IA e Cibersegurança

FEBRABAN
/CYBER LAB

Laboratório de Segurança Cibernética - 20/03/2025

TLP:AMBER

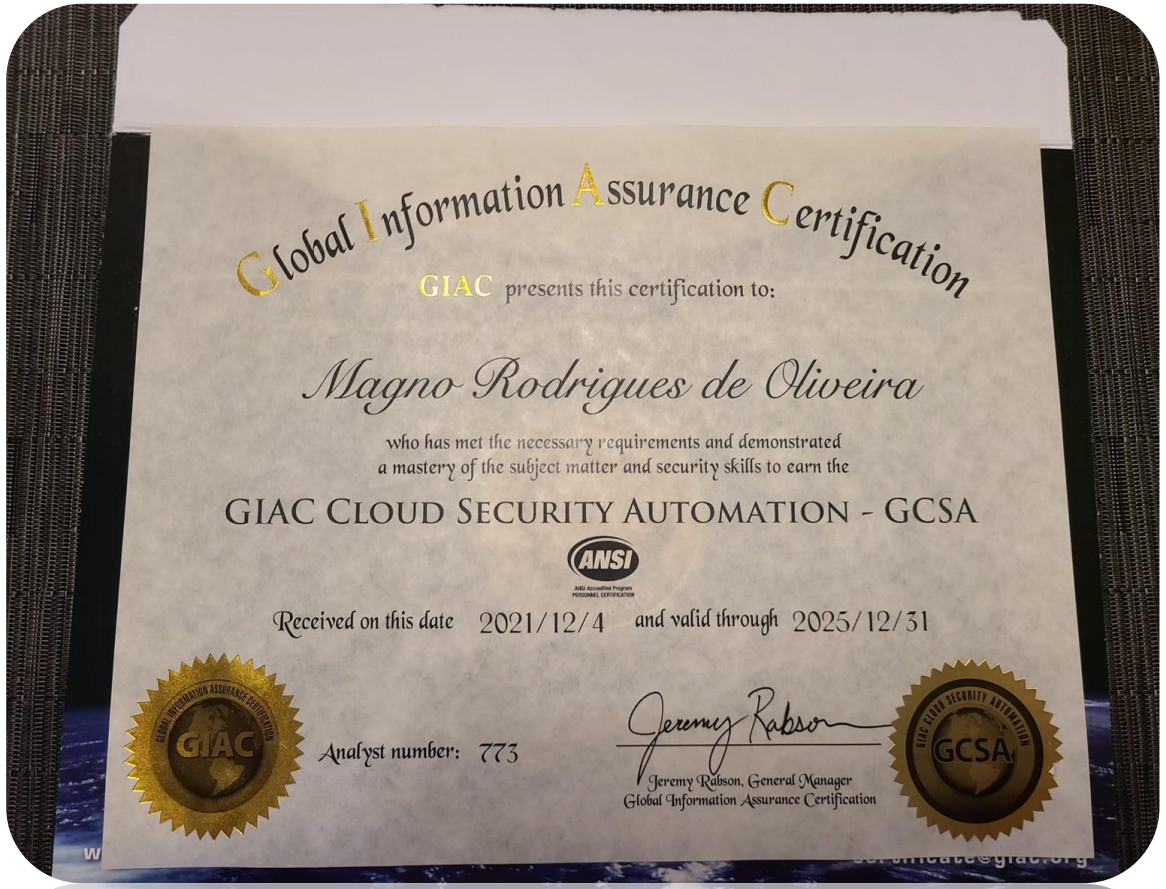
Traffic Light Protocol (TLP) Amber: Divulgação limitada aos participantes da organização. Destinatários podem compartilhar essas informações apenas com membros da própria organização que necessitem saber o conteúdo para tomada de ações cabíveis

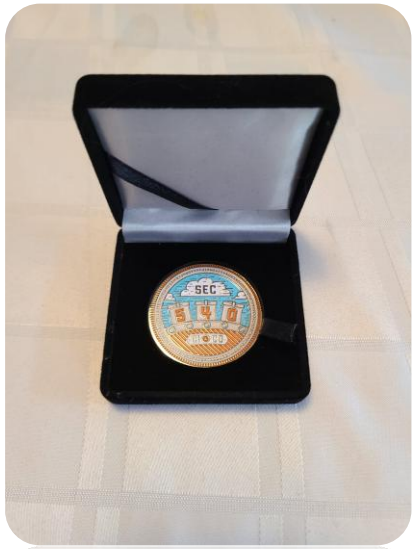
Magno Logan – Instrutor GoHacking

FEBRABAN / CYBER LAB

- Especialista em Segurança da Informação, atuando no Canadá, liderando o programa de Security Champions
- Background em desenvolvimento com +15 anos de XP com AppSec, DevSecOps, Containers e K8s
- Implantou diversas ferramentas de AppSec em pequenas e grandes empresas (SAST, DAST, SCA, Secret Scanning)
- Possui diversas certificações da SANS, CompTIA, EC-Council AWS, Microsoft e EXIN
- Palestrante em diversas conferências internacionais como DEFCON, OWASP AppSec, NorthSec, H2HC, KubeCon, etc.

Magno Logan – Instrutor GoHacking





Agenda

1. Conceitos e definições
2. Principias áreas da IA
3. Aplicações práticas de IA
4. IA na atualidade (LLM)
5. IA e Segurança Cibernética

Introdução a Inteligência Artificial - Conceitos e Definições

FEBRABAN
/CYBER LAB

O que é Inteligência Artificial?

FEBRABAN
/CYBER LAB

Conceito Básico

Inteligência Artificial é o campo da ciência da computação que cria sistemas capazes de simular a inteligência humana – como por exemplo:

- Aprender com a experiência
- Compreender linguagem natural
- Tomar decisões
- Resolver problemas
- Reconhecer padrões e imagens

O que é Inteligência Artificial?

FEBRABAN
/CYBER LAB

IA != Magia

- IA não “pensa” como um ser humano. Ela usa **matemática, estatística e dados** para encontrar padrões e tomar decisões baseadas em algoritmos.

Exemplos:

- Assistentes de voz (Siri, Alexa)
- Recomendações da Netflix ou Spotify

Linha do Tempo da Inteligência Artificial

FEBRABAN
CYBER LAB

Ano	Marco	Descrição
1950	Teste de Turing	Alan Turing propõe um teste para avaliar se uma máquina pode imitar o comportamento humano.
1956	Nascimento oficial da IA	Conferência de Dartmouth: o termo "Inteligência Artificial" é usado pela primeira vez por John McCarthy.
1960s	Surgem os primeiros sistemas especialistas	Programas que tomavam decisões baseadas em regras fixas, usados em medicina e engenharia.
1980s	Boom dos sistemas especialistas	IA volta a ganhar popularidade com uso corporativo, mas limitada pela capacidade dos computadores.

Linha do Tempo da Inteligência Artificial

FEBRABAN CYBER LAB

Ano	Marco	Descrição
1997	Deep Blue vence Kasparov	Computador da IBM derrota o campeão mundial de xadrez – marco importante de IA simbólica.
2012	Revolução do Deep Learning	Algoritmos de redes neurais profundas conseguem reconhecer imagens com precisão superior à humana.
2016	AlphaGo vence campeão mundial de Go	IA da DeepMind derrota Lee Sedol, em um jogo considerado mais complexo que o xadrez.
2020s	Explosão dos Modelos de Linguagem (LLMs)	Modelos como GPT-3, ChatGPT, Claude e Gemini tornam-se amplamente utilizados por empresas e usuários comuns.

Principias áreas da IA

FEBRABAN
/CYBER LAB

Principais Áreas da IA

FEBRABAN
/CYBER LAB

- **Aprendizado de Máquina (Machine Learning):** Algoritmos que aprendem com dados
- **Processamento de Linguagem Natural (NLP):** Interação entre máquinas e linguagem humana
- **Visão Computacional:** Análise de imagens e vídeos
- **Robótica:** Máquinas que executam ações no mundo físico
- **Sistemas Especialistas:** Sistemas com conhecimento específico para tomada de decisão

Aprendizado de Máquina

FEBRABAN
/CYBER LAB

O que é:

É a área da IA que ensina máquinas a aprender a partir de dados. Em vez de serem programadas com regras fixas, elas **identificam padrões e tomam decisões sozinhas** com base nos dados que recebem.

Exemplos práticos:

- **Bancos:** Identificação de transações suspeitas (fraude)
- **Netflix / YouTube:** Sugestões personalizadas com base no que você assistiu
- **E-commerce:** Recomendação de produtos semelhantes
- **Cibersegurança:** Detecção de ameaças por comportamento anormal (UEBA)

Processamento de Linguagem Natural (NLP)

FEBRABAN
/CYBER LAB

O que é:

Permite que computadores entendam, interpretem, gerem e respondam à **linguagem humana (escrita ou falada)** de forma natural.

Exemplos práticos:

- **Assistentes virtuais:** Alexa, Siri, Google Assistant
- **Chatbots em sites:** Atendimento automatizado
- **Tradução automática:** Google Tradutor, DeepL
- **Análise de sentimentos:** Descobrir se um comentário nas redes é positivo ou negativo
- **Ferramentas de IA como ChatGPT**

Visão Computacional

FEBRABAN
/CYBER LAB

O que é:

Capacita máquinas a "ver", interpretar e entender o **conteúdo de imagens e vídeos**, como se fosse a visão humana.

Exemplos práticos:

- **Reconhecimento facial:** Desbloqueio de celulares, segurança em aeroportos
- **Câmeras inteligentes:** Identificação de placas de veículos (OCR)
- **Diagnósticos médicos:** IA que detecta tumores em exames de imagem
- **Indústria:** Controle de qualidade em fábricas (detecção de defeitos em produtos)

Robótica

FEBRABAN
/CYBER LAB

O que é:

Combina IA com engenharia para criar **máquinas físicas capazes de executar tarefas automatizadas**, muitas vezes com autonomia e adaptabilidade.

Exemplos práticos:

- **Robôs em linhas de montagem:** Montagem de carros
- **Robôs aspiradores (Roomba):** Navegam pela casa sozinhos
- **Drones autônomos:** Entregas ou mapeamentos em áreas de risco
- **Robôs hospitalares:** Entregam medicamentos e coletam amostras em hospitais

Sistemas Especialistas

FEBRABAN
CYBER LAB

O que é:

São sistemas que simulam o conhecimento de um **especialista humano em uma área específica**, utilizando regras e bancos de conhecimento.

Exemplos práticos:

- **Diagnóstico médico automatizado:** Baseado em sintomas e histórico
- **Sistemas jurídicos:** Auxiliam juízes e advogados em pareceres técnicos
- **Suporte técnico automatizado:** Diagnóstico de falhas em máquinas ou sistemas
- **Ferramentas de compliance:** Avaliam risco de transações financeiras ou contratos

Principais Áreas da IA e Exemplos

FEBRABAN
CYBER LAB

Área	Exemplo do Dia a Dia
Machine Learning	Recomendação da Netflix
NLP	ChatGPT ou Google Tradutor
Visão Computacional	Câmera de reconhecimento facial
Robótica	Robô aspirador ou drone de entrega
Sistemas Especialistas	Diagnóstico médico por IA

Aplicações práticas de IA

FEBRABAN
/CYBER LAB

Aplicações práticas de IA

FEBRABAN
/CYBER LAB

Segurança da Informação:

- A IA ajuda a **detectar, prever e responder a ameaças digitais** com muito mais velocidade e precisão do que um humano conseguiria sozinho
- Detecção de Ameaças em Tempo Real
- Análise de Comportamento (UEBA – User and Entity Behavior Analytics)
- Resposta Automatizada a Incidentes (SOAR)
- Antivírus com IA

Aplicações práticas de IA

FEBRABAN
/CYBER LAB

Saúde:

A IA está revolucionando a **prevenção, diagnóstico e tratamento de doenças**, apoiando profissionais de saúde e melhorando o atendimento ao paciente

- Diagnóstico assistido por IA
- Chatbots Médicos
- Análise Genética e Medicina Personalizada
- Previsão de Epidemias

Aplicações práticas de IA

FEBRABAN
/CYBER LAB

Transporte:

A IA está no centro da **transformação do setor de mobilidade**, tornando os deslocamentos mais inteligentes, seguros e eficientes

- Carros autônomos
- Previsão de rotas e tráfego
- Manutenção Preditiva em Frotas
- Sistemas de Transporte Público Inteligente

Aplicações práticas de IA

FEBRABAN
/CYBER LAB

Serviços ao Cliente:

IA melhora a **experiência do consumidor** ao automatizar atendimentos, personalizar interações e acelerar o tempo de resposta

- Chatbots e Assistentes Virtuais
- Recomendações Personalizadas
- Análise de Sentimento
- Atendimento com Voz Natural

IA na atualidade (LLMs)

FEBRABAN
/CYBER LAB

IA na atualidade (LLMs)

FEBRABAN
/CYBER LAB

O que são LLMs (Modelos de Linguagem de Grande Escala)?

LLMs, ou Large Language Models, são modelos de inteligência artificial treinados com enormes volumes de texto (livros, sites, artigos, fóruns) para entender e gerar linguagem humana com coerência, contexto e criatividade. Esses modelos são capazes de:

- Responder perguntas e simular conversas naturais
- Ajudar em programações e planejamentos
- Criar textos, resumos, e-mails, traduções
- Gerar código, arte, música

IA na atualidade (LLMs)

FEBRABAN
CYBER LAB

Como LLMs funcionam?

Treinamento com muitos textos:

- Os modelos leem bilhões de palavras da internet, livros e artigos para "aprender" o idioma, os padrões e a forma como as pessoas escrevem.

Previsão de palavras:

- O modelo não "pensa" como um humano. Ele prevê qual é a próxima palavra provável, dada a frase anterior. Exemplo:
- Entrada: "O céu está..."
- Resposta esperada: "azul" (porque é comum)

IA na atualidade (LLMs)

FEBRABAN
/CYBER LAB

Como LLMs funcionam?

Ajustes finos (Fine-tuning):

- Depois do treinamento geral, o modelo pode ser ajustado com dados específicos, como conversas de atendimento, códigos de programação ou informações médicas.

Feedback humano (RLHF – Reinforcement Learning with Human Feedback):

- Pessoas corrigem e avaliam respostas, ajudando o modelo a melhorar suas escolhas e evitar respostas incorretas ou perigosas.

Linha do Tempo dos LLMs

FEBRABAN
CYBER LAB

Ano	Descoberta	Descrição
2013	Word2Vec (Google)	Técnica que permite representar palavras como vetores — avanço crucial para o entendimento semântico.
2017	Transformer (Google)	Publicação do paper “Attention is All You Need” — nova arquitetura que revolucionou o processamento de linguagem.
2018	BERT (Google)	Modelo de linguagem com "atenção bidirecional", melhorando muito a compreensão de contexto.
2020	GPT-3 (OpenAI)	Primeiro LLM com grande impacto público: 175 bilhões de parâmetros.

Linha do Tempo dos LLMs

FEBRABAN
CYBER LAB

Ano	Descoberta	Descrição
2022	ChatGPT (OpenAI)	Lançamento com interface amigável — popularizou a IA no mundo.
2023	GPT-4, Claude, Bard (Gemini)	Modelos multimodais mais avançados e integrados com outras ferramentas (visão, som, programação).
2024–2025	LLMs especializados e abertos	Avanço dos modelos de código aberto (como Mistral e LLaMA 3), e integração com agentes autônomos.

Parâmentros em LLMs

FEBRABAN
/CYBER LAB

Modelo	Parâmetros Estimados
GPT-2	1,5 bilhões
GPT-3	175 bilhões
GPT-4	Estimado acima de 1 trilhão* (número oficial não revelado)
LLaMA 3	8B a 70B (modelo aberto da Meta)

IA e Segurança Cibernética

FEBRABAN
/CYBER LAB

IA e Segurança Cibernética

FEBRABAN
/CYBER LAB

Como a IA ajuda na segurança:

- Análise automatizada de logs
- Detecção de ataques em tempo real
- Redução de falsos positivos
- Previsão de ameaças (threat intelligence)

Ferramentas com IA usadas em cibersegurança:

- Darktrace, CrowdStrike, Microsoft Defender, SentinelOne

Principais riscos cibernéticos com IA

FEBRABAN
/CYBER LAB

Ataques com suporte de IA:

- Phishing automatizado mais convincente
- Deepfakes para fraude e manipulação
- Criação de malware com LLMs

Vazamento de dados:

- IA treinada com dados sensíveis inadvertidamente

Principais riscos cibernéticos com IA

FEBRABAN
CYBER LAB

Alucinações de IA:

- Geração de respostas falsas, mas convincentes

Uso indevido por atacantes:

- Ferramentas de pentest automatizadas sendo utilizadas por hackers

Desinformação e manipulação social:

- Propagação de fake news com IA em larga escala

Boas Práticas e Conscientização

FEBRABAN
/CYBER LAB

Boas Práticas e Conscientização

FEBRABAN
CYBER LAB

- Não compartilhe informações sensíveis com sistemas de IA públicos
- Use ferramentas confiáveis e com políticas de segurança claras
- Monitore o uso de IA nas organizações
- Mantenha-se informado sobre novas ameaças e regulamentações

Conclusão

FEBRABAN
/CYBER LAB

Conclusão

FEBRABAN
CYBER LAB

- IA está cada vez mais presente no nosso dia a dia
- É uma aliada poderosa na segurança, mas também traz novos riscos
- O conhecimento e a conscientização são as melhores defesas

"Com grandes poderes vêm grandes responsabilidades — inclusive na Inteligência Artificial."