

COMO A INTELIGÊNCIA ARTIFICIAL PODE SER APLICADA CONTRA AS TENTATIVAS DE PHISHING

HOW ARTIFICIAL INTELLIGENCE TECHNOLOGIES CAN BE APPLIED AGAINST PHISHING ATTEMPTS

Marcos Antonio Inacio Junior¹; Alberane Lucio Thiago da Cunha²

RESUMO

Inteligência Artificial é um conceito no mundo da tecnologia que consiste em simular a capacidade humana, máquinas que possuem a capacidade de aprender a partir de análise e interpretação de dados e utilizam desse aprendizado para realizar tarefas ou resolver problemas. Na área da segurança da informação o uso da inteligência artificial é um fator decisivo para que as políticas de segurança cibernéticas se tornem mais pró-ativas e ao mesmo tempo preditivas, tendo então maior efetividade no combate a suas ameaças. Especificamente o Phishing é um tipo de golpe que está em constante crescimento devido às dezenas de novos ambientes digitais onde esses golpes podem ser aplicados, em conjunção ao aumento exponencial do consumo de tecnologia pela população. Esta pesquisa tem como objetivo investigar através da literatura científica as principais abordagens da inteligência artificial na segurança cibernética. Dados divulgados pela empresa Check Point Research, divisão de inteligência em ameaças de segurança, demonstram que no ano de 2022, a cada semana são registrados 1.540 incidentes de cibersegurança no Brasil. Os números, também, são maiores que os vistos na média global, onde são 1.200 ataques semanais contra empresas e organizações. Se justifica pela necessidade

¹ Aluno do Curso de Ciência da Computação do Centro Universitário do Sul de Minas. Email: marcos.junior2@alunos.unis.edu.br

² Professor do Curso de Ciência da Computação do Centro Universitário do Sul de Minas. Email: alberane.cunha@professor.unis.edu.br

de reforçar a proteção de dados dentro de ambientes corporativos, uma vez que estes dados possam conter informações sigilosas sobre a empresa, como o planejamento financeiro, estratégico ou político da organização que, se expostos, podem afetar a sua estabilidade econômica.

Palavras-chave: Cibersegurança. Inteligência Artificial. Phishing. Dados

ABSTRACT

Artificial Intelligence is a concept in the world of technology that consists of simulating human capacity, machines that have the ability to learn from the analysis and interpretation of data and use this learning to perform tasks or solve problems. In the area of information security, the use of artificial intelligence is a decisive factor for cybersecurity policies to become more proactive and predictive, thus having greater effectiveness in combating threats. Phishing specifically is a type of scam that is constantly growing due to the dozens of new digital environments where these scams can be applied, in conjunction with the exponential increase in technology consumption by the population. This research aims to investigate through the scientific literature the main approaches of artificial intelligence in cybersecurity. Data released by Check Point Research, a security threat intelligence division, show that in the year 2022, 1,540 cybersecurity incidents are recorded every week in Brazil. The numbers are also higher than those seen in the global average, where there are 1,200 weekly attacks against companies and organizations. It is justified by the need to strengthen data protection within corporate environments, since these data may contain confidential information about the company, such as the organization's financial, strategic or political planning, which, if exposed, may affect its economic stability.

Palavras-chave: Cybersecurity. Artificial Intelligence. Phishing. Data.

1 INTRODUÇÃO

Inteligência Artificial é um conceito no mundo da tecnologia que consiste em simular a capacidade humana, máquinas que possuem a capacidade de aprender a partir de análise e interpretação de dados e utilizam desse aprendizado para realizar tarefas ou resolver problemas. Estas máquinas treinadas são capazes de analisar uma quantidade extremamente mais elevada de informações que o ser humano, se torna um fato de que a inteligência artificial é superior à capacidade humana no quesito realizar tarefas repetitivas, principalmente em grande escala. Na área da segurança da informação o uso da inteligência artificial é um fator decisivo para que as políticas de segurança cibernéticas se tornem mais pró-ativas e ao mesmo tempo preditivas, tendo então maior efetividade no combate a suas ameaças.

O phishing é uma das ameaças mais antigas com o quais devemos nos preocupar, contudo, na atualidade esse tipo de golpe está em constante crescimento devido às dezenas de novos ambientes digitais onde esses golpes podem ser aplicados, em conjunção ao aumento exponencial do consumo de tecnologia pela população. Esse tipo de ameaça é aplicada pelos criminosos por meio de ambientes eletrônicos, sejam eles sites ou telecomunicação e consiste primordialmente em extrair informações das vítimas através de fraudes e falsas identidades.

Dados divulgados pela empresa Check Point Research, divisão de inteligência em ameaças de segurança, demonstram que no ano de 2022, a cada semana são registrados 1.540 incidentes de cibersegurança no Brasil. Os números, também, são maiores que os vistos na média global, onde são 1.200 ataques semanais contra empresas e organizações.

Este artigo se justifica pela necessidade de reforçar a proteção de dados dentro de ambientes corporativos, uma vez que estes dados possam conter informações sigilosas sobre a empresa, como o planejamento financeiro, estratégico ou político da organização que, se expostos, podem afetar a sua estabilidade de mercado. Organizações que são responsáveis pelos dados pessoais de seus clientes fazem com que esta necessidade se torne uma obrigação legislativa, podendo a organização responder criminalmente se os dados de seus clientes não estiverem devidamente protegidos de acordo com a Lei Geral de Proteção de Dados Pessoais

(LGPD), Lei nº 13.709/2018, que foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo.

A pesquisa tem como objetivo investigar através da literatura científica e publicações de empresas renomadas as principais abordagens da computação cognitiva na área da segurança cibernética, sob este estudo mapear como a inteligência artificial tem sido utilizada, ou ainda pode ser utilizada, para aprimorar a segurança da informação, pontuando os seguintes objetivos específicos: Apresentar o conceito de cibersegurança; Apresentar o conceito de inteligência artificial; Relacionar de que forma a inteligência artificial têm sido utilizada contra o Phishing;

2 REFERENCIAL TEÓRICO

2.1 Cibersegurança

A cibersegurança é um conjunto de políticas, ferramentas, práticas e procedimentos de segurança da informação que através da perícia e análise e gerenciamento de riscos conseguem então proteger as organizações do cibercrime. Sendo utilizada para garantir propriedades de segurança para evitar possíveis riscos no ciberespaço, tal como, integridade, confidencialidade e disponibilidade. A cibersegurança não é focada somente na proteção do ambiente digital, mas também na proteção do que é executado em seu ambiente e em quaisquer ativos que tenham uma relação com ele (ROSSOUW; JOHAN, 2013).

Possui como premissa garantir que usuários mal intencionados não consigam ter acesso a mensagens destinadas a outros usuários, evitar ameaças como o acesso remoto de usuários não autorizados a sistemas de informação privados. Se propõe a combater ameaças digitais não somente como vírus cibernéticos, mas, confirmar a legitimidade de mensagens onde todas as informações passam por um processo de validação, verificando se é realmente uma mensagem de um remetente confiável ou uma organização criminosa de terceiros (TANENBAUM, 2011, p. 763).



2.2 Phishing

A técnica de phishing é uma ameaça comum encontrada pela internet, Ivan Belcic (2020, p.1) a define como:

O phishing é um dos golpes mais antigos e conhecidos da internet. Podemos definir phishing como qualquer tipo de fraude por meios de telecomunicação, que usa truques de engenharia social para obter dados privados das vítimas.

Um ataque de phishing possui as características marcantes, primeiramente o ataque é realizado por algum meio de comunicação eletrônica, nesta abordagem o criminoso irá se identificar como outra pessoa ou organização e seu principal objetivo é extrair informações valiosas do outro indivíduo como senhas ou números de cartão de crédito. Em uma comunicação direta pode convencer a vítima a abrir algum link, baixar anexos ou até mesmo enviar pagamentos reais (IVAN BELCIC, 2020).

A Microsoft indica que os criminosos podem utilizar de vários meios de comunicação eletrônicas:

Os criminosos cibernéticos também podem fazer com que você visite sites falsos com outros métodos, tais como mensagens de texto ou ligações telefônicas. Criminosos cibernéticos sofisticados organizam call centers para ligar ou mandar SMS automaticamente para os números de possíveis alvos. Estas mensagens muitas vezes incluem avisos para que você digite um número PIN ou algum outro tipo de informação pessoal.

2.2.1 Pharming

Essa técnica ataca algumas das vulnerabilidades do sistema DNS, essa ação é conhecida também como DNS cache poisoning. O servidor DNS é responsável por traduzir uma URL em endereço de máquina, ou IP, ao digitar www.google.com.br o sistema DNS que é responsável por lhe direcionar ao IP 74.125.234. Caso o servidor DNS esteja vulnerável, o endereço digitado poderá ser direcionado para uma página falsa hospedada em outro servidor com outro endereço IP. Essa ação é feita de forma automática, por esse motivo é uma técnica muito difícil de ser percebida pelo usuário (PAIVA, 2007).



2.2.2 Spear Phishing

Spear phishing é um golpe realizado por e-mail ou comunicação eletrônica, direcionado a um indivíduo, organização ou empresa específicos. Tendo a intenção de roubar dados para fins maliciosos, os criminosos virtuais podem instalar algum malware no computador do usuário para prejudicar seu sistema diretamente (KASPERSKY, s.d).

2.2.3 Whaling / CEO Fraud

Focado em se passar por pessoas de alto poder executivo, esse tipo de ataque normalmente vem atrelado a intimidações judiciais ou notificações empresariais internas. Este ataque utiliza meios como comunicados fraudulentos que fazem parecer vir de uma pessoa muito influente na organização, pois psicologicamente os funcionários tendem a acreditar mais em informações de quem eles consideram importante (SALVIANO et. al, 2022).

2.2.4 Vishing

Fugindo do conceito de mensagens eletrônicas, este é um golpe aplicado por meio de voz (VoIP). Do outro lado da linha, um criminoso pode tentar se passar por um representante de uma empresa para confirmar informações do usuário. Frequentemente, empresas de telecomunicações ou bancos são exploradas neste tipo de golpe. É importante estar especialmente atento ao contexto das chamadas de voz, pois os servidores de VoIP permitem mudar o número que identifica a chamada (BLOCKBIT, s.d.).

2.2.5 Clone Phishing

Os criminosos clonam um e-mail legítimo recebido anteriormente que contenha um link ou um anexo. Em seguida, os links antes contidos na mensagem são substituídos por endereços maliciosos que podem conter malwares dentre outras ameaças. Usuários ingênuos podem clicar



no link ou abrir o anexo que, geralmente, permite que seus sistemas sejam recrutados (MALWAREBYTES, s.d).

2.3 Inteligência Artificial

A inteligência artificial busca reproduzir grandes capacidades da humanidade, como a aprendizagem e a resolução de problemas, tais capacidades que durante a história foram investigadas pela ciência de forma a entender o seu funcionamento, isto é, como compreendemos, como previmos ou como manipulamos o que está à nossa volta. A inteligência artificial, no entanto, não se limita apenas em compreender, mas também em criar entidades inteligentes (RUSSELL; NORVIG, 2010).

Grandes avanços teóricos em inteligência artificial tem produzido aplicações práticas que alimentam muitos de nossos aplicativos e sistemas, nos próximos anos irá fabricar a maioria do que consumimos e muito provavelmente terá o potencial de tirar nossos empregos (LEE; BARBÃO, 2019).

2.3.1 Redes Neurais

Redes neurais são sistemas de computação com nós interconectados que funcionam como os neurônios do cérebro humano. Através de algoritmos, essas redes neurais são capazes de reconhecer padrões escondidos e correlações em dados brutos, podendo então agrupá-los e classificá-los, atitude que conseqüentemente com o tempo irá aperfeiçoar seu funcionamento de forma a aprender e melhorar continuamente (SAS, s.d.).

2.3.2 Machine Learning

Machine learning é um subcampo da inteligência artificial que se concentra no uso de dados e algoritmos para reproduzir a maneira como os humanos aprendem, melhorando gradualmente sua precisão (IBM, 2020).

Por meio do uso de métodos estatísticos, os algoritmos são treinados para fazer classificações ou previsões, revelando os principais insights em projetos de mineração de dados. Esses insights subsequentemente conduzem a tomada de decisões em aplicativos e negócios, impactando de forma ideal as principais métricas de crescimento (IBM, 2020).

Dentro do conceito de Machine Learning existem algumas categorias a serem detalhadas, dentre elas :

- a) Aprendizado supervisionado : é um modelo onde os dados utilizados já são familiares e conhecidos, as suas características já são identificadas previamente em relação ao ambiente da aplicação (BI; QIFANG et. al., 2019).
- b) Aprendizado não-supervisionado : o algoritmo recebe dados sem categorização prévia, em seguida tenta identificá-los por relações naturais e após isso irá agrupá-los (BI; QIFANG et. al, 2019).
- c) Aprendizado semi-supervisionado : é um híbrido entre os dois modelos anteriores, possuindo então dados qualificados ou não, se torna útil quando o custo de qualificação é mais elevado (BI; QIFANG et al., 2019).
- d) Aprendizado por reforço : a máquina aprenderá por tentativa e erro, seu conhecimento é baseado em feedbacks positivos ou negativos através de suas próprias ações (BI; QIFANG et al., 2019).

2.3.3 Deep Learning

Como o Deep Learning e o Machine Learning tendem a ser usados de maneira alternada, é importante destacar que há diferença entre os dois. No entanto, o deep learning é, na verdade, um subcampo do machine learning (IBM, 2020).

Segundo a IBM pode-se diferenciar o Deep Learning e o Machine Learning :

A maneira pela qual o deep learning e o machine learning diferem é em como cada algoritmo aprende. O deep learning automatiza grande parte do processo de extração de recursos, eliminando parte da intervenção humana manual necessária e permitindo



o uso de conjuntos de dados maiores. Você pode pensar em deep learning como "machine learning escalável.

O Deep Learning se baseia na rede neural profunda, em essência, uma percepção mais apurada de inteligência artificial, que se aproxima com a do ser humano e é capaz de gerar conteúdos baseado no aprendizado a partir dessa assimilação. Os algoritmos de Deep Learning são capazes de analisar dados não-estruturados sem que haja algum tipo de pré-processamento ou supervisão (GOODFELLOW et. al, 2016).

2.3.4 Natural Language Processing

Pode ser descrita como uma gama de técnicas computacionais destinadas a analisar e representar textos que ocorrem naturalmente em um ou mais níveis de análise linguística com o objetivo de obter processamento de linguagem semelhante ao humano para uma variedade de tarefas ou aplicativos (LIDDY; E.D, 2001).

O Natural Language Processing (NLP) usa machine learning para revelar a estrutura e o significado do texto. Com aplicações de processamento de linguagem natural, as organizações podem analisar textos e extrair informações sobre pessoas, lugares e eventos (GOOGLE, 2022).

2.3.5 Fuzzy Logic

A lógica fuzzy determina um número que descreve um conjunto potencialmente grande de variáveis incertas e vagas associando intervalos a variáveis linguísticas, permitindo a fácil alteração da aplicação lógica clássica aumentando e facilitando seu uso em condições variadas e multidimensionais agregando valores a variáveis além do conceito binário de modo que sua implementação possibilita o tratamento de variáveis antes de fugir ao controle (SHAW; SIMÕES, 1999).

A maneira como a lógica fuzzy lida com a ambiguidade da informação e a incerteza do mundo real fez com que este raciocínio fosse aplicado na inteligência artificial devido sua



capacidade de imitar o raciocínio humano, que considera verdades parciais ou graus de verdade (GIGCH; PIPINO, 1980).

As variáveis são associadas a termos que definem seu pertencimento e as operações são feitas a partir da linguagem natural, cujo maior benefício é a codificação de conhecimentos inexatos, se aproximando de um modelo cognitivo, característicos da mente humana (RUHOFF et al., 2005).

2.4 Relação entre as áreas

2.4.1 Deep Neural Network (DNN)

Este tipo algoritmo suporta um largo volume de dados, são utilizados para verificar URLs, retornando se a mesma é realmente legítima ou uma tentativa de Phishing. A utilização do DNN para detectar e combater ataques de Phishing é eficiente pela sua alta precisão, sendo possível utilizar vários algoritmos de Deep Learning simultaneamente para tornar a defesa do sistema mais robusta, uma vez que os algoritmos irão se complementar (SUMATHI; SUJATHA, 2019; VREJOIU, 2019).

No entanto, o aumento do número de recursos de entrada irá afetar o desempenho computacional. O aprendizado por retropropagação pode ser utilizado para aprimorar o desempenho do modelo DNN. O ajuste de peso pode ser feito pela retropropagação do erro nos neurônios da camada de saída para as camadas anteriores. A seleção adequada de hiperparâmetros afeta diretamente o desempenho, encontrar o melhor modelo de parâmetros é uma questão importante (GLOROT; BENGIO, 2010).

2.4.2 Convolutional Neural Network (CNN)

Primeiramente familiarizado com a identificação de padrões ocultos da imagem sequencialmente, ou seja, da identificação de recursos de baixo nível para recursos de alto nível. As camadas inferiores da rede são responsáveis pela identificação de características básicas e



suas camadas subsequentes são responsáveis por identificar recursos complexos. O modelo CNN é mais frequentemente usado para o problema de classificação no processamento de imagens (GOODFELLOW et. al, 2016).

2.4.3 Natural Language Processing

As técnicas de NLP são aplicadas para analisar cada sentença e identificar o significado semântico de palavras essenciais no contexto de uma mensagem. O algoritmo utilizado analisa a sentença no e-mail, então identifica se o e-mail é confiável ou não, também é utilizada uma verificação à parte em todos os links anexados no e-mail. Pode detectar diferentes contextos e conteúdos em um golpe de e-mail padrão, o qual facilita imensamente a identificação (MUKHERJEE et.al, 2019).

2.4.4 Fuzzy Logic

Fazendo uso da regra de IF-THEN do sistema Fuzzy na forma de obter conhecimentos de especialistas, permitindo lidar com problemas imprecisos e vagos. É utilizado em várias aplicações para otimização, controle e identificação de sistemas. Os Sistemas Fuzzy primordialmente não têm a capacidade de aprendizado e nem de se reajustar sobre si mesmos, foi então que surgiu a ideia de sistemas Fuzzy aplicarem o comportamento das Redes Neurais, assim surgiu o sistema Neuro-Fuzzy, esse modelo pode ser aplicado ao combate contra o Phishing, uma vez que este consegue identificar se a comunicação eletrônica é Phishing, ou legítima (NGUYEN; TO, 2016).

3 CONCLUSÃO

Através da informação mais detalhada sobre as técnicas de cada uma das áreas, foi possível fomentar o conhecimento em cibersegurança centralizado nas ameaças de Phishing, bem como a Inteligência Artificial e o seu uso no combate a essas ameaças.

Este artigo foi baseado em uma revisão da literatura dentre livros, artigos científicos e publicações de grandes empresas com atuação na área, selecionando as fontes mais relevantes. Primeiramente foi apresentada uma conceitualização das áreas, em busca de conhecer suas características e valências, após, foi observado quais as técnicas da Inteligência Artificial que apresentam uma maior presença no combate ao Phishing, com estas técnicas identificadas seguiu-se uma seleção da literatura científica que cruzam ambas as áreas e apresentam sua eficiência e eficácia.

A Cibersegurança concentra-se na proteção e defesa de um sistema no ciberespaço, através de ferramentas, políticas e outras, para auxiliar no combate de possíveis ameaças. O que se pretendeu foi encontrar formas de minimizar os danos causados por estes ataques, através do uso da Inteligência Artificial, esta centra-se na aprendizagem das máquinas tendo como base o comportamento cognitivo do ser humano.

A inteligência artificial não possui uma única técnica que irá predominar no combate a essas ameaças, uma vez que as mesmas possam possuir diversas formas de atacar. É destacada a união de algoritmos que se complementam, formando defesas robustas que irão conseguir decifrar e impedir ataques cada vez mais complexos.

O objetivo deste estudo foi apresentar e descrever algo útil para os gestores de Tecnologias de Informação, que auxiliará no momento de decisão sobre o que pretendem utilizar para melhorar a segurança de seu sistema. A área da Inteligência Artificial por ser muito ampla, neste estudo foram mencionadas apenas as principais áreas e as que demonstraram maior utilidade para ajudar a combater os ataques cibernéticos.

REFERÊNCIAS

BI, Qifang & KATHERINE, E. Goodman & JOSHUA, Kaminsky & JUSTIN, Lessler, What is Machine Learning? A Primer for the Epidemiologist. American Journal of Epidemiology. Volume 188, Issue 12. Pages 2222–2239. Dez 2019.

BLOCKBIT, Fique alerta para os tipos comuns de phishing. s.d. Disponível em : <https://www.blockbit.com/pt/blog/fique-alerta-para-os-tipos-comuns-de-phishing/>. Acesso em: 1.out.2022

FUKUSHIMA, K & MIYAKE, S. Neocognitron: a self-organizing neural network model for a mechanism of visual pattern recognition. In: Competition and cooperation in neural nets. Springer, Berlin, Heidelberg, pp 267–285. 1982.

GIGCH, J.; PIPINO, L. Form Absolute to Probable to Fuzzy in Decision Making. Kybernetes, v. 19, p. 433-461. 1980.

GLOROT, X & BENGIO, Y. Understanding the difficulty of training deep feedforward neural networks. Proceedings of the thirteenth international conference on artificial intelligence and statistics, p 249–256. 2010.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. Deep Learning. Cambridge: MIT Press. Jan, 2016.

GOOGLE, O que é processamento de linguagem natural?. s.d. Disponível em : <https://cloud.google.com/learn/what-is-natural-language-processing?hl=pt-br>. Acesso em: 3.out.2022

IBM, O que é Machine Learning?. Jul, 2020. Disponível em: <https://www.ibm.com/br-pt/cloud/learn/machine-learning#toc-mtodos-de--jJ9aK-QI>. Acesso em: 3.out.2022

IVAN, Belcic. O que é phishing?. Avast. Fev, 2020. Disponível em : <https://www.avast.com/pt-br/c-phishing#topic-4>. Acesso em: 22.set.2022

LEE, Kai-Fu. & BARBÃO, Marcelo. Inteligência artificial edição português. Globo Livros. Nov, 2019

KASPERSKY, O que é spear phishing?. s.d. Disponível em : <https://www.kaspersky.com.br/resource-center/definitions/spear-phishing>. Acesso em: 15.set.2022

LIDDY, E.D. Natural Language Processing. In Encyclopedia of Library and Information Science, 2nd Ed. NY. Marcel Decker, Inc. 2001

LU et. Al. BIM and Big Data for Construction Cost Management. Abingdon, Oxon: Routledge. P. 112. 2019

MALWAREBYTES, O que é Phishing?. Disponível em :
<https://br.malwarebytes.com/phishing>. Acesso em: 10.set.2022

Microsoft, Proteja-se contra phishing. Disponível em: [https://support.microsoft.com/pt-br/windows/proteja-se-contraphishing-0c7ea947-ba98-3bd9-7184-430e1f860a44#:~:text=Phishing%20\(pronunciado%3A%20fishing\)%20é,sites%20que%20finagem%20ser%20legítimos](https://support.microsoft.com/pt-br/windows/proteja-se-contraphishing-0c7ea947-ba98-3bd9-7184-430e1f860a44#:~:text=Phishing%20(pronunciado%3A%20fishing)%20é,sites%20que%20finagem%20ser%20legítimos). Acesso em: 12.set.2022

MUKHERJEE, Anirban & AGARWAL,Nimit & GUPTA, Shubham. A SURVEY ON AUTOMATIC PHISHING EMAIL DETECTION USING NATURAL LANGUAGE PROCESSING TECHNIQUES. International Research Journal of Engineering and Technology (IRJET). Volume: 06 Issue: 11. Nov 2019

NGUYEN, L. A., NGUYEN, H. J., & To, B. L. An Efficient Approach Based on Neuro-Fuzzy for Phishing Detection. Journal of Automation and Control Engineering. 2016

PAIVA, Cláudio. Scam, phishing e pharming: as fraudes praticadas no ambiente Internet Banking e sua recepção no Brasil, 2007.

ROSSOUW, Von Solms; JOHAN, Van Niekerk. From information security to cyber security. Computers & Security, v. 38, p. 97-102. Out, 2013

RUSSEL, S. J. , & Norvig, P. Artificial Intelligence: A Modern Approach 3rd Edition. Upper Saddle River, New Jersey 07458.: Pearson Education, Inc. 2010

SALVIANO, Edgard Mesquita & SANTOS, João Pedro Ribeiro & Silva, Matheus Almeida. Principais tipos de ataques Phishing e mecanismos de segurança. UNICEPLAC. Jul, 2022

SAS, Redes Neurais, o que são e qual sua importância?. Disponível em:
https://www.sas.com/pt_br/insights/analytics/neural-networks.html. Acesso em: 11.out.2022

SHAW, I. S.; SIMÕES, M. G. Controle e modelagem Fuzzy. São Paulo: E. Blücher, p.165. 1999.

SUMATHI, K., & SUJATHA, V. Deep learning based-Phishing attack detection. International Journal of Recent Technology and Engineering. 2019

TANENBAUM, Andrew Stuart; WETHERALL, David J. Computer Networks. Prentice Hall, Cloth, 2011.



VREJOIU, M. H. Neural Networks and Deep Learning in Cyber Security. Romanian Cyber Security Journal. 2019