



**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO
TOCANTINS
CAMPUS ARAGUATINS
CURSO SUPERIOR DE LICENCIATURA EM COMPUTAÇÃO**

ROGÉRIO BANDEIRA DE SOUSA

**INTELIGÊNCIA ARTIFICIAL E SUA APLICAÇÃO EM SEGURANÇA
CIBERNÉTICA**

**ARAGUATINS – TO
2025**

ROGÉRIO BANDEIRA DE SOUSA

**INTELIGÊNCIA ARTIFICIAL E SUA APLICAÇÃO EM SEGURANÇA
CIBERNÉTICA**

Trabalho de Conclusão de Curso
apresentado à Coordenação do Curso de
Licenciatura em Computação, do Instituto
Federal de Educação, Ciência e Tecnologia
do Tocantins – Campus Araguatins, para a
obtenção do grau de Licenciado em
Computação.

Orientador: Prof. Me. Rogério Pereira de
Sousa.

**ARAGUATINS – TO
2025**

Dados Internacionais de Catalogação na Publicação (CIP)
Bibliotecas do Instituto Federal do Tocantins

S725i Sousa, Rogério Bandeira de
 Inteligência artificial e sua aplicação em segurança cibernética /
 Rogério Bandeira de Sousa. – Araguatins, TO, 2025.
 32 f.

Trabalho de Conclusão de Curso (Licenciatura em Computação)
– Instituto Federal de Educação, Ciência e Tecnologia do Tocantins,
Campus Araguatins, Araguatins, TO, 2025.

Orientador: Me. Rogério Pereira de Sousa

1. Inteligência artificial. 2. Segurança cibernética. 3. Tecnologia
da informação. I. Sousa, Rogério Pereira de. II. Título.

CDD 004

A reprodução total ou parcial, de qualquer forma ou por qualquer meio, deste documento é autorizada para fins
de estudo e pesquisa, desde que citada a fonte.

Elaborado pelo sistema de geração automática de ficha catalográfica do IFTO com os dados fornecidos
pelo(a) autor(a).



Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins
Campus Araguatins

FOLHA DE APROVAÇÃO

TÍTULO DO TRABALHO: INTELIGÊNCIA ARTIFICIAL E SUA APLICAÇÃO EM SEGURANÇA CIBERNÉTICA

AUTOR: ROGÉRIO BANDEIRA DE SOUSA

ORIENTADOR: Prof. M.e Rogério Pereira de Sousa

Trabalho de Conclusão de Curso apresentado ao Instituto Federal de Educação, Ciência e Tecnologia do Tocantins, *Campus Araguatins*, como parte das exigências para a conclusão do Curso de Licenciatura em Computação.

Aprovado em 25 de junho de 2025.

Prof. M.e Rogério Pereira de Sousa
Presidente da Banca

Profª. Esp. Juçara Kelly Coelho Sobrinho Galvão
Primeiro avaliador

Prof. Dr. Ramásio Ferreira Melo
Segundo avaliador



Documento assinado eletronicamente por **Ramasio Ferreira de Melo, Coordenador**, em 25/06/2025, às 21:03, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Juçara Kelly Coelho Sobrinho Galvão, Servidora**, em 25/06/2025, às 21:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Rogério Pereira de Sousa, Servidor**, em 04/07/2025, às 17:12, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.iftto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2821869** e o código CRC **AFF01547**.

AGRADECIMENTOS

Agradeço a Deus por ter me dado forças o suficiente para chegar até o final dessa caminhada. A minha mãe, pelo investimento, apoio e ensinamentos que me fizeram trilhar um caminho honesto e íntegro. Não poderia deixar de agradecer à minha noiva, Andressa Silvino, pelo apoio e pela ajuda em minha trajetória acadêmica. Ao meu orientador, Prof. Me. Rogério Pereira, pela paciência e dedicação para o rendimento deste trabalho. Sem esquecer, é claro, dos meus amigos de turma, que dividiram comigo preocupações, responsabilidades e também momentos alegres e descontraídos que serviram para nossa formação como profissionais qualificados.

RESUMO

A saber, o desenvolvimento de algoritmos de Inteligência Artificial foi impulsionado em meados da década de 50, ganhando abrangência nas mais diversas áreas, estimulado sobretudo pelo aumento da capacidade de processamento do conjunto de dispositivos que processam informações por meio de dispositivos eletrônicos. Assim, com o início do século XXI, o crescimento dessa capacidade impulsionou o desenvolvimento de vários sistemas. Vale dizer que grande parcela de empresas em escala mundial e instituições públicas passou a utilizar sistemas em nuvem aliados a sistemas de Inteligência Artificial. Para tanto, é nessa conjuntura que a segurança cibernética passa a ser fundamental, em decorrência do impulsionamento e desenvolvimento de novas tecnologias. Em vista disso, o presente trabalho tem como principal escopo apresentar uma análise acerca do atual cenário da Inteligência Artificial aplicada dentro da segurança cibernética, realizada por meio de uma revisão bibliográfica através do Google Acadêmico e do banco de dados da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior. Após uma vasta pesquisa e com o estudo realizado, entendemos que a I.A. possui um potencial transformador substancial para aprimorar a eficiência operacional, a adaptabilidade e a precisão de respostas em sistemas de controle em diversas áreas. Em nossa conclusão, elucidamos que, enquanto os benefícios da IA em sistemas de controle são amplos e promissores, a integração bem-sucedida e plena desses sistemas depende de avanços técnicos que contemplem segurança, confiabilidade e adequação ética. Logo, diversos setores vêm cada vez mais se beneficiando das soluções práticas que a IA oferece, potencializando melhorias jamais vistas antes.

Palavras-chaves: Inteligência artificial; Segurança cibernética; Tecnologia da informação.

