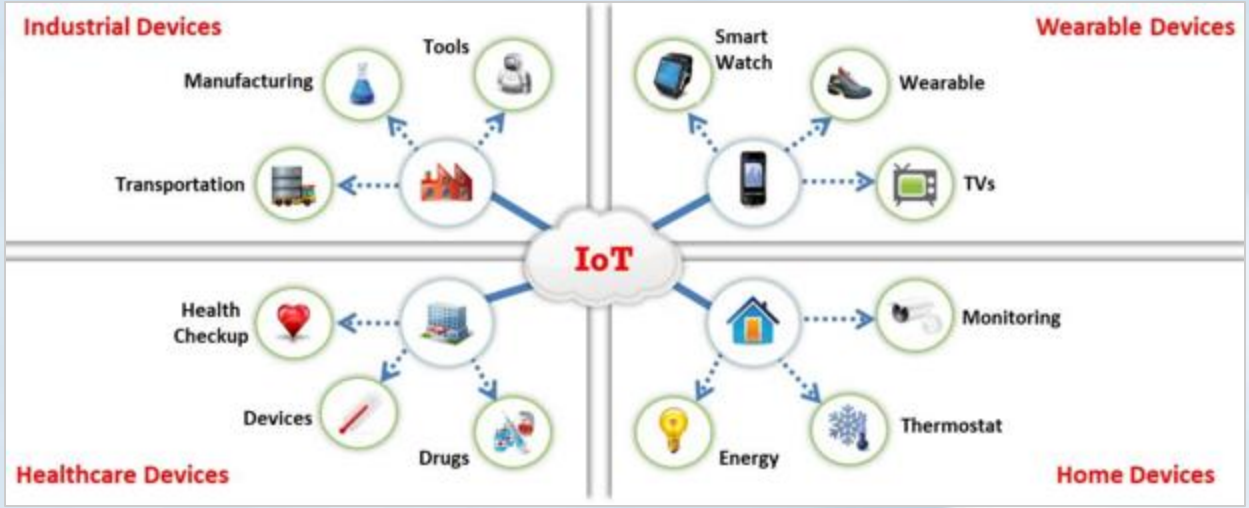
bit.ly/recrutatech202

RecrutaTech

IoT / IoE

- Construção
- Indústria
- Energia
- Transporte
- Infraestrutura
- Saúde
- Casa
- Segurança
- Redes
- Assistentes digitais

- Quantidade massiva de dados. Big data
- Machine to machine
- Stuxnet, celulares no carrinho de mão



Ferramenta: Cisco Packet Tracer, Shodan.io
OWASP Internet of Things Project - OWASP

RecrutaTech

bit.ly/recrutatech202

Cibersegurança

- Estratégico: mundo digital
- Necessário: estamos preparados para o ataque?
- A melhor defesa é o conhecimento e preparação.

- Monitorar ameaças em tempo real
- Capacitar a equipe contra ameaças

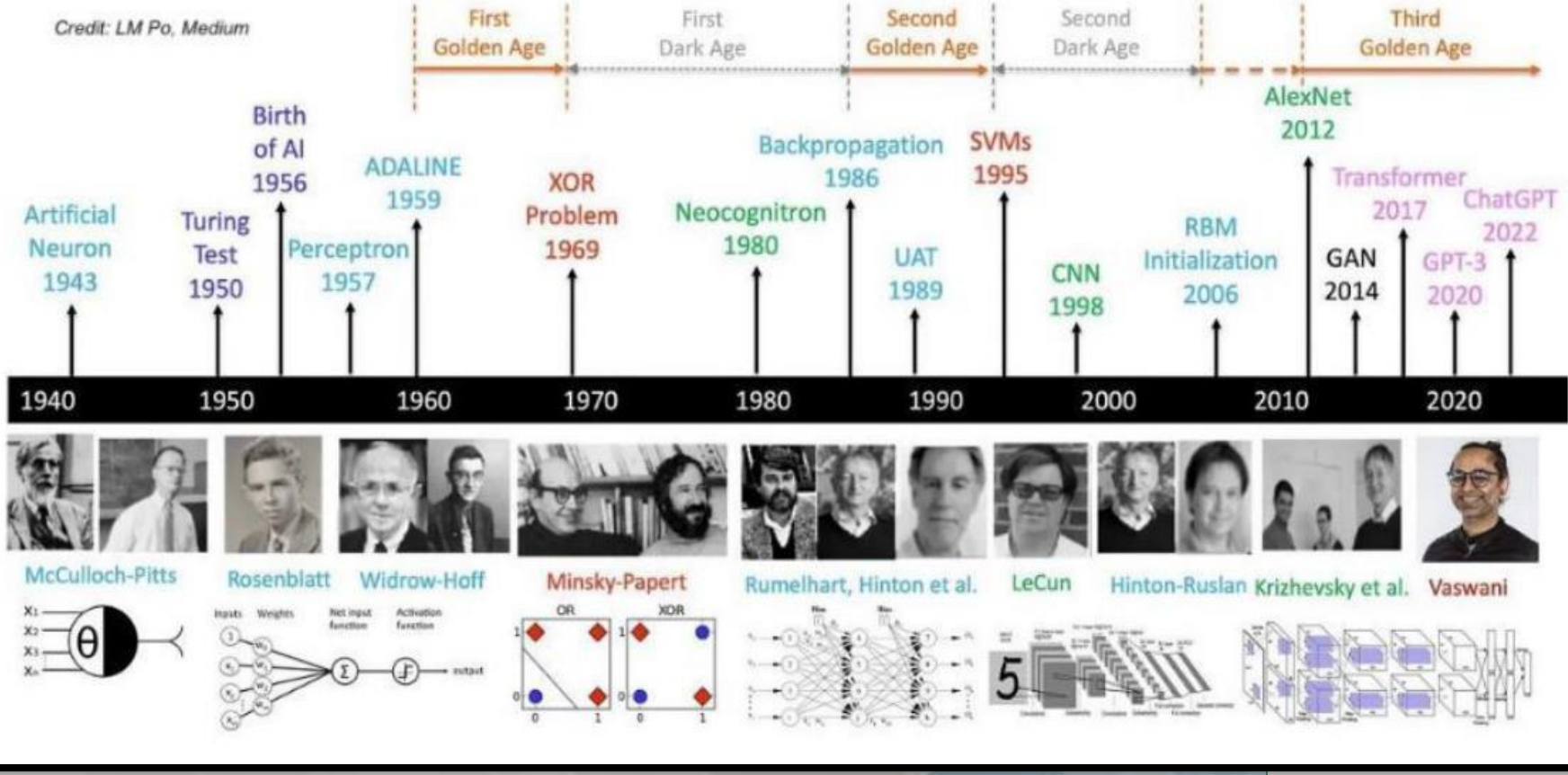
- Adotar soluções robustas
- A segurança não é um produto, mas um processo.

- A próxima parte da história será escrita com IA, que está sendo utilizada para defesa e para o ataque.

RecrutaTech

bit.ly/recrutatech2025

A Brief History of AI with Deep Learning



https://**bit.ly/recrutatech2025**

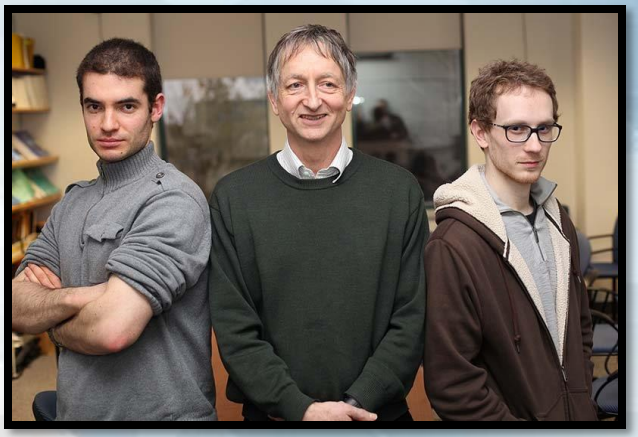
RecrutaTech

Inteligência Artificial

- ImageNet Large Scale Visual Recognition Challenge de 2012 (ILSVRC)
- AlexNet: Machine Learning
- Redes neurais convolucionais profundas (CNNs, deep learning) treinadas em 2 GPUs

- Veículos autônomos

- Insight: notebooks antigos que ganham nova vida

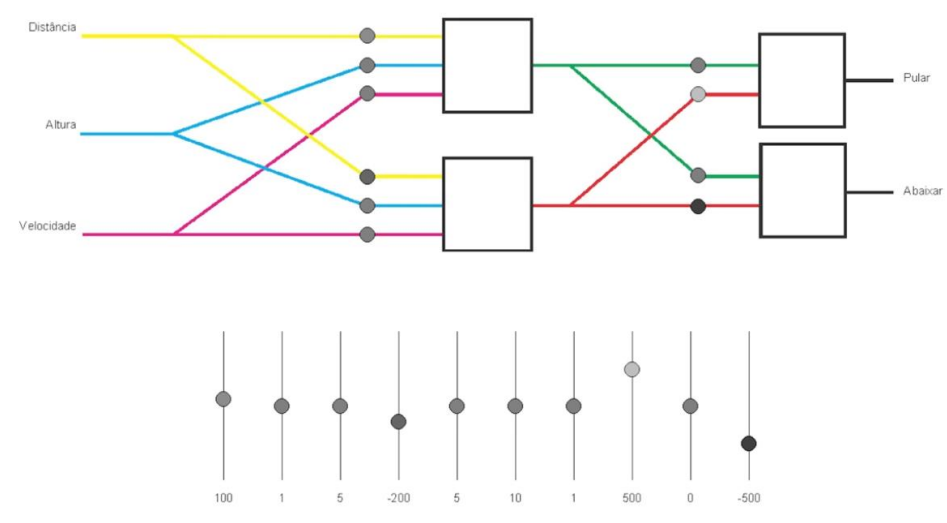


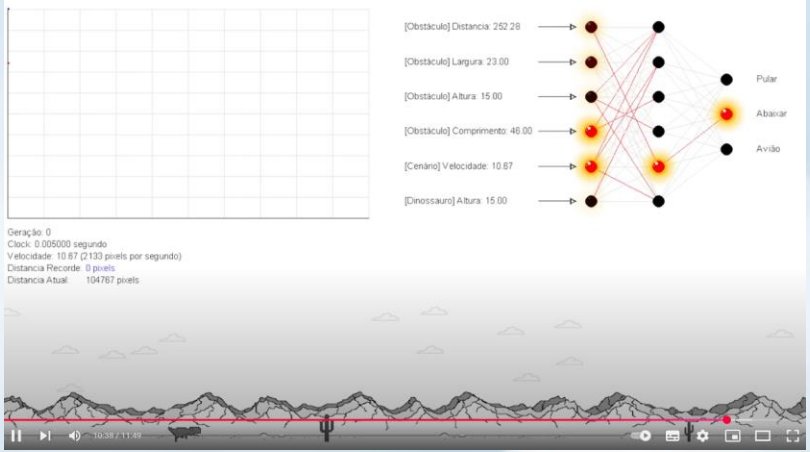
Geoffrey Hinton, Alex Krizhevsky e Ilya Sutskever

RecrutaTech

bit.ly/recrutatech2025

Redes Neurais





https://www.youtube.com/watch?v=NZlIYr1slAk

https://bit.ly/redesneuraisdinossauro

https://**bit.ly/recrutatech2025**

RecrutaTech

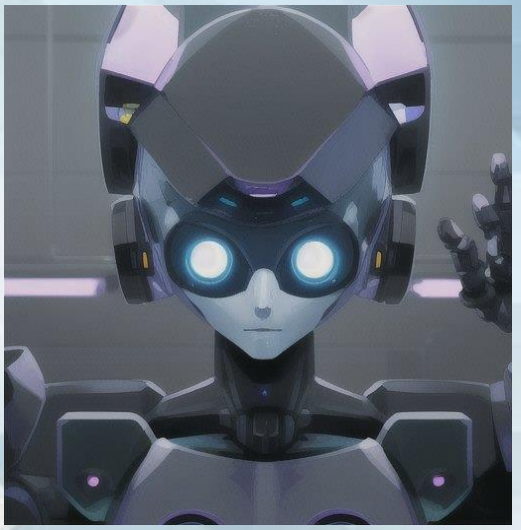
Online

- ChatGPT.com (OpenAI)
- Google AI Studio, Gemini (Google)
- Grok (xAI)

- Copilot (Microsoft)

- NotebookLM: podcast personalizado instantâneo.

- Poderosos, mas privados?



RecrutaTech

bit.ly/recrutatech2025

Offline

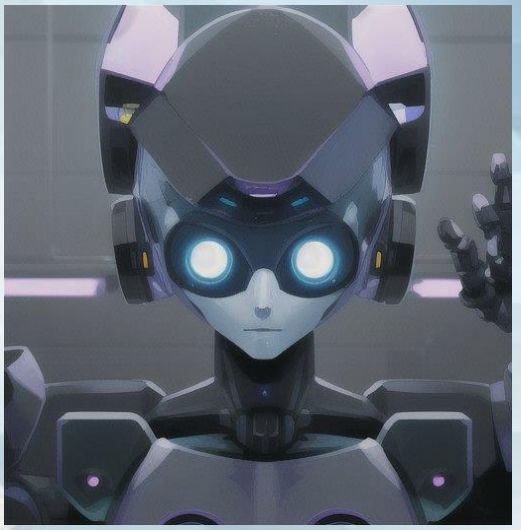
- Ollama
- LM Studio

- Codificação: VS-Code com a extensão Continue

- Criação de Imagens: Easy Diffusion (Stable Diffusion com instalador)

- Modelos disponíveis: CivitAI e HuggingFace

- Poder menor, privacidade maior.
- Possibilidades de personalização.
- PrivateGPT (RAG)
- ChatRTX da Nvidia



RecrutaTech

bit.ly/recrutatech2025

https://civitai.com/models

CIVITAI Pro

Create

Checkpoint | IL

Crody

Nova Furry XL

14.5K 328 29 60 1.6K

Embedding | IL

LAZY EMBEDDINGS

✨ Lazy Embeddings for ALL illustrious NoobAI Pony SDXL models LazyPositive...

29.2K 347 9 0 1.5K

LoRA | IL

VelvetS

Velvet's Mythic Fantasy Styles | Flux + Pony + illustrious

15.1K 495 10 3.3K 1.4K

LoRA | NAI

reakaakasky

Stabilizer IL/NAI

13.8K 363 19 1.1K 1.3K

https://huggingface.co

Transformers
148,566
State-of-the-art AI models for PyTorch

Diffusers
30,388
State-of-the-art Diffusion models in PyTorch

Safetensors
3,407
Safe way to store/distribute neural network weights

Hub Python Library
2,856
Python client to interact with the Hugging Face Hub

Tokenizers
10,005
Fast tokenizers optimized for research & production

TRL
15,177
Train transformers LMs with reinforcement learning

Transformers.js
14,377
State-of-the-art ML running directly in your browser

smolagents
22,244
Smol library to build great agents in Python

PEFT
19,360
Parameter-efficient finetuning for large language models

Datasets
20,530

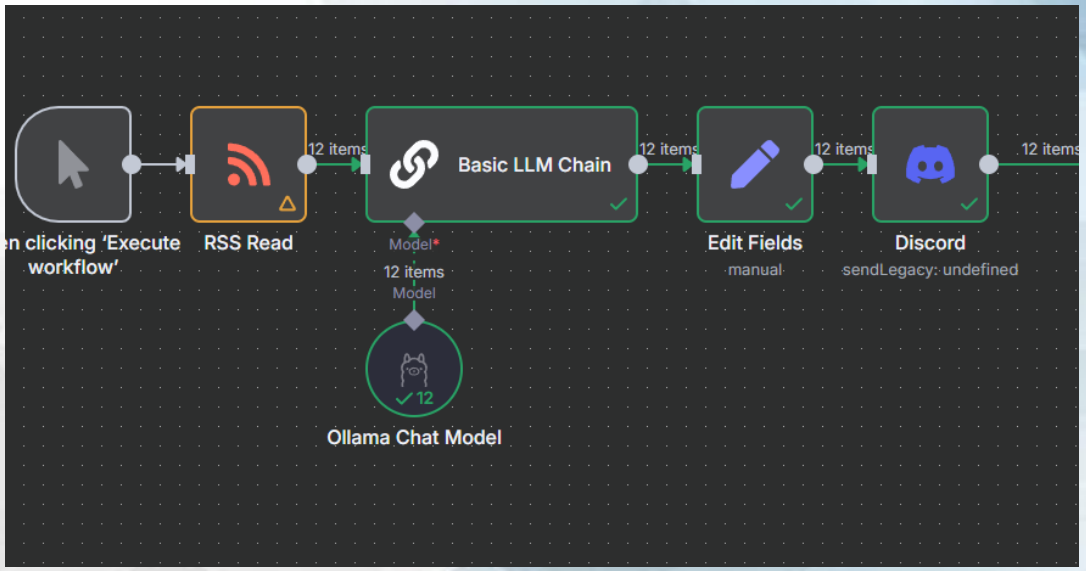
Text Generation Inference
10,435
Serve language models with TGI optimized

Accelerate
9,056
Train PyTorch models with

RecrutaTech

Automação

- N8N
- Infinitas possibilidades
- Pega um feed de notícias, cria um resumo com a IA localmente e envia pro canal do discord



bit.ly/recrutatech2025

RecrutaTech

Inteligência Artificial na Cibersegurança

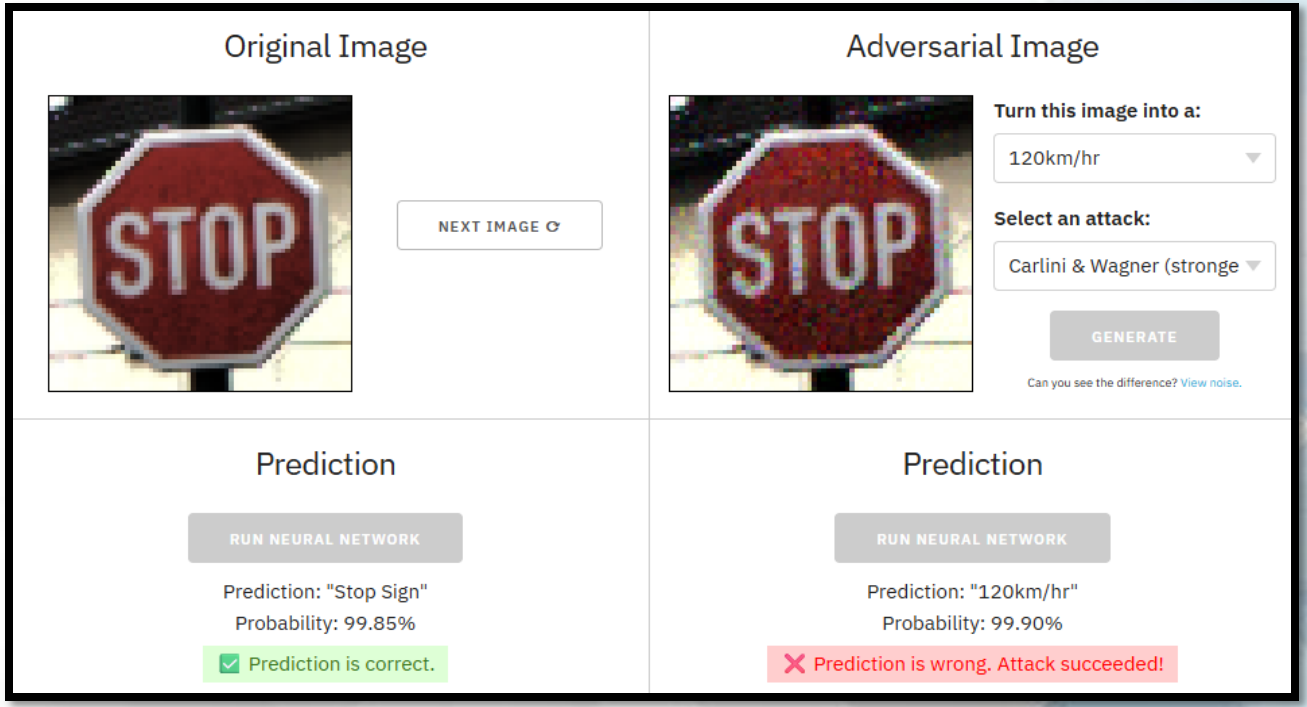
- Microsoft Sentinel – Motor de dados - SIEM (Security Information and Event Management) e SOAR (Security Orchestration, Automation and Response) baseada na nuvem
- Microsoft Cybersecurity Copilot - Um assistente de segurança baseado em IA generativa, projetado para ajudar analistas a entender, investigar e responder a ameaças com mais rapidez.
- Greylog e n8n
- Atacantes conseguem auxílio no desenvolvimento de estratégias, criação de emails de phishing e execução de planos de ataque.

RecrutaTech

bit.ly/recrutatech2025

Hacking IA

- https://kennysong.github.io/adversarial.js/



Adversarial examples para quase todas as tarefas de aprendizado de máquina:

- Reconhecimento de fala
- Classificação de texto
- Detecção de fraudes
- Tradução automática
- Reinforcement learning
- ...

RecrutaTech

bit.ly/recrutatech202

jason
@singingpigs.online
+ Follow

my wife googled "united airlines customer service" the other day and the AI summary seemed legit enough so she called the number that it listed. she got like 30 seconds into the call before they were asking for her BANK INFO. a scammer had gotten their number prominent enough that the AI grabbed it.

October 9, 2024 at 2:09 PM Everybody can reply

RL Blog

Threat Research | February 6, 2025

Malicious ML models discovered on Hugging Face platform

Software development teams working on machine learning take note: RL threat researchers have identified nullifAI, a novel attack technique used on Hugging Face.

BLOG AUTHOR
Karlo Zanki, Reverse Engineer at ReversingLabs. READ MORE...

https://**bit.ly/recrutatech2025**

RecrutaTech

O Futuro

- Ray Kurzweil: a singularidade. "Imortalidade".
- Em 2030 a IA estará conectada conosco.
- DNA e informação: biotecnologia
- Em 2045 o mundo terá mudado pra sempre.
- AGI.
- Desafios, oportunidades e riscos.

bit.ly/recrutatech2025

RecrutaTech

Carreira no Século XXI

- Ikigai
- Cooperação Solidária
- Pensamento crítico
- Confiança
- Atitude
- Ser autêntico
- Ser útil
- Fazer falta

RecrutaTech

bit.ly/recrutatech2025

Consciência e Atitude

- "Não há nada encoberto que não venha a ser revelado, nem oculto que não venha a ser conhecido. Porque tudo o que vocês disseram às escuras será ouvido em plena luz; e o que disseram ao pé do ouvido no interior da casa será proclamado dos telhados." Lucas 12:2-3

- "Com grandes poderes vem grandes responsabilidades." Tio Ben para Peter Parker.

RecrutaTech

bit.ly/recrutatech2025

Obrigado!

me adicione no linkedin, instagram,
me mande um email!

@gazstao - gazstao@gmail.com

aztechtecnologia.com.br

https://**bit.ly/recrutatech2025**

RecrutaTech