INTERFACE TECNOLÓGICA

O PAPEL DA INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA CIBERNÉTICA: o uso de sistemas inteligentes em benefício da segurança dos dados das empresas

THE ROLE OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY: the use of intelligent systems for the benefit of corporate data security

Eduarda Pagim Zequim – mydd1@hotmail.com
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

Douglas Francisco Ribeiro – douglas.ribeiro@fatectq.edu.br
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

DOI: 10.31510/infa.v19i1.1358
Data de submissão: 15/12/2021
Data do aceite: 25/05/2022
Data da publicação: 30/06/2022

RESUMO

Presente na rotina na maioria das pessoas e principalmente nas organizações, a tecnologia tem sido a principal responsável para resoluções de problemas de forma inteligente, mas seu uso de forma inadequada pode abrir espaço para brechas nos sistemas da organização, ocasionando ataques mal-intencionados e vindo a causar prejuízos em larga escala. Com isso, esse trabalho tem o objetivo de apresentar o quanto a Inteligência Artificial é importante para as grandes, médias e pequenas organizações, auxiliando principalmente na identificação de ataques mal-intencionados e reforçando assim a segurança da informação.

Palavras-chave: Segurança da informação. Inteligência artificial nas empresas. Ataque Hacker.

ABSTRACT

Present in the routine of most people and especially in organizations, technology has been the main responsible for solving problems in an intelligent way, but its improper use can open space for breaches in the organization's systems, causing malicious attacks and coming causing large-scale damage. With that, this work aims to present how Artificial Intelligence is important for large, medium and small organizations, helping mainly in the identification of malicious attacks and thus reinforcing information security.

Keywords: Information security. Artificial intelligence in companies. Hacker Attack.

1. INTRODUÇÃO

Grande parte das organizações tem considerado a informação como um dos seus principais recursos para auxiliar na tomada de decisões no meio corporativo. Assim, podemos afirmar que, sem a informação a dificuldade das empresas se manterem competitivas no mercado aumenta a cada dia.

Como a informação é um ativo importante na sociedade, estas precisam ser protegidas contra as ameaças que podem pôr em risco seu conteúdo, seja por alguma modificação, divulgação não autorizada ou até mesmo perda, (BEAL, 2008).

Atualmente já existem diversos mecanismos de proteção, tais como: antivírus, sistemas de autenticação de token, dentre outros. Essas ferramentas tecnológicas têm a função de manter os dados em segurança, porém ainda não é o suficiente para garantir a confidencialidade dos dados.

Esse estudo tem como o objetivo avaliar o conceito da Inteligência Artificial (IA) e a sua importância na segurança da informação para as empresas, reforçando a segurança e diminuindo os ataques que levam a perderem os seus dados.

A metodologia do estudo será a revisão bibliográfica, realizada através de revisão de livros, materiais específicos e artigos, a fim de compreender e demonstrar a importância da segurança de dados e como esses processos podem ser realizados utilizando a inteligência artificial. Após as análises realizadas, o estudo avança a uma avaliação sobre os benefícios do uso de inteligência artificial no âmbito da segurança cibernética.

O estudo se justifica por verificar que, cada vez mais, a segurança da informação vem abrangendo o mercado, precisando de maior segurança e identificação de ocorrências de problemas cibernéticos nas organizações, assim sugerindo medidas de proteção e aumentando a segurança através da identificação de falhas que resultam em perdas de dados.

2. INTELIGENCIA ARTIFICIAL

Segundo Fernandes (2003), a palavra inteligência artificial se origina do latim, ela se divide em inter (entre) e legere (escolher), ou seja, a inteligência é aquilo que o homem pode escolher entre uma coisa e outra, entre realizar tarefas e de resolver problemas.

A inteligência artificial pode ser definida como uma área da ciência da computação que desenvolve e estuda sistemas inteligentes, esses sistemas em que se assemelham no comportamento humano, como por exemplo: aprendizado, compreensão da linguagem e resolução de problemas, (FERNANDES, 2003).

Podemos dizer que a Inteligência Artificial aprende como uma criança. Aos poucos, o sistema absorve, analisa e organiza os dados de forma a entender e identificar o que são objetos, pessoas, padrões e reações de todos os tipos, (COSSETI, 2019).