ABSTRACT

The development of Artificial Intelligence (AI) algorithms began to gain momentum in the mid-1950s, expanding into various fields, mainly driven by the increased processing power of devices capable of handling large volumes of information. With the onset of the 21st century, this growth accelerated the development of multiple systems. A significant portion of global companies and public institutions began adopting cloud-based systems integrated with AI technologies. Within this context, cybersecurity has become a fundamental concern due to the advancement and expansion of emerging technologies. This study aims to analyze the current landscape of Artificial Intelligence applied to cybersecurity, based on a bibliographic review conducted through Google Scholar and the CAPES database. The research reveals that AI holds substantial transformative potential to enhance operational efficiency, adaptability, and the accuracy of response in control systems across various sectors. In conclusion, while the benefits of AI in control systems are vast and promising, successful integration depends on technical advancements that ensure security, reliability, and ethical compliance. Consequently, several industries are increasingly benefiting from the practical solutions AI provides, fostering unprecedented improvements.

Keywords: Artificial intelligence; Cybersecurity; Information technology.

SUMÁRIO

1. INTRODUÇÃO	9
1.1. Problema da Pesquisa	10
1.2. Justificativa.....	10
1.3. Objetivos	11
1.3.1. Objetivo Geral	11
1.3.2. Objetivos Específicos	11
2. REVISÃO DE LITERATURA.....	12
2.1.Segurança Cibernética: Definição e Desafios	16
3. PROCEDIMENTOS METODOLÓGICOS	19
Quadro 1 – Quantitativo da Pesquisa Bibliográfica	20
4. GESTÃO DE RISCOS RELACIONADOS À INTELIGÊNCIA ARTIFICIAL	21
5. AMEAÇAS CIBERNÉTICAS CONTEMPORÂNEAS	24
6. RESULTADOS E DISCUSSÃO	26
7. CONSIDERAÇÕES FINAIS	28
REFERÊNCIAS	31

1. INTRODUÇÃO

A Inteligência Artificial (IA) é um campo amplo que abrange diversas áreas, incluindo lógica, probabilidade, matemática, percepção, raciocínio, aprendizado e ação. Com o tempo, surgiram questionamentos sobre como entender e agir de forma inteligente. Indo além da compreensão das ações humanas, a IA busca criar máquinas inteligentes que possam reproduzir e auxiliar nas atividades do dia a dia.

Segundo Boechat (2022), a Inteligência Artificial continua sendo implementada na cibersegurança e para desenvolver tecnologias de ponta. Dessa maneira, para se ter um certo nível de desempenho aceitável, é necessário encontrar e adaptar-se contra a evolução de todas as ameaças dentro da rede. Isso mostra que os recursos avançados de defesa estão sendo utilizados cada vez mais, em maior número e com notável grau de relevância no atual cenário.

Conforme William Stallings (2014), uma boa segurança visa alcançar os objetivos de preservar a integridade, disponibilidade e a confidencialidade dos recursos de Sistemas da Informação. A saber, esses três componentes são chamados de coração da Segurança de Computadores. Os três garantem, respectivamente, que os dados sejam alterados apenas com autorização, que os serviços estejam sempre acessíveis a usuários autorizados e que as informações estejam protegidas contra acessos não autorizados.

A segurança cibernética, antes da aplicação de IA, não tinha a capacidade de reagir em tempo real. Os ataques teriam que ser descobertos dentro do sistema e, em seguida, seriam contornados e/ou resolvidos. Como o atual cenário exhibe ataques mais frequentes, sofisticados e distribuídos, vê-se necessária a implementação de uma IA para auxiliar o sistema de segurança.

O presente trabalho visa identificar o uso da tecnologia de Inteligência Artificial e sua aplicação em segurança cibernética. Nos seus objetivos específicos, buscamos mostrar o conceito de Inteligência Artificial e segurança cibernética. Dessa maneira, apresentaremos uma revisão bibliográfica de artigos que nos permitem ter uma vasta pesquisa versando sobre a segurança cibernética e a IA. A saber, a metodologia adotada para este trabalho será uma revisão bibliográfica.

1.1. Problema da Pesquisa

Diante da crescente complexidade e sofisticação dos ataques cibernéticos, e da limitação dos métodos tradicionais de segurança em responder a essas ameaças em tempo real, de que forma a aplicação da inteligência artificial pode contribuir para o fortalecimento da segurança cibernética, garantindo a integridade, confidencialidade e disponibilidade das informações?

1.2. Justificativa

A Inteligência Artificial não é apenas uma área de estudo da ciência da computação que busca criar sistemas capazes de fazer tarefas que, em suma, requerem inteligência humana; é também uma fonte de soluções práticas para desafios do mundo real. Com o crescimento da tecnologia, a I.A. tem se tornado cada vez mais comum em nosso cotidiano, desde assistentes virtuais até sistemas de segurança altamente poderosos.

A I.A. tem a capacidade de transformar diversos setores, desde as áreas da agricultura, saúde, educação, industrial até a área militar. Por meio da análise de grandes volumes de dados e do aprendizado decorrente deles, a I.A. pode facilitar a tomada de decisões e aumentar a eficiência nas mais diversas áreas. Dessa maneira, é importante apresentar as oportunidades e os obstáculos da I.A., examinando suas utilizações e consequências em diferentes contextos. Entendê-la melhor é essencial para se ter um melhor aproveitamento de suas vantagens e, de certa forma, minimizar possíveis perigos advindos dela.

Na agricultura, a Inteligência Artificial tem revolucionado a forma como os dados agrícolas são coletados, analisados e interpretados, podendo ser aplicada em diferentes tipos de dados, até mesmo nos advindos de sensores operando em campos ou em máquinas. O exemplo mais notório é o mapeamento por meio de imagens de drones em plantios de eucalipto. Esse tipo de operação permite a geração de resultados que possibilitam uma melhor tomada de decisão em relação aos modos convencionais.

Na saúde, a I.A. tem um vasto potencial de aplicações, desde o diagnóstico de doenças, tratamentos e até mesmo na gestão de recursos hospitalares, assim como no auxílio ao desenvolvimento de novos medicamentos.

Em ambientes militares, a I.A. é fundamental para identificar e neutralizar ameaças, otimizar treinamentos de oficiais, orientar aeronaves e veículos tripulados e não tripulados, coletar informações e realizar a cibersegurança dos locais militares.

