



TREINANDO A INTELIGÊNCIA ARTIFICIAL DE SEGURANÇA

Pedro Bezerra

Consultor em Segurança da Informação

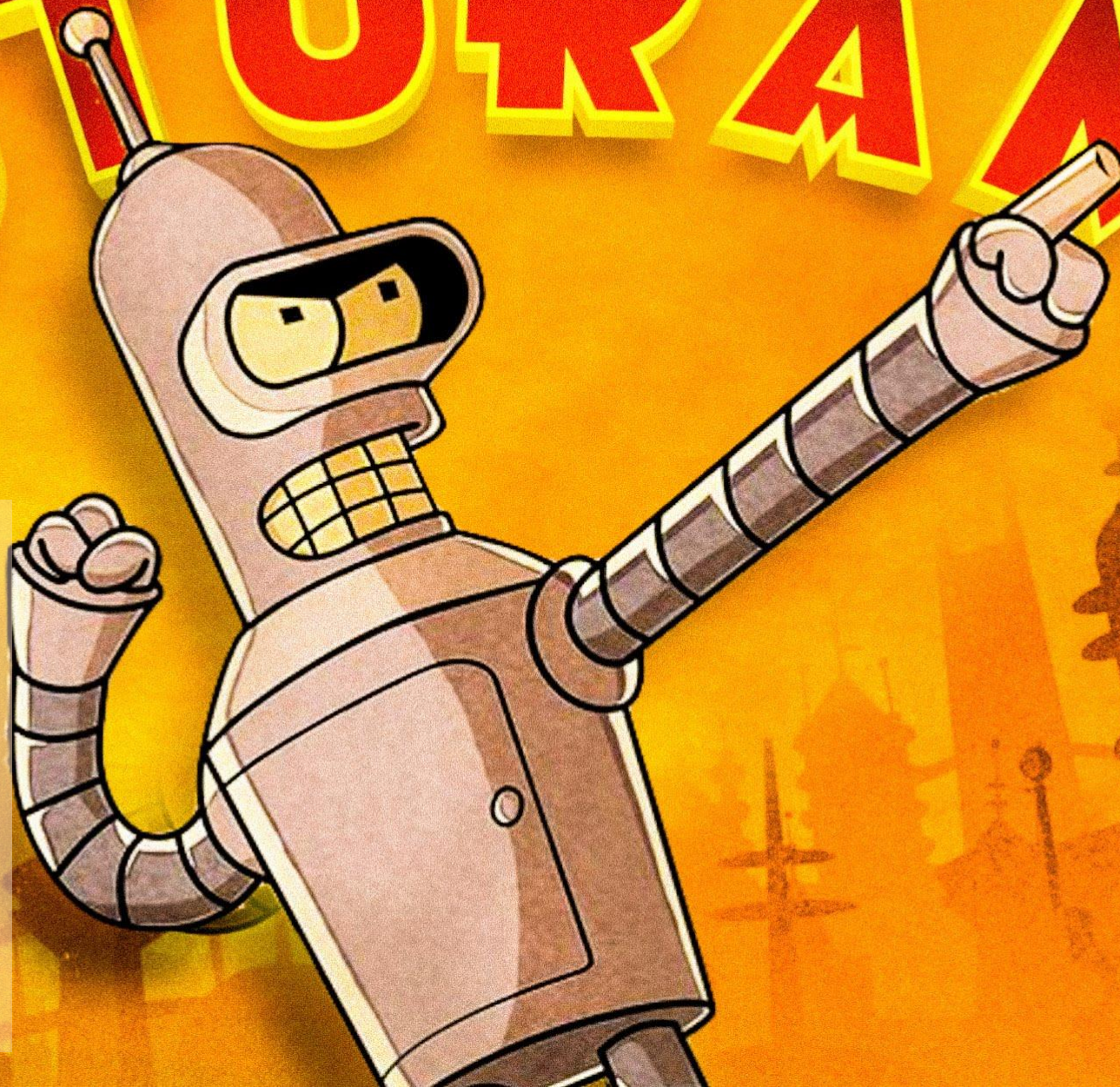
Agosto/2017

FUTURAMA

Bender:

um robô alcoólatra, fumante, cleptomaníaco, misantropo, egocêntrico, de boca suja e pavio curto **desenvolvido** pela Mom's Friendly Robot Company

pt.wikipedia.org



Mundobit – UOL - Renato Mota em Destaque

Inteligência artificial da Microsoft vira racista depois de um dia na internet

Tay foi criada para interagir com o público jovem pelo Twitter, Snapchat, Kik e Groupme. Na China, a Microsoft lançou o chatbot Xiaolce, que já conversou com 40 milhões de usuários e não teve problemas como Tay.

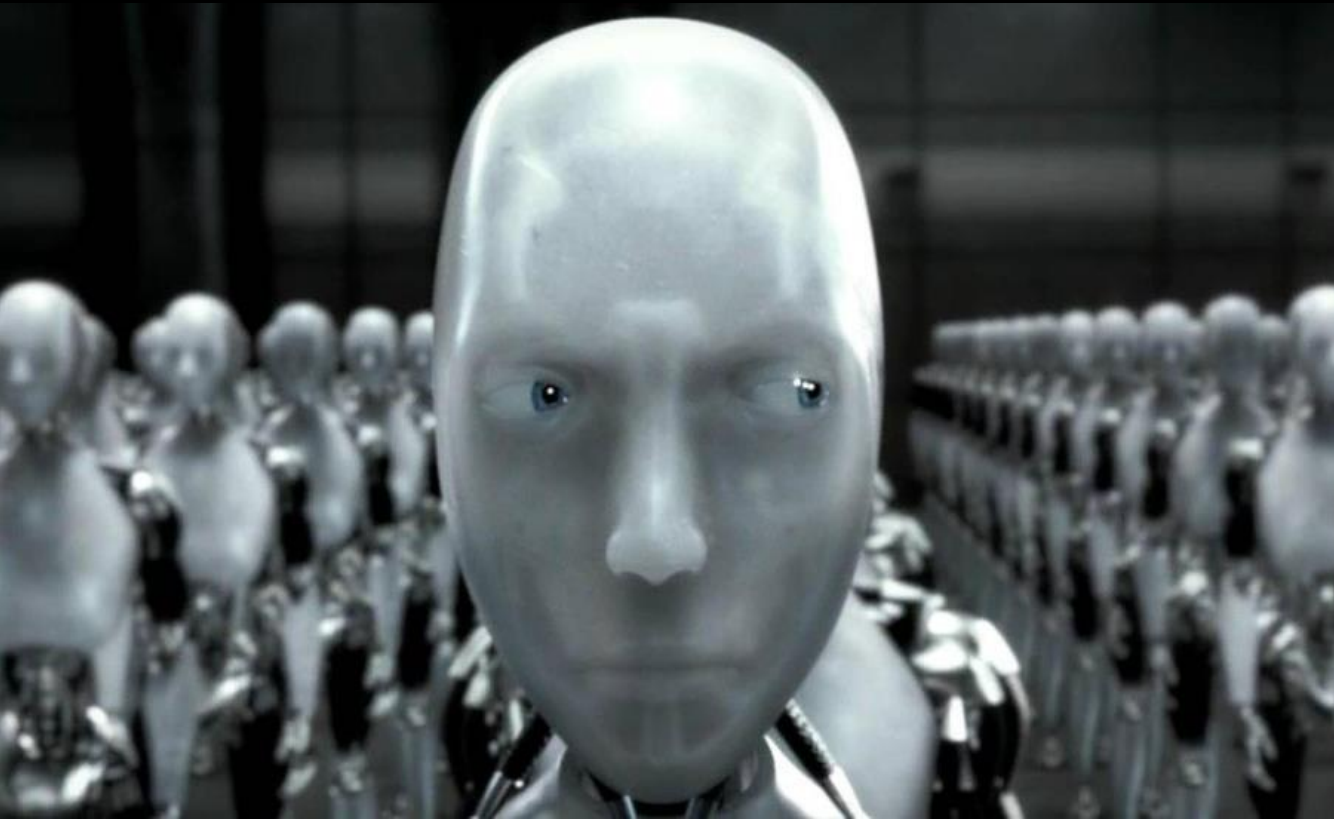
“Hitler não fez nada de errado”



SEREMOS
DOMINADOS



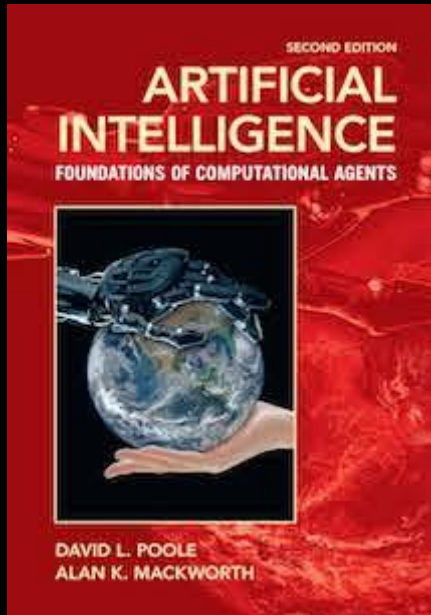
SEREMOS
SALVOS





Ex_Machina: Instinto Artificial - <http://www.adorocinema.com/filmes/filme-219931/>

O que é AI ?



“A inteligência artificial, ou AI, é o campo que estuda a síntese e análise de agentes computacionais que atuam de forma inteligente”

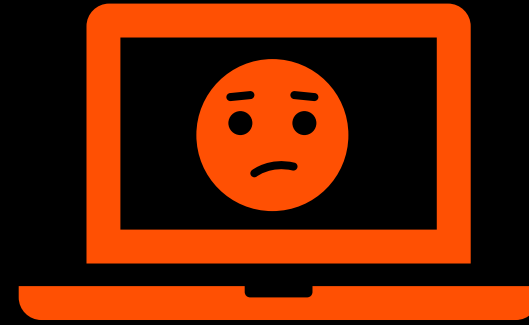
*Artificial Intelligence:
Foundations of Computational Agents*

2010 – 1st Edition
2017 – 2st Edition

David Poole

Alan Mackworth

<http://artint.info/html/ArtInt.html>



Como ser inteligente ?

1. Analisar informações
2. Formular e testar hipóteses
3. Construir e experimentar

Toda AI que simula um ser humano é inteligente. Será ?



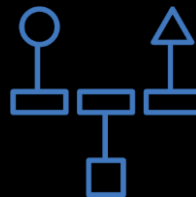
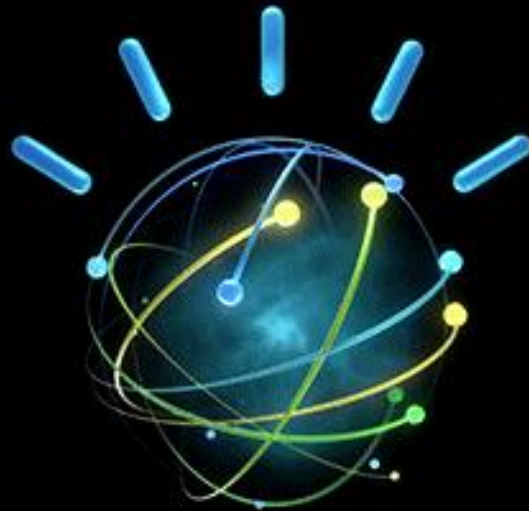
Chapolin Vemos Cérebro Não Sabemos (1974) - Episódio Ex-Perdido - YouTube

Política de Segurança da Informação (SI)



SEM AI

Perguntas frequentes sobre “onde que está dizendo isso”.



Watson Natural Language Classifier



COM AI

**Mais tempo livre
para os
profissionais de SI**

**Maior adoção de
segurança na
operação**

A	B
28 Qual a tecnologia de fonte de dados utilizada para riscos?	Norma de Cultura e Gestão de Riscos
29 Qual tecnologia é utilizada para gestão de treinamentos de segurança?	Norma de Cultura e Gestão de Riscos
30 Qual a tecnologia é utilizada para suportar o site interno de divulgação?	Norma de Cultura e Gestão de Riscos
31 Qual a tecnologia utilizada para fazer simulações de engenharia social?	Norma de Cultura e Gestão de Riscos
32 Qual a tecnologia utilizada para reportar incidentes de segurança?	Norma de Cultura e Gestão de Riscos
33 Qual a tecnologia utilizada para pesquisas de segurança?	Norma de Cultura e Gestão de Riscos
34 Qual a tecnologia utilizada para controle de riscos?	Norma de Cultura e Gestão de Riscos
35 Quais os processos para mapeamento dos riscos de segurança?	Norma de Cultura e Gestão de Riscos
36 Quais os processos para desenvolvimento de políticas de segurança?	Norma de Cultura e Gestão de Riscos
37 Quais os processos para reforçar o cumprimento das políticas de segurança?	Norma de Cultura e Gestão de Riscos
38 Quais os processos para educação e conscientização de segurança?	Norma de Cultura e Gestão de Riscos
39 Para os processos utilizados para conectar segurança com outras disciplinas?	Norma de Cultura e Gestão de Riscos
40 Quais os processos para verificar o conhecimento das políticas de segurança?	Norma de Cultura e Gestão de Riscos
41 Quais os processos de gestão de riscos?	Norma de Cultura e Gestão de Riscos
42 Quais os processos de comunicação e informação de segurança?	Norma de Cultura e Gestão de Riscos
43 Quais os processos para conscientização de segurança da identidade?	Norma de Cultura e Gestão de Riscos
44 Quais os processos utilizados para direcionar a estratégia de comunicação?	Norma de Cultura e Gestão de Riscos
45 Quais os processos para simulação de engenharia social?	Norma de Cultura e Gestão de Riscos
46 Quais os processos para administração dos incidentes de segurança?	Norma de Cultura e Gestão de Riscos
47 Qual processo para gestão na comunicação do blog/comunidade de segurança?	Norma de Cultura e Gestão de Riscos
48 Quais os processos utilizados para direcionar pesquisas de segurança?	Norma de Cultura e Gestão de Riscos
49 Qual a estrutura organizacional da segurança da informação?	Norma de Cultura e Gestão de Riscos
50 Quem são os profissionais que fazem parte da segurança da informação?	Norma de Cultura e Gestão de Riscos
51 Quais as funções e responsabilidades dos profissionais de segurança da informação?	Norma de Cultura e Gestão de Riscos
52 Como é feito a conscientização?	
53 Quais métricas são utilizadas para a segurança da informação?	
54 Quais métricas são utilizadas para a segurança da informação?	
55 Quais métricas são utilizadas para a segurança da informação?	
56 Quais métricas são utilizadas para a segurança da informação?	
57 Quais métricas são utilizadas para a segurança da informação?	
58 Quais métricas são utilizadas para a segurança da informação?	
59 Quais métricas são utilizadas para a segurança da informação?	



Consulta Política de Segurança

Informe sua necessidade sobre Segurança da Informação e o Watson irá informar a norma que poderá lhe auxiliar.

<https://consultapoliticasi.mybluemix.net/>

IBM Watson Natural Language Classifier

Training data Classifiers

Classes 12

+ Add class

Norma de Cultura e Gestão de Riscos	42
Norma de Gestão de Identidade e Acessos	29
Norma de Privacidade de dados	21
Norma de Resposta a Incidentes	46
Norma de Segurança Tecnológica	27
Norma de desenvolvimento seguro	30
Norma de mobilidade e redes sociais	30
Norma de segurança de cloud e virtualização	31
Norma de segurança de rede	24

Texts 300

Create classifier

+ Add text

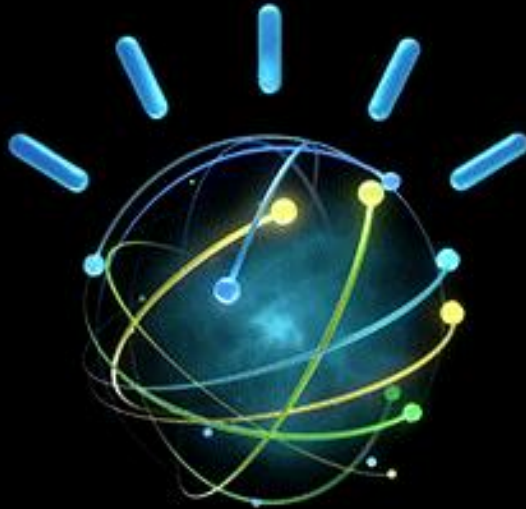
eu gostaria de saber sobre gestão de identidade e acesso	✓
Norma de Gestão de Identidade e Acessos	
Como são medidas as violações de segurança na nuvem?	
Norma de segurança de cloud e virtualização	
Como são medidos a continuidade e disponibilidade de serviços em nuvem e virtualização?	
Norma de segurança de cloud e virtualização	
Como são medidos a integração segura entre os sistemas/ambientes legados?	
Norma de segurança de cloud e virtualização	
Como são medidos a qualidade do programa de segurança dos dados?	
Norma de Privacidade de dados	

Agente inteligente de segurança



SEM AI

Luta eterna para diminuir os alertas de segurança ou chamados de “usuário e senha”



COM AI



Automação, padronização, “simpatia com o usuário” e foco no que realmente é crítico.



Watson Conversation



Node-Red

Agente de Segurança

A	B
28 Qual a tecnologia de fonte de dados utilizada para riscos?	Norma de Cultura e Gestão de Riscos
29 Qual tecnologia é utilizada para gestão de treinamentos de segurança?	Norma de Cultura e Gestão de Riscos
30 Qual a tecnologia utilizada para suportar o site interno de divulgação?	Norma de Cultura e Gestão de Riscos
31 Qual a tecnologia utilizada para fazer simulações de engenharia social?	Norma de Cultura e Gestão de Riscos
32 Qual a tecnologia utilizada para reportar incidentes de segurança?	Norma de Cultura e Gestão de Riscos
33 Qual a tecnologia utilizada para pesquisas de segurança?	Norma de Cultura e Gestão de Riscos
34 Qual a tecnologia utilizada para controle de riscos?	Norma de Cultura e Gestão de Riscos
35 Quais os processos para mapeamento dos riscos de segurança?	Norma de Cultura e Gestão de Riscos
36 Quais os processos para desenvolvimento de políticas de segurança?	Norma de Cultura e Gestão de Riscos
37 Quais os processos para reforçar o cumprimento das políticas de segurança?	Norma de Cultura e Gestão de Riscos
38 Quais os processos para educação e conscientização de segurança?	Norma de Cultura e Gestão de Riscos
39 Para os processos utilizados para conectar segurança com outras áreas?	Norma de Cultura e Gestão de Riscos
40 Quais os processos para verificar o conhecimento das políticas de segurança?	Norma de Cultura e Gestão de Riscos
41 Quais os processos de gestão de riscos?	Norma de Cultura e Gestão de Riscos
42 Quais os processos de comunicação e informação de segurança?	Norma de Cultura e Gestão de Riscos
43 Quais os processos para conscientização de segurança da identidade?	Norma de Cultura e Gestão de Riscos
44 Quais os processos utilizados para direcionar a estratégia de comunicação?	Norma de Cultura e Gestão de Riscos
45 Quais os processos para simulação de engenharia social?	Norma de Cultura e Gestão de Riscos
46 Quais os processos para administração dos incidentes de segurança?	Norma de Cultura e Gestão de Riscos
47 Qual processo para gestão na comunicação do blog/comunidade de segurança?	Norma de Cultura e Gestão de Riscos
48 Quais os processos utilizados para direcionar pesquisas de segurança?	Norma de Cultura e Gestão de Riscos
49 Qual a estrutura organizacional da segurança da informação?	Norma de Cultura e Gestão de Riscos
50 Quem são os profissionais que fazem parte da segurança da informação?	Norma de Cultura e Gestão de Riscos
51 Quais as funções e responsabilidades dos profissionais de segurança?	Norma de Cultura e Gestão de Riscos
52 Como é feita a conscientização de segurança na organização?	Norma de Cultura e Gestão de Riscos
53 Quais métricas são utilizadas para medir o envolvimento dos usuários?	Norma de Cultura e Gestão de Riscos
54 Quais métricas são utilizadas para medir o comportamento dos usuários?	Norma de Cultura e Gestão de Riscos
55 Quais métricas são utilizadas para medir o conhecimento dos usuários?	Norma de Cultura e Gestão de Riscos
56 Quais métricas são utilizadas para medir o conhecimento dos usuários?	Norma de Cultura e Gestão de Riscos
57 Quais métricas são utilizadas para medir resultados das pesquisas?	Norma de Cultura e Gestão de Riscos
58 Quais métricas são utilizadas para medir o alinhamento da segurança?	Norma de Cultura e Gestão de Riscos
59 Quais métricas estão contidas no dashboard do sistema de GRC?	Norma de Cultura e Gestão de Riscos



Watson Conversation / falecomoconsultorv2-2 / Build

Intents

Entities

Dialog

IniciaConversa

conversation_start

1 Response / 5 Context set

GatoNoTeclado

#GatoNoTeclado

1 Response / 0 Context set

IniciaAvaliacao

#AvaliacaoDeSeguranca

1 Response / 5 Context set

AVALIAR

#ComecaAvaliacao

1 Response / 0 Context set

Encerra conversa

@saudacoesFim

Try it out

Clear Manage Context 12

Olá, sou seu assistente de segurança, sou treinado para indicar práticas ou avaliar o nível de maturidade de segurança. Me diga, o que gostaria de fazer?

Enter something to test your bot

Use the up key for most recent

Show help



Meu Minion



SEM AI

Analise manual de diversos tipos diferentes de informações para evidenciar um “falso positivo”.



Cloudant



COM AI

**MUITO MAIS TEMPO
para atuar nos
alertas que
realmente
precisam de
atenção.**

Dúvidas



#TREINE SUA AI



Pedro Bezerra

[HTTPS://GOO.GL/W9WQOH](https://goo.gl/W9WQOH)