Para Pimenta (2021), a inteligência artificial é uma área responsável por simular o comportamento e a inteligência humana utilizando apenas máquinas. Podemos dizer que o objetivo da inteligência artificial é executar atividades humanas, desde a mais complexas até as mais simples, como dirigir um carro por exemplo.

Por mais que a inteligência artificial esteja se tornando muito boa em tarefas humanas ela ainda é um robô. Suas especialidades são estruturadas e definidas em regras exatas. É justamente essa característica que faz com que a inteligência artificial tenha desempenho em algo lógico: a otimização de processos. Essa tecnologia pode avaliar estatísticas e dados e agilizar processos, corrigindo assim os desvios e determinando o que pode ou não ser eliminado, (PIMENTA, 2021).

3. SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação, em inglês também conhecida como *InfoSec,* é o que garante que não haja acessos não autorizados a computadores, dados e redes. Contudo, ela consegue manter a autenticidade, confidencialidade e disponibilidade de informações de extrema importância para as organizações, (GAIDARGI, 2018).

Segundo Zeferino (2020), a segurança da informação é um conjunto de boas práticas e ações que tem a finalidade de proteger um grupo de dados. Essas medidas de segurança podem ser executadas em todas as empresas que trabalham com dados, uma vez que a organização gera informações próprias. Ela é baseada em quatro pilares que sustentam as medidas tomadas para garantir a confidencialidade dos dados, que são: confidencialidade, autenticidade, integridade e disponibilidade.

Um erro na confidencialidade, por mais simples que seja, pode ocasionar grandes danos a uma organização, deixando-os livres para que pessoas mal-intencionadas ou até mesmo concorrentes possam acessá-los, manipulá-los e causar violentamente altos riscos a empresa. Também poderá ocorrer ataques nos servidores da organização por parte de *hackers*[1]resultando no vazamento de dados de clientes armazenados.

[1]*Hacker* é uma palavra em inglês do âmbito da informática que indica uma pessoa que possui bons conhecimentos em nessa área a ponto de conseguir fazer modificações em alguns sistemas informáticos.

Nestes casos, a empresa poderá sofrer o risco de ser multada, perder clientes e, contudo, sofrer prejuízos financeiros, sem dizer na imagem que a instituição acabará passando para o mercado, sem dizer de como ficará manchada por conta de todas as falhas de segurança a todos os clientes que a pertencia, sendo assim um dos pontos mais críticos na obtenção de conquistar novos clientes.

Quando o assunto é autenticidade, estamos falando sobre todos os mecanismos utilizados para que haja uma garantia de que as informações sejam autenticas para evitar fraudes, deixando assim os clientes e a organização em segurança.

De acordo com Zeferino (2020), a integridade dos dados está ligada aos mecanismos de segurança e ferramentas, como os backups, podendo assim assegurar que os dados não sejam vazados ou perdidos em caso de erros de segurança adotados pela organização.

Quando falamos em disponibilidade, estamos falando da capacidade de acessar os dados a qualquer momento. É de extrema importância que todas as informações estejam disponíveis aos usuários quando solicitado, trazendo um fator que agrega uma maior agilidade nos processos da instituição, sendo elas organizacionais ou não.

A segurança da informação assegura que as informações e os dados sigilosos da empresa não caiam em mãos de pessoas não autorizadas. Ela também impossibilita o acesso aos dados e possíveis ataques hackers ou até mesmo a destruição das informações, (GAIDARGI, 2018).

4. SEGURANÇA CIBERNÉTICA

A segurança cibernética é um conjunto de ações sobre processos, pessoas e tecnologias que são utilizados contra os ataques cibernéticos. Algumas vezes nomeada como segurança de TI ou segurança digital, é uma ramificação na segurança da informação, (FERNANDES, 2021).

A segurança cibernética é um braço da segurança da informação, nesse caso a segurança cibernética tem o objetivo de prevenir ataques realizados por sistemas que se aproveitam de falhas sistêmicas para assim invadir dispositivos, manipulando, roubando e tornando indisponível uma série de dados ou arquivos, (SCHULTZ, 2020).

De acordo com Fernandes (2021), um fator equivocado que as pequenas e médias empresas cometem é não conhecer ou minimizar o valor da informação, pois muitos acreditam que somente grandes empresas são alvos de hackers, mas a verdade é que os cibe

criminosos estão 24 horas buscando informações, sejam elas de grandes ou pequenas empresas, eles estão sempre à procura de uma oportunidade para roubá-las.

Para Guido (2019), o elemento mais problemático da segurança cibernética é a constante evolução dos riscos. A abordagem tradicional tem sido concentrar os recursos nos componentes mais importantes do sistema para se proteger das maiores ameaças, o que significa que as vezes pode não proteger os sistemas contra os riscos menos críticos.

Fernandes (2021), cita que, caso informações cruciais caírem em mãos erradas, afetarão toda a funcionalidade dos negócios. Um exemplo simples: Imagine que uma empresa sofra um ataque, onde ocorre a exposição de números de cartões de créditos dos clientes. Uma grande falha como essa poderá gerar ações judiciais por parte dos prejudicados pelo vazamento dos dados.

O principal objetivo da segurança da informação é proteger os dados físicos e digitais de todas as empresas, pois um ataque pode colocar todos os seus dados confidenciais em risco, podendo até mesmo levar as empresas em falência e processos judiciais.

4.1 O que é um ataque cibernético?

Segundo a Kaspersky, um ataque cibernético é uma tentativa de ataque a servidores, computadores, sistemas eletrônicos e dispositivos móveis. O termo abrange uma série de métodos, como o malware, a injeção SQL2 (*Structured Query Language*) e *phishing*. (BALDISSERA, 2021).

As ameaças podem ser divididas em três tipos, de acordo com o objetivo:

- **Crime virtual:** cibercriminosos buscam ganhos financeiros com o ataque.
- **Ataque cibernético:** indivíduos ou grupos de hackers realizam ataques por motivação política.
- **Terrorismo cibernético**: causar pânico ou medo é o objetivo dos ataques hackers.

Esses crimes se tornaram o tipo de ameaça virtual mais comum durante o período de pandemia, o que ocasionou uma alta demanda de profissionais de TI especializados em *Cybersecuriyt*[2]. Outra profissão que aumentou nesse período foi a arquitetura de software,

[2]*Cybersecuriyt* diz respeito à proteção da rede e infraestrutura corporativa, são as camadas externas de proteção que estão preocupadas em proteger o principal ativo das empresas, os dados e informações.

uma área que também é fundamental para oferecer segurança aos dados das empresas e consumidores, (BALDISSERA, 2021).

4.2 Tipos de ataques cibernéticos

Existe várias formas de se realizar um ataque cibernético, podem ser contra as empresas ou até mesmo pessoas físicas e jurídicas que utilizam meios sociais. Há inúmeras formas de se destacar os tipos de ataques, nesse artigo está presente dentre as inúmeras formas, apenas duas formas de se realizar ataques cibernéticos, sendo eles: *Phishing* e *ZeroDay*.

4.2.3 Phishing

Quase sempre realizado via e-mail, o *phishing* é um ataque virtual no qual os hackers estimulam os usuários a revelarem informações sigilosas, incluindo senhas, dados bancários e números de documentos, (ZIMMER, 2020)

Esse tipo de ataque é bem elaborado e leva o usuário a uma página web idêntica a página verdadeira de um site oficial, como um site de uma agência bancária, por exemplo. Assim, os hackers "pescam" as informações importantes dos usuários. Esse ataque é um dos ataques mais comuns e que possuírem mais sucessos nas tentativas, (ZIMMER, 2020).

4.4.4 ZeroDay

Geralmente conhecido como "dia zero", o *ZeroDay* é um ataque que busca falhas de segurança em aplicativos ou programas recém-lançados, em que são capazes de explorar brechas e bugs antes de que eles sejam corrigidos. Esse ataque é um ataque menos comum, pois é caracterizo a lançamentos de novidades no meio digital, (ZIMMER, 2020).

5. COMO A INTELIGÊNCIA ARTIFICIAL E A SEGURANÇA CIBERNÉTICA TRABALHAM JUNTAS

A grande capacidade de aprendizagem da máquina e dos sistemas de Inteligência Artificial em assumir muitas das tarefas que são realizadas por humanos terá um papel significativos na crescente demanda por habilidade em segurança cibernética, (MANKY, 2020).

Um dos objetivos em adquirir uma estratégia de inteligência artificial focada na segurança é desenvolver um sistema que seja imunológico para a rede semelhante ao corpo humano. No corpo humano, os glóbulos brancos são resgatados quando um problema ocorre, agindo assim de forma autônoma no combate a infecção. Na rede, a Inteligência Artificial pode executar a mesma tarefa, assim identificando ameaças e iniciando rapidamente uma resposta, (MANKY, 2020).

Outro motivo para se utilizar a Inteligência Artificial em sistemas de segurança é que se espera que elas não cometam erros que são comidos por humanos ao realizarem tarefas, assim as ameaças serão respondidas de maneira eficaz e eficiente, (HACKERSEC, 2019).

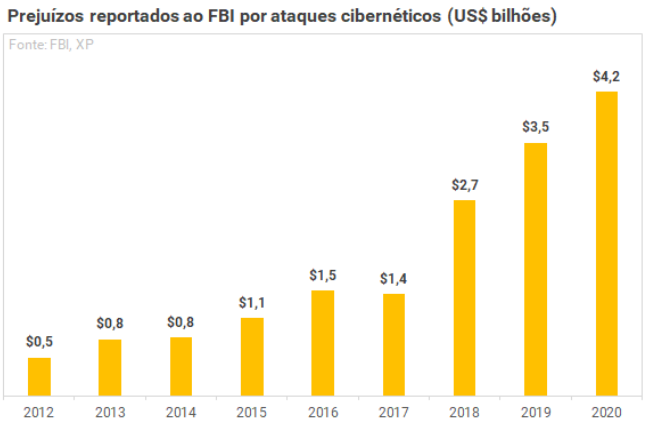
6. INTELIGÊNCIA ARTIFICIAL NAS EMPRESAS

Em 2020, pela primeira vez, os incidentes cibernéticos foram considerados a principal ameaça para as empresas ao redor do mundo, segundo o estudo Allianz Risk Barometer 2020. Sete anos antes, o assunto ocupava a 15ª colocação, (MANSUR, 2021).

Com o regime de home office adotado pelas empresas devido a pandemia do coronavírus o número de ameaças aumentou 394% de Janeiro a Novembro do ano de 2020, em comparação com 2019, de acordo com um levantamento da empresa Apura Cybersecurity, citou também, (MANSUR, 2021).

Segundo Bertolli (2019), os gastos com crimes cibernéticos estão aumentando e os custos que estão associados podem causar grandes problemas para as empresas que ignoraram. Por outro lado, o orçamento para a segurança cibernética está crescendo a medida em que as empresas percebem a importância e o valor desse investimento.

Gráfico 1 – Prejuizos reportados ao FBI por ataques cibernéticos

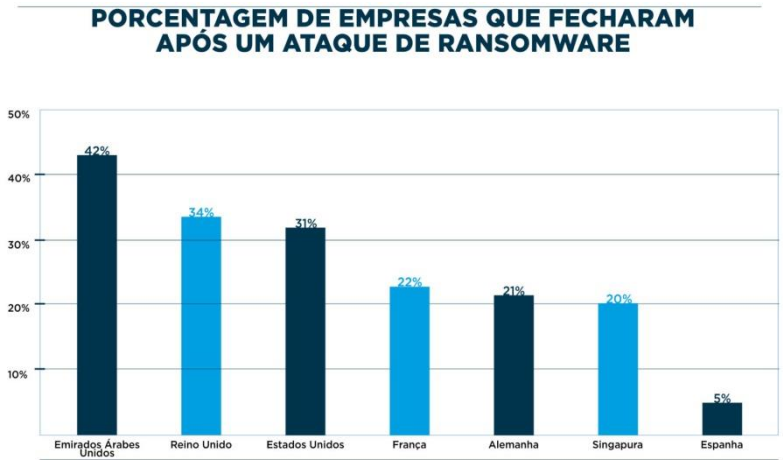


Fonte: *COE HACK: Segurança Cibernética - XP Investimentos (2021)*

No gráfico 1representa o grande aumento de prejuízos que foram reportados ao FBI (*Federal Bureau of Investigation* que significa "Departamento Federal de Investigação em português", devido ao grande aumento dos ataques cibernéticos em decorrer do avanço dos anos. Com isso destaca-se principalmente o quanto é importante investir na segurança da informação das empresas. O gráfico traz o grande prejuízo que as empresas vêm enfrentando a cada ano que se passa. No ano de 2012 começaram a ocorrer os grandes ataques cibernéticos, no ano de 2020 as empresas chegaram a um prejuízo de aproximadamente U$ 4 bilhões de dólares, isso demonstra o quanto o sistema de informação é fundamental para as empresas se protegerem de terríveis ataques cibernéticos.

Segundo Goulart (2021), uma pesquisa realizada pela Deloitte mostra que 41% das empresas já sofreram ataques cibernéticos e quase 90% optaram por realizar investimentos em segurança depois de ter sofrido ataque. As empresas que ainda não tiveram registros de ataques, 69% delas investem em segurança cibernética. Essa pesquisa foi realizada entre os meses de Fevereiro e Março com 122 empresas de diferentes setores.

Gráfico 2 – Porcentagem de empresas que fecharam após um ataque de *Ransomware*



Fonte: Forbes Tech (2021).

De acordo com o gráfico 2, o mesmo representa da porcentagem de empresas que vieram a decretar a falência após sofrerem um ataque hacker, conhecido como '*Ransomware*'. Além disso, também podemos analisar que o país que mais sofreu com esse tipo de ataque foi o Emirados Arabes Unidos, com 42% de empresas que chegaram a falência.

O Reino Unido é o segundo pais mais afeteado pela prática de Ransomware, com 34% de empresas que decretaram a falência mas não deixando muito atrás o pais dos Estados Unidos que também sofreu com esse tipo de ataque tendo 31% das empresas falidas. Na França, Alemanha e Singapura os ataques foram menores comparados aos paises anteriores, mas ainda sim sofreram com este tipo de ataque, ficando na faixa de 20% a 22%. O menor número de ataques registrando foi na Espanha, com apenas 5%. Com isso, é possivel perceber o quão importante a segurança informação e dos dasos é para o todo de uma organização, sendo ela pequena, média ou de grande porte, pois se uma organização não possui alguma ferramenta de segurnaça da informação a sua chance de ir a falencia cresce a cada dia.

6.1 Ferramentas que utilizam a Inteligencia Artificial como forma de proteção

Várias organizaões estão empregando inteligência artificial em suas estratégias de compliance para entrarem em conformidade com a Lei Geral de Proteção de Dados, (REVOREDO, 2021).

Nas áreas de segurança e vigilância, a utilização de algoritmos inteligentes e redes neurais permitiu que os sistemas realizassem identificações mais precisas. Um exemplo

popularmente conhecido é o reconhecimento facial, ele permite a identificação automática das características das pessoas, tambem sendo indispensavel para o reconhecimento de placas de veículos e possui a capacidade para detecão de situações de perigo, (VEOLINK, 2021).

Tambem tem se usado a inteligência artificial via NLP (Natural Language Processing), com a finalidade de ajudar a organização a entender o significado de seus contratos legais em determinado contexto (como no contexto da LGPD), analisando as cláusulas dentro do contrato em relação a outros documentos corporativos. (REVOREDO, 2021).

Outra ferramenta que começou a utilizar a Inteligencia Artificial a seu favor é o antivirus. Segundo o site oficial da Avast, consta que o sistema de inteligencia artificial usa a maquina para extrair dados de toda a base de usuarios e depois treina cada módulo de segurança. Assim, ao descobrir uma nova amostra de malware, os produtos AVAST são atualizados automaticamente com identificadores providenciando assim a proteção atualizada, (AVAST, 2021).

7 VANTAGENS E DESVANTAGENS DE UTILIZAR A INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA CIBERNÉTICA

Apesar da Inteligência Artificial na Segurança Cibernética ser de extrema importância para o todo de uma organização se manter no mercado de trabalho, é possível verificar que possui alguns pontos principais nos quais impedem que esse tipo de tecnologia seja adotado por todo e qualquer tipo de organização.

7.1 Vantagens de se utilizar a Inteligência artificial na Segurança Cibernética

Uma das principais vantagens quando falamos em Inteligência Artificial é que ela atua 24 horas por dia, monitorando e emitindo alertas, mantendo a qualidade da segurança da organização.

Além de reduzir falhas, trabalhos repetitivos e de otimizar processos a inteligência artificial influencia para a tomada de decisão que seja mais assertiva, pois a decisão é realizada a partir dos dados levantados, (TEIXEIRA, 2021).

7.2 Desvantagens de se utilizar a Inteligência artificial na Segurança Cibernética

Apesar da Inteligência Artificial possuir algumas desvantagens, essas não superam as vantagens que a tecnologia pode trazer para a nossa evolução como sociedade, (MARGOTTI, 2021).

Podemos ressaltar também que é preciso ter profissionais extremamente qualificados para lidar com esse tipo de tecnologia adequadamente, sabendo lidar com qualquer ocorrência que aparecer.

É necessário a aquisição de máquinas e equipamentos independente do nível de inteligência integrada, pois elas demandam reparos e manutenções que podem ter custos bem elevados, (MARGOTTI, 2021).

Apesar da Inteligência Artificial ser uma ótima aliada para a Segurança da Informação, ela demanda tempo para se adequar e possui dificuldade para inovar. Como o aprendizado é contínuo e progressivo é preciso tempo até que a base de dados esteja completamente adequada para iniciar o trabalho na organização.

8. CONCLUSÃO

Com o decorrer dos anos, o aumento nos números de incidentes a ataques cibernéticos nas organizações mostra que manter as informações seguras é um desafio, apesar do surgimento das leis de segurança para combater os crimes cibernéticos, os ataques estão se tornando cada vez mais recorrentes. Em virtude disso, as empresas passaram a ter um olhar mais crítico em relação a segurança da informação, resultando no grande aumento de empresas que começar a utilizar a Inteligência Artificial na Segurança Cibernética com o intuito de diminuir os ataques mal-intencionados e assim reforçar a segurança da informação.

A utilização da Inteligência Artificial na Segurança da Informação está sendo cada vez mais procurada pelas organizações para prevenir e combater os ataques *hackres*. Com esse estudo concluímos que a Inteligência Artificial está sendo cada vez mais utilizada para auxiliar e prevenir esses ataques. Apesar do seu alto custo as organizações estão cada vez mais a procura desta ferramenta para manter suas informações em segurança e se manter ativa no mercado de trabalho.

REFERÊNCIAS

BEAL, Adriana. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2008. 175 p.

FERNANDES, Anita Maria da Rocha. Inteligência artificial: noções gerais. Florianópolis: Visual Books, 2003.

COSSETTI, Melissa. **O que é inteligência artificial.** Disponível em: :<https://tecnoblog.net/responde/o-que-e-inteligencia-artificial/>. Acesso em: 12 de Agosto de 2021.

PIMENTA, Igor. **Inteligência Artificial: o que é, conceito e métodos de IA.** Disponível em: <https://www.take.net/blog/tecnologia/inteligencia-artificial/> Acesso em: 15 de Agosto de 2021.

GAIDARGI, Juliana. **Segurança da Informação. O que faz? Para que serve?**. Disponível em: <https://www.infonova.com.br/artigo/seguranca-da-informacao-o-que-faz-para-que-serve/> Acesso em: 15 de Agosto de 2021

ZEFERINO, Denis. **O que é Segurança da Informação e qual sua importância?**. Disponível em: <https://www.certifiquei.com.br/seguranca-informacao/> Acesso em: 16 de Agosto de 2021

FERNANDES, Mirian. **Tudo sobre Segurança Cibernética**. Disponível em: <https://blog.starti.com.br/tudo-sobre-seguranca-cibernetica/> Acesso em: 16 de Agosto de 2021

SCHULTZ, Felix. **Segurança Cibernética: o que é e como ser um especialista no assunto**. Disponível em: <https://blog.milvus.com.br/seguranca-cibernetica-o-que-e/> Acesso em: 18 de Agosto de 2021

GUIDO, Leandro. **O que é a Segurança Cibernética? (Cyber Security)**. Disponível em: <https://www.cobracorps.com.br/o-que-e-seguranca-cibernetica-cyber-security/> Acesso em: 18 de Agosto de 2021

BALDISSERA, Olívia. **Os maiores ataques cibernéticos de 2021 (até agora).** Disponível em: <https://posdigital.pucpr.br/blog/ataques-ciberneticos> Acesso em: 20 de Agosto de 2021

ZIMMER, Kelvin. **8 tipos de ataques cibernéticos e como se proteger.** Disponível em: <https://www.lumiun.com/blog/8-tipos-de-ataques-ciberneticos-e-como-se-proteger/> Acesso em: 20 de Agosto de 2021

MANKY, Derek. **O uso da inteligência artificial e a segurança cibernética.** Disponível em: <https://itforum.com.br/noticias/o-uso-da-inteligencia-artificial-e-a-seguranca-cibernetica/> Acesso em: 20 de Agosto de 2021.

O PAPEL da inteligência artificial na segurança cibernética. HACKERSEC, 2021. Disponível em: <https://hackersec.com/o-papel-da-inteligencia-artificial-na-seguranca-cibernetica/> Acesso em: 25 de Agosto de 2021.

MANSUR, Rafaela. **Ameaças cibernéticas crescem 394% durante a pandemia.** Disponível em: <https://www.otempo.com.br/economia/ameacas-ciberneticas-crescem-394-durante-a-pandemia-1.2434524> Acesso em: 4 de Setembro de 2021

BERTOLI, Emilia. **Conheça as principais estatísticas em segurança digital para 2020**. Disponível em: <https://blog.varonis.com.br/conheca-as-principais-estatisticas-em-seguranca-digital-para-2020/> Acesso em: 8 de Setembro 2021

COE HACK: Segurança Cibernética. EXPERT XP, 2021. Disponível em: <https://conteudos.xpi.com.br/coe/relatorios/coe-hack-seguranca-cibernetica/> Acesso em: 4 de Setembro de 2021.

GOULART, Josette. **Pesquisa mostra que 41% das empresas brasileiras sofreram ataques hackers**. Disponível em: <https://veja.abril.com.br/blog/radar-economico/pesquisa-mostra-que-41-das-empresas-brasileiras-sofreram-ataques-hackers/> Acesso em: 10 de Setembro de 2021.

ATAQUES de ransomwares podem provocar fechamento de mais de 30% dos negócios em alguns países. FORBES, 2021. Disponível em: <https://forbes.com.br/forbes-tech/2021/07/ataques-de-ransomwares-podem-provocar-fechamento-de-mais-de-30-dos-negocios-em-alguns-paises/> Acesso em: 15 de Setembro de 2021.

REVOREDO, Tatiana. **O papel da inteligencia artificial na cibersegurança**. Disponivel em: <encurtador.com.br/djtI0>. Acesso em: 10 de Maio de 2022.

CRESCE o uso de inteligência artificial em segurança eletrônica. VEOLINK, 2021. Disponível em: <encurtador.com.br/nrCE4 >. Acesso em: 10 de Maio de 2022.

INTELIGENCIA artificial e aprendizagem de máquina. AVAST, 2021. Disponivel em: <https://www.avast.com/pt-br/technology/ai-and-machine-learning#pc/>. Acesso em: 18 de Setembro de 2021.

TEIXEIRA, Thais. **As vantagens e desvantagens da inteligência artificial**. Disponível em: <https://izap.com.br/blog/as-vantagens-e-desvantagens-da-inteligencia-artificial/>. Acesso em: 25 de Outubro de 2021.

MARGOTTI, Anelise. **Você sabe quais são as vantagens e desvantagens da inteligência artificial? Descubra agora.** Disponível em: <https://rockcontent.com/br/blog/desvantagens-da-inteligencia-artificial/ > Acesso em: 10 de Novembro de 2021.