Sendo uma área em contínua transformação, este estudo busca contribuir para elucidar a eficiência e a precisão da Inteligência Artificial na segurança cibernética. Através de uma análise minuciosa, pretendemos oferecer percepções relevantes sobre como a I.A. pode ser aplicada para aprimorar determinada área e solucionar problemas complexos.

1.3. Objetivos

1.3.1. Objetivo Geral

Realizar uma revisão bibliográfica para analisar como a inteligência artificial tem sido empregada no campo da segurança cibernética, com ênfase na sua contribuição para a proteção da integridade, confidencialidade e disponibilidade das informações em ambientes digitais.

1.3.2. Objetivos Específicos

- Levantar e analisar materiais acadêmicos e técnicos que abordem a aplicação da inteligência artificial em segurança cibernética.
- Identificar as principais formas como a IA tem sido utilizada para proteger dados e sistemas digitais.
- Compreender de que maneira a IA contribui para garantir a integridade, a confidencialidade e a disponibilidade das informações.
- Observar os avanços e desafios no uso da IA frente às ameaças cibernéticas cada vez mais sofisticadas.
- Refletir sobre os benefícios e limitações da inteligência artificial aplicada à cibersegurança com base nos estudos analisados.

2. REVISÃO DE LITERATURA

A Inteligência Artificial (I.A.) pode ser definida como um estudo de um agente que tem percepções de um ambiente e executa ações ensinadas de um humano para uma máquina inteligente, conforme destacado por Pereira e Magalhães (2021). Para tanto, na atualidade, cabe destacar que a utilização da Inteligência Artificial se propagou entre as mais variadas áreas da computação, onde existe uma promessa de grandes avanços através da utilização da I.A. e da cibersegurança. Amplamente utilizada em aplicações de Visão Computacional, permite aos profissionais de diversas áreas desenvolverem soluções eficazes.

Segundo Pires 2020, em termos históricos, aborda que a Inteligência Artificial tem seguido essas quatro linhas de pensamento distintas:

- I. Sistemas que pensam como seres humanos: "O novo e interessante esforço para fazer os sistemas pensarem como mentes, no sentido total e literal";
- II. Sistemas que atuam como seres humanos: "A arte de criar sistemas que executam funções que exigem inteligência quando executadas por pessoas";
- III. Sistemas que pensam de forma racional: "O estudo das faculdades mentais pelo seu uso de modelos computacionais";
- IV. E sistemas que atuam de forma racional: "A inteligência computacional é o estudo do projeto de agentes inteligentes".

Destarte, a I.A. pode ser empregada como um recurso para proteger as empresas contra potenciais ameaças. As mesmas analisam o empreendimento e observam se existem potenciais ameaças, para então buscarem as corretas providências, visando sanar atos de criminosos. A inteligência artificial oferece às empresas ferramentas avançadas para detectar, analisar e responder rapidamente a potenciais ameaças cibernéticas, minimizando riscos e fortalecendo a segurança organizacional de maneira proativa (RUSSELL; NORVIG, 2020, p. 682).

Dessa maneira, a I.A., através de softwares, é utilizada como ferramenta eficiente contra diversos crimes virtuais. Após um período de relativa descrença no meio científico, a I.A. ressurgiu como um campo promissor para a solução de uma variedade de problemas, com especial destaque para questões relacionadas à automatização de processos (BARRETO, 1999).

Figura 1 - Princípios básicos Segurança da Informação.



Fonte: <https://www.proviti.com.br/cybersecurity/pilares-seguranca-da-informacao/>

Nesse contexto, a IA emerge como uma ferramenta cada vez mais eficaz, proporcionando soluções inovadoras diariamente e auxiliando as empresas a reduzirem seus custos operacionais, bem como aprimorar a qualidade de seus produtos e serviços (BARRETO, 1999). A IA tem transformado significativamente o panorama dos sistemas de controle, introduzindo métodos e tecnologias que permitem sistemas mais autônomos, eficientes e adaptativos.

Outrossim, o objetivo da segurança da informação é garantir a continuidade dos negócios e minimizar os danos aos negócios, limitando o impacto de incidentes de segurança. Segurança da tecnologia da informação e comunicação (TIC) lida com a proteção da real tecnologia baseada em sistemas nos quais as informações são comumente armazenadas e/ou transmitidas. Se segurança cibernética é sinônimo de segurança da informação, seria razoável supormos que os incidentes de segurança cibernética também podem ser descritos em termos das características usadas para definir a segurança da informação. Assim, um incidente de segurança cibernética, por exemplo, também levaria a uma violação da confidencialidade, integridade ou disponibilidade de informação, que também são pilares que compõem a segurança da informação. Porém, existem ameaças de segurança cibernética que não fazem parte do âmbito da segurança da informação, como casos de cyberbullying e invasões de equipamentos IoT (BOECHAT, 2022, p. 6).

Com Tanenbaum (2007), entendemos que as informações guardadas dentro de empresas e organizações variam entre informações técnicas,

comerciais, financeiras ou legais. A maior parte das informações está guardada em computadores. Computadores domésticos também contêm dados que podem ser valiosos para atacantes, como informações pessoais, financeiras ou de caráter sigiloso.

BOECHAT (2022, p. 16) explica: confidencialidade é uma propriedade da política de segurança que normalmente se refere à proteção de informações e sistemas de partes não autorizadas. A ameaça de confidencialidade pode normalmente destinar-se a bancos de dados, servidores de aplicativos e administradores de sistema e pode ser considerada como “roubo de dados”. Integridade: evitar qualquer tipo de destruição ou modificação de informações por terceiros não autorizados. A ameaça de integridade normalmente inclui ameaças relacionadas a finanças, como alterar dados financeiros, roubar dinheiro, redirecionar depósitos e danos à confiabilidade da organização, podendo ser considerada como “alteração de dados”. Disponibilidade: garantir o acesso de sistemas de informação ou ativos para uma parte autorizada ou entidade de forma confiável e tempestiva. A ameaça de disponibilidade normalmente inclui negação de serviço ou destruição, e pode ser considerada como “negação de acesso de dados”.

A segurança cibernética começou em um momento em que não havia necessidade de desenvolver técnicas destinadas a melhorar a segurança do ambiente digital e de seus ativos. A princípio, até meados dos anos 90, o número de computadores pessoais presentes nas casas dos cidadãos comuns era mínimo, e a maioria dos computadores estava em sociedades, universidades e outras organizações. A maioria dessas máquinas era isolada em seu próprio ambiente, desconectado de qualquer rede.

Seguindo adiante, a chegada da transformação digital nas organizações fez surgir diferentes forças de inovação, dentre as quais se destaca a Inteligência Artificial. Não obstante, merecem menção a Cloud Computing, a Big Data e a Robótica. Assim, é fundamental considerar cada uma dessas tecnologias, reconhecendo suas forças inovadoras e vulnerabilidades na área cibernética (CRUZ, 2021).

Novos avanços são feitos no campo de TI quase que diariamente. Com isso, observamos também que, devido ao alto grau de utilização de tecnologias conectadas, setores não focados em segurança de dados também sofrem com vazamentos e intrusões, gerando custos.

Devido ao crescimento dos ataques cibernéticos e à grande multiplicação de dispositivos atualmente, a IA assume papel de destaque no auxílio ao combate de atos de cibercriminosos, automatizando a detecção de ameaças e respondendo com mais eficácia e rapidez do que as técnicas convencionais, orientadas por software ou manuais.

Em um ambiente cada vez mais digitalizado, com o aumento do uso de tecnologias como a nuvem e a inteligência artificial, a segurança cibernética tornou-se essencial para garantir que dados pessoais, empresariais e

governamentais não sejam comprometidos. De acordo com o especialista em cibersegurança Bruce Schneier, “A segurança cibernética é uma área de crescente importância e complexidade. Ela não se resume apenas a ferramentas ou a protocolos, mas exige uma abordagem integrada, que envolva políticas públicas, educação, conscientização e treinamento para todos os envolvidos” (SCHNEIER, 2018, p. 23).

A segurança cibernética envolve a implementação de diversas tecnologias, como firewalls, antivírus e criptografia, que trabalham em conjunto para proteger as informações armazenadas em sistemas de computadores e redes. A conformidade com legislações, como a Lei Geral de Proteção de Dados (LGPD), no Brasil, também tem se mostrado crucial para garantir a privacidade dos usuários e a segurança das informações pessoais, enfrentando diversos desafios no cenário atual. Segundo Bishop (2018), a adoção de IA em ambientes corporativos exige planejamento estratégico.

Além disso, a escassez de profissionais qualificados em segurança cibernética é uma preocupação crescente. Segundo o relatório da (ISC)² de 2021, “A falta de profissionais qualificados em segurança cibernética é um dos maiores obstáculos enfrentados pelas empresas na implementação de suas estratégias de proteção. A escassez de talento nesse campo é um desafio que não deve ser subestimado” (ISC, 2021, p. 18). A rápida evolução das tecnologias exige um conhecimento especializado que nem sempre acompanha o ritmo das ameaças, tornando difícil a atualização constante dos profissionais.

Muitas organizações subestimam a importância da segurança cibernética até sofrerem um ataque, resultando em uma preparação inadequada e respostas reativas, em vez de proativas. Para garantir a proteção contra essas ameaças, é fundamental que as empresas adotem medidas preventivas e treinamentos contínuos para suas equipes de TI e todos os colaboradores.

A governança de segurança da informação é essencial para garantir que as políticas e práticas de segurança estejam alinhadas com os objetivos estratégicos da organização. Como bem explica a Wikipedia, “a governança de segurança da informação envolve o estabelecimento de políticas, processos e controles que garantam que os dados e sistemas da organização estejam protegidos contra riscos e ameaças, enquanto se promove o alinhamento com as metas e valores corporativos.”

Uma governança eficaz envolve a implementação de controles de acesso, monitoramento constante e a capacidade de resposta a incidentes. De acordo com o especialista em governança Chris Moschovitis, “A segurança da informação não é uma responsabilidade isolada, mas sim uma responsabilidade corporativa que envolve todos os níveis da organização, desde a alta gestão até os funcionários de linha de frente. Uma política de segurança robusta deve ser claramente definida e comunicada, garantindo que todos os membros da organização estejam cientes das suas responsabilidades em relação à proteção da informação” (MOSCHOVITIS, 2019, p. 56). Além disso, deve-se garantir que as políticas de segurança sejam comunicadas e compreendidas por todos os membros da organização, promovendo uma cultura de segurança. A segurança não pode ser vista apenas como uma função de TI, mas como parte integral da estratégia organizacional.

2.1. Segurança Cibernética: Definição e Desafios

A segurança cibernética tornou-se um dos principais desafios da sociedade contemporânea, à medida que indivíduos, empresas e governos se tornam cada vez mais dependentes da tecnologia digital. Segundo Stallings (2019), a segurança cibernética pode ser definida como o conjunto de práticas, tecnologias e processos projetados para proteger redes, dispositivos, programas e dados contra ataques, danos ou acesso não autorizado. Essa definição reflete a complexidade do tema e destaca a necessidade de abordagens multidimensionais para sua efetiva implementação.

Nos últimos anos, a frequência e sofisticação dos ataques cibernéticos cresceram exponencialmente. Ataques como ransomware, phishing, negação de serviço (DDoS) e engenharia social são cada vez mais comuns e afetam desde pequenas empresas até grandes corporações e órgãos públicos (Oliveira & Veronese, 2017). Esses ataques comprometem não apenas dados sensíveis, mas também a continuidade operacional das organizações, o que torna a segurança da informação uma prioridade estratégica.

De acordo com Whitman e Mattord (2021), uma política de segurança bem estruturada é essencial para mitigar os riscos associados ao ambiente digital. Essa política deve abranger aspectos técnicos, como o uso de firewalls e criptografia, mas também elementos humanos e organizacionais, como treinamento de usuários e protocolos de resposta a incidentes. Essa visão

holística é fundamental para lidar com ameaças que evoluem constantemente.

A engenharia social, por exemplo, é um tipo de ataque que explora vulnerabilidades humanas em vez de falhas técnicas. Conforme Mitnick e Simon (2002), o elo mais fraco na cadeia da segurança da informação é frequentemente o usuário final, o que reforça a importância da conscientização e da educação em cibersegurança. Programas de capacitação contínuos são recomendados para minimizar a exposição a riscos causados por erro humano.

Além disso, o crescimento da Internet das Coisas (IoT) amplia ainda mais a superfície de ataque. Dispositivos conectados, muitas vezes, não possuem mecanismos robustos de segurança, o que os torna alvos fáceis para invasores. Para Gollmann (2011), a segurança em ambientes distribuídos e integrados requer soluções específicas, que vão desde o desenvolvimento seguro até atualizações periódicas de firmware.

As legislações também desempenham um papel importante na proteção do ciberespaço. No Brasil, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) estabelece diretrizes claras sobre o tratamento de dados pessoais, impondo obrigações às organizações que lidam com essas informações. Segundo Doneda (2021), a LGPD representa um avanço significativo no alinhamento do país com padrões internacionais de privacidade e segurança da informação.

Outra abordagem emergente é o uso de inteligência artificial e aprendizado de máquina para detectar padrões anômalos e prever ataques antes que causem danos. Segundo Bishop (2018), sistemas de detecção baseados em IA podem ser mais eficazes do que soluções tradicionais, desde que bem treinados e atualizados constantemente. Moura et al. (2020) reforçam que o uso de aprendizado de máquina tem se mostrado eficaz na detecção de ataques zero-day, que não são identificáveis por assinaturas convencionais.

Contudo, apesar dos avanços tecnológicos, a cultura organizacional ainda representa um dos maiores obstáculos à efetiva implementação da segurança cibernética. Conforme Rezende (2018), muitas organizações investem em tecnologia, mas negligenciam fatores culturais e de governança, o que compromete a eficácia das medidas adotadas. Gomes e Silva (2019) ressaltam que a segurança da informação deve estar incorporada à cultura

organizacional e ao planejamento estratégico, e não apenas como uma questão técnica isolada.

A cooperação internacional também se mostra essencial diante da natureza transnacional dos crimes cibernéticos. Para Valeriano e Maness (2015), a cibersegurança não pode ser tratada apenas como um problema local, exigindo uma abordagem coordenada entre países para o compartilhamento de informações, padrões e práticas. Nesse contexto, Silva et al. (2021) argumentam que a diplomacia cibernética tem se tornado um instrumento relevante na mediação de conflitos no ciberespaço e na construção de acordos multilaterais.

Além disso, o crescimento do trabalho remoto, impulsionado pela pandemia de COVID-19, trouxe novos desafios à segurança digital. Segundo Cruz et al. (2021), o aumento da conectividade fora dos perímetros tradicionais das redes corporativas intensificou a exposição a vulnerabilidades, exigindo novas estratégias de proteção, como redes privadas virtuais (VPNs) e autenticação multifatorial.

Segundo Amorim (2020), é importante reconhecer que a segurança cibernética não é um estado final, mas um processo contínuo de adaptação e aprimoramento. O dinamismo das ameaças exige uma postura proativa e resiliente por parte das organizações e indivíduos, com foco em prevenção, resposta e recuperação. Além disso, para Araújo e Almeida (2020), a formação de profissionais especializados e a pesquisa acadêmica são pilares essenciais para o avanço sustentável da cibersegurança.

Por fim, ainda é preciso fortalecer a integração entre as áreas de tecnologia e gestão dentro das organizações. De acordo com Laudon e Laudon (2020), a segurança da informação deve ser parte integrante da governança de TI, promovendo alinhamento entre objetivos de negócio e proteção digital.

3. PROCEDIMENTOS METODOLÓGICOS

Este trabalho foi desenvolvido com base em uma pesquisa qualitativa de cunho exploratório, com o objetivo de investigar a aplicação da Inteligência Artificial (IA) na segurança cibernética. Para isso, foi realizada uma revisão bibliográfica sistemática, fundamentada em fontes acadêmicas confiáveis.

As bases e repositórios utilizados para a coleta dos materiais foram:

- **Google Scholar (Google Acadêmico)**
- **SciELO (Scientific Electronic Library Online)**
- **IEEE Xplore Digital Library**
- **Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES)**

As buscas foram conduzidas no período de abril a junho de 2025, utilizando os seguintes descritores:

"Inteligência Artificial" e "Segurança Cibernética" (combinados em português e, quando aplicável, em inglês: "Artificial Intelligence" and "Cybersecurity").

Foram definidos os seguintes critérios de inclusão:

- **Publicações entre 2015 e 2024;**
- **Textos completos e gratuitos;**
- **Trabalhos acadêmicos revisados por pares (artigos, dissertações e teses);**
- **Conteúdos que abordassem diretamente a aplicação da IA na segurança cibernética.**

Critérios de exclusão:

- **Artigos duplicados entre bases;**
- **Notícias, textos de opinião e publicações sem rigor acadêmico;**
- **Trabalhos que mencionassem IA ou segurança cibernética apenas de forma superficial.**

Após a triagem e aplicação dos critérios, os dados foram organizados e analisados de maneira qualitativa, a fim de identificar tendências, benefícios, limitações e perspectivas futuras da aplicação da IA na segurança digital.

Quadro 1 – Quantitativo da Pesquisa Bibliográfica

Base de Dados	Artigos Encontrados	Artigos Seleccionados	Palavras-chave Utilizadas
Google Scholar	99	18	"Inteligência Artificial" e "Segurança Cibernética"
SciELO	30	8	"Inteligência Artificial" e "Segurança Cibernética"
IEEE Xplore	183	17	"Artificial Intelligence" AND "Cybersecurity"
Portal de Periódicos CAPES	70	20	"Inteligência Artificial" e "Segurança Cibernética"
Total	382	63	

Destarte, inicialmente esse estágio nos auxilia significativamente, uma vez que visa nos apresentar se já existe uma base científica sobre o tópico da pesquisa planejada, contribuindo assim para a escolha do problema a ser abordado e a seleção de uma metodologia apropriada.

Tudo isso é realizado com base nos estudos já divulgados. A pesquisa bibliográfica desempenha um papel fundamental na estruturação da pesquisa científica, uma vez que nos proporciona uma compreensão mais aprofundada do fenômeno que está sob investigação. (Sousa, 2021).

4. GESTÃO DE RISCOS RELACIONADOS À INTELIGÊNCIA ARTIFICIAL

A inteligência artificial tem se consolidado como uma das tecnologias mais disruptivas da atualidade, transformando diversos setores da sociedade, como saúde, finanças, indústria e serviços. Sua capacidade de realizar tarefas complexas, aprender com grandes volumes de dados e tomar decisões autônomas oferece um vasto potencial de inovação e melhoria da eficiência operacional. No entanto, a implementação de sistemas de IA não está isenta de riscos. Esses riscos podem variar desde falhas técnicas até questões éticas, regulatórias e de segurança, os quais precisam ser adequadamente geridos para evitar danos significativos a indivíduos, empresas e à sociedade como um todo.

Os riscos relacionados à IA podem ser classificados em diferentes categorias, com implicações diretas nos processos de gestão de riscos. Conforme destacado por Russell e Norvig (2016), a IA pode ser associada a uma série de desafios técnicos e éticos, que incluem a confiabilidade dos sistemas, a privacidade dos dados e os impactos sobre o mercado de trabalho. A utilização de IA em áreas sensíveis, como a saúde e a segurança pública, pode apresentar consequências significativas se os sistemas falharem ou forem manipulados de maneira inadequada. Binns (2018) enfatiza que os sistemas de IA devem ser projetados e gerenciados de maneira a garantir que suas decisões sejam compreensíveis e justificáveis, evitando que se tornem "caixas-pretas" que dificultam a responsabilização e o controle por parte dos gestores.

Segurança cibernética é outro ponto crítico. Sistemas de IA são vulneráveis a ataques de hackers que podem explorar suas fraquezas, manipulando os algoritmos ou os dados com os quais a IA opera. Sharma (2020) argumenta que a proteção dos dados utilizados em sistemas de IA é um dos maiores desafios, já que os dados são fundamentais para o treinamento dos modelos. A violação de dados pode comprometer a privacidade dos usuários e resultar em danos financeiros e reputacionais para as organizações. Assim, a gestão de riscos relacionada à segurança cibernética deve ser uma prioridade, garantindo que as medidas de proteção sejam robustas e eficazes.

Os riscos éticos são outra dimensão importante na gestão de IA. A implementação de IA em processos decisórios, como na seleção de

candidatos para vagas de emprego ou na determinação de penas judiciais, levanta questões sobre justiça, transparência e viés algorítmico. O'Neil (2016), em seu livro *Weapons of Math Destruction*, descreve como os algoritmos podem reforçar desigualdades sociais e discriminar certos grupos, caso não sejam devidamente monitorados e auditados. Para Bryson (2018), a IA precisa ser projetada de forma a garantir que as decisões automatizadas respeitem princípios éticos fundamentais, como a equidade e a responsabilidade.

No contexto regulatório, a falta de uma legislação global unificada sobre IA representa um risco significativo. Calo et al. (2019) afirmam que, enquanto alguns países estão avançando na criação de regulamentações específicas para a IA, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, outros ainda carecem de uma estrutura jurídica clara. A gestão de riscos regulatórios exige, portanto, que as organizações estejam atentas às diferentes exigências legais nos mercados em que atuam, adaptando suas práticas e processos de acordo com a legislação local e internacional.

A gestão de riscos na implementação da IA envolve a adoção de uma série de estratégias para mitigar os riscos identificados, garantindo que os benefícios da IA sejam aproveitados sem comprometer a segurança, a ética e a confiança do público. Uma das primeiras etapas nesse processo é a avaliação contínua dos riscos associados à IA. De acordo com Aven (2015), a avaliação de riscos deve ser dinâmica e flexível, já que as tecnologias de IA estão em constante evolução, assim como os desafios e as ameaças que as acompanham. A adoção de métodos de auditoria e monitoramento de sistemas de IA é essencial para garantir que os modelos estejam funcionando de maneira eficaz e sem gerar resultados indesejados.

Além disso, as empresas devem estabelecer políticas claras de governança de dados e de responsabilidade. Isso inclui garantir que os dados utilizados para treinar os algoritmos sejam de alta qualidade, representativos e livres de vieses. A implementação de práticas de transparência algorítmica também é crucial. Diakopoulos (2016) argumenta que a explicabilidade dos algoritmos deve ser uma prioridade, permitindo que as decisões tomadas pelos sistemas de IA possam ser auditadas e compreendidas pelas partes interessadas, incluindo consumidores, reguladores e acionistas.

Outra abordagem importante é o design ético de IA. De acordo com

Floridi (2019), as organizações devem adotar princípios de design que integrem considerações éticas desde a fase inicial de desenvolvimento da IA. Isso pode incluir a aplicação de testes rigorosos para identificar e mitigar potenciais vieses antes que o sistema seja implantado em um ambiente real.

A liderança é fundamental para garantir que a gestão de riscos relacionada à IA seja tratada de maneira adequada em todas as organizações. Luger (2019) argumenta que os gestores e líderes devem ser treinados para entender os riscos da IA e como supervisioná-la de forma ética e responsável. A criação de comitês de governança de IA, compostos por profissionais de diferentes áreas, como tecnologia, direito e ética, é uma prática recomendada para garantir que as decisões relacionadas à IA estejam alinhadas com os valores organizacionais e as normas regulatórias.

Além disso, as organizações devem estar cientes da importância de um plano de contingência robusto para lidar com falhas ou crises relacionadas à IA. Siau e Wang (2020) destacam que os planos de resposta a incidentes devem ser preparados com antecedência, contemplando a identificação rápida de problemas e a implementação de soluções para mitigar os danos.

A gestão de riscos relacionados à inteligência artificial é uma tarefa complexa, que exige a combinação de práticas de segurança, ética, regulamentação e governança. A IA oferece enormes benefícios, mas também traz desafios significativos, desde riscos técnicos até questões sociais e éticas. Para garantir que os sistemas de IA sejam implementados de maneira segura e eficaz, é essencial que as organizações adotem uma abordagem proativa e abrangente para a gestão de riscos, com a implementação de processos contínuos de avaliação, monitoramento e governança.

5. AMEAÇAS CIBERNÉTICAS CONTEMPORÂNEAS

As ameaças cibernéticas evoluíram consideravelmente nas últimas décadas, impulsionadas pela crescente digitalização das sociedades e pela sofisticação das técnicas dos atacantes. Segundo Amorim (2020), essas ameaças representam riscos significativos à integridade, confidencialidade e disponibilidade dos sistemas de informação. As organizações e os governos enfrentam o desafio constante de identificar, compreender e mitigar essas ameaças em tempo real.

Entre as ameaças mais recorrentes, destacam-se os ataques de ransomware, que bloqueiam o acesso aos dados da vítima mediante o pagamento de resgate. Conforme relata Stallings (2019, p. 251), esse tipo de ataque explora vulnerabilidades em sistemas desatualizados e na falta de políticas de backup. Um exemplo notório é o ataque WannaCry, que afetou centenas de milhares de computadores em 2017 e gerou prejuízos bilionários.

Outra ameaça crescente é o phishing, uma técnica de engenharia social que visa enganar o usuário para roubo de credenciais ou instalação de malware. Mitnick e Simon (2002) destacam que a engenharia social se aproveita da confiança e do desconhecimento dos usuários, sendo um dos métodos mais eficazes de comprometimento inicial em ataques cibernéticos. Segundo os autores, “as pessoas são o elo mais fraco da segurança” (MITNICK; SIMON, 2002, p. 17).

O aumento da conectividade, especialmente com a proliferação de dispositivos da Internet das Coisas (IoT), ampliou a superfície de ataque. Para Gollmann (2011), dispositivos IoT muitas vezes carecem de medidas básicas de segurança, como autenticação robusta e atualizações automáticas, tornando-os alvos fáceis para botnets e ataques de negação de serviço (DDoS).

Além disso, os ataques a infraestruturas críticas, como redes de energia, saúde e transporte, têm preocupado especialistas em segurança. Bishop (2018, p. 394) afirma que a interdependência entre sistemas digitais e serviços essenciais amplia o impacto potencial dos ataques, podendo gerar crises sociais e econômicas.

A espionagem cibernética é outra ameaça relevante, geralmente praticada por atores estatais ou grupos patrocinados por governos. Valeriano e Maness (2015) analisam como essa modalidade de ataque visa à coleta de informações estratégicas e à sabotagem de sistemas adversários,

configurando uma nova forma de conflito no ciberespaço.

Segundo Doneda (2021), a proteção de dados pessoais também é afetada por ameaças contemporâneas, especialmente em razão de vazamentos massivos de dados armazenados por empresas e órgãos públicos. A exposição de informações sensíveis compromete a privacidade dos indivíduos e pode gerar impactos financeiros e reputacionais às organizações.

Os ataques de dia zero (zero-day) representam um grande desafio, pois exploram falhas desconhecidas pelos desenvolvedores e para as quais ainda não há correção. A saber, Moura et al. (2020) explicam que a detecção desses ataques requer soluções baseadas em inteligência artificial e análise comportamental.

A desinformação e as campanhas de manipulação em redes sociais também configuram ameaças cibernéticas, com impactos sociais e políticos. Segundo Cruz et al. (2021), essas campanhas podem afetar processos democráticos, como eleições, e disseminar conteúdo falso com grande alcance.

Diante desse cenário, a mitigação das ameaças cibernéticas exige uma abordagem integrada, envolvendo tecnologia, políticas públicas e educação. Para Rezende (2018, p. 209), é essencial fortalecer a governança de TI, adotar padrões de segurança e promover a capacitação dos usuários para enfrentar esse ambiente de ameaças em constante transformação.

6. RESULTADOS E DISCUSSÃO

A análise das ameaças cibernéticas contemporâneas revela um cenário de crescente complexidade e impacto, no qual a transformação digital tem sido simultaneamente uma facilitadora de desenvolvimento e um vetor de riscos. A literatura especializada confirma que a digitalização expõe as organizações a uma ampla variedade de ataques, exigindo abordagens multidimensionais de defesa.

Destarte, Stallings (2019, p. 251) destaca que “as ameaças à segurança da informação se diversificam à medida que a infraestrutura tecnológica se torna mais complexa”, enfatizando a importância de atualizações constantes e políticas de backup como barreiras contra ataques como o ransomware. Esse tipo de ataque, como discutido anteriormente, representa uma das formas mais disruptivas de incidente cibernético, afetando dados críticos e exigindo resgates financeiros para sua recuperação.

Além disso, as técnicas de engenharia social, como o phishing, continuam sendo extremamente eficazes. Mitnick e Simon (2002, p. 17) afirmam que “as pessoas são o elo mais fraco da segurança”, evidenciando a necessidade de ações educativas contínuas para mitigação dessas vulnerabilidades humanas. A maioria dos ataques bem-sucedidos inicia com falhas comportamentais dos usuários, o que torna imprescindível a construção de uma cultura organizacional voltada à segurança.

O papel da Internet das Coisas (IoT) nesse contexto é igualmente relevante. Para tanto, Gollmann (2011) observa que a ausência de padrões de segurança robustos nos dispositivos conectados multiplica os pontos de entrada para possíveis invasões. Isso é agravado pelo crescimento do número de dispositivos, muitas vezes implementados sem uma análise prévia de risco.

No campo das infraestruturas críticas, os dados sugerem que a digitalização de sistemas vitais amplia o potencial de dano em caso de incidentes. Bishop (2018, p. 394) explica que a dependência de sistemas automatizados pode transformar falhas técnicas em crises de grandes proporções, com impactos sociais e econômicos severos. Portanto, os sistemas que sustentam serviços públicos e essenciais devem ser tratados como ativos estratégicos de segurança nacional.

Os ataques de dia zero representam outro ponto crítico na literatura. Assim, Moura et al. (2020) argumentam que a detecção precoce dessas

ameaças exige o uso de tecnologias emergentes, como aprendizado de máquina, o que implica investimentos em pesquisa e desenvolvimento. Esses ataques, por explorarem vulnerabilidades desconhecidas, desafiam os métodos tradicionais de defesa.

O aspecto geopolítico também tem se tornado mais evidente nos resultados analisados. Valeriano e Maness (2015) descrevem a ciberespionagem como uma nova forma de conflito entre Estados, pautada não apenas em danos físicos, mas na coleta estratégica de informações. Esse cenário reforça a necessidade de políticas públicas robustas voltadas à soberania cibernética.

Adicionalmente, Doneda (2021) enfatiza a importância da proteção de dados pessoais diante do crescimento de vazamentos e uso indevido de informações sensíveis. A Lei Geral de Proteção de Dados (LGPD), nesse contexto, é apontada como uma resposta legislativa fundamental, embora ainda dependa de ampla efetividade na aplicação.

A manipulação de informações em ambientes digitais, como redes sociais, se apresenta como um desafio sociotécnico. Cruz et al. (2021) evidenciam que a desinformação não apenas mina a confiança pública, mas também afeta diretamente a integridade de processos democráticos. Tal fenômeno exige uma resposta coordenada entre plataformas tecnológicas, instituições de controle e sociedade civil.

Finalmente, os resultados mostram que a segurança cibernética eficaz requer governança. Rezende (2018, p. 209) reforça que “a gestão de riscos deve ser parte estruturante da estratégia organizacional”, destacando que a proteção digital não deve ser vista apenas como custo, mas como investimento essencial para a sustentabilidade institucional.

7. CONSIDERAÇÕES FINAIS

O avanço tecnológico e a digitalização de serviços vêm acompanhados do crescimento exponencial de ameaças cibernéticas, tornando a segurança da informação uma prioridade global. As análises desenvolvidas neste trabalho demonstraram que a complexidade dos ataques atuais exige respostas que combinem tecnologia, governança e formação humana. Segundo Amorim (2020), a cibersegurança deixou de ser um campo técnico restrito para se tornar uma necessidade estratégica em organizações públicas e privadas.

A diversificação das ameaças — como ransomware, phishing, ataques de dia zero e manipulação de dados — demanda medidas de proteção mais inteligentes e adaptativas. Para Stallings (2019, p. 251), “a defesa cibernética moderna deve ir além das soluções reativas, incorporando capacidades preditivas e proativas no combate às ameaças”. Isso implica reconhecer que abordagens convencionais, baseadas exclusivamente em antivírus ou firewalls, não são mais suficientes.

Nesse cenário, a inteligência artificial (IA) surge como um dos principais recursos para o fortalecimento da ciberdefesa. De acordo com Moura et al. (2020), técnicas de aprendizado de máquina permitem identificar padrões anômalos e responder a ataques em tempo real, fator essencial diante do volume crescente de dados em redes corporativas. Gollmann (2011) acrescenta que a IA também contribui significativamente para a análise comportamental de usuários e sistemas, aumentando a capacidade de detecção de ações maliciosas.

Contudo, a adoção da IA não está isenta de desafios éticos e técnicos. Para Doneda (2021), o uso massivo de dados para treinar algoritmos pode violar princípios de privacidade se não houver uma governança adequada. Taddeo e Floridi (2018) reforçam que “a segurança digital deve ser informada por uma ética robusta que considere não apenas a eficácia das soluções, mas seus impactos sociais” (p. 14). Isso aponta para a necessidade de pesquisas futuras voltadas à construção de sistemas explicáveis (XAI) e auditáveis, capazes de aliar desempenho à transparência.

Além disso, o desenvolvimento de sistemas de IA para ciberdefesa ofensiva, como agentes automatizados para testes de penetração (red teaming), tende a crescer. Isso abre um novo campo de investigação sobre

contramedidas defensivas igualmente inteligentes, criando um ecossistema de combate cibernético entre IA ofensiva e IA defensiva. Tais avanços requerem regulamentações tecnológicas mais ágeis e eficazes, além de estruturas legais que acompanhem essa evolução.

Outra dimensão crítica é a segurança em sistemas de Internet das Coisas (IoT) e infraestruturas críticas. Esses ambientes são particularmente vulneráveis, dada a sua baixa capacidade de defesa e o alto impacto de uma possível violação. Soluções baseadas em arquiteturas distribuídas, como blockchain, e abordagens como zero trust e IA embarcada, devem ser priorizadas nos projetos de pesquisa e desenvolvimento.

A computação quântica também desponta como um fator disruptivo. Conforme Stallings (2019, p. 307), “a criptografia tradicional será desafiada por tecnologias com poder computacional exponencial”, o que torna urgente o investimento em criptografia pós-quântica e em novos modelos de segurança para redes e sistemas sensíveis.

No campo da proteção de dados, a legislação avança com iniciativas como a LGPD no Brasil e o GDPR na Europa. No entanto, a velocidade da inovação tecnológica exige mecanismos regulatórios mais dinâmicos, como agências especializadas em regulação algorítmica, além de instrumentos legais que assegurem a transparência e a responsabilização de sistemas automatizados. Como destaca Doneda (2021), a regulação da tecnologia deve estar ancorada em princípios como transparência, necessidade e responsabilidade.

Além das soluções técnicas, a dimensão humana permanece como elo essencial da segurança. Mitnick e Simon (2002, p. 17) alertam que “a tecnologia pode ser invencível, mas os usuários não”, reforçando a importância da cultura organizacional de segurança e da educação digital continuada. Amorim (2020, p. 163) defende que “a educação continuada é um dos pilares da resiliência cibernética”, o que abre espaço para estratégias educacionais inovadoras, como gamificação, treinamentos baseados em IA e simulações com realidade aumentada.

No panorama geopolítico, o ciberespaço tem se consolidado como novo domínio de disputas internacionais. Valeriano e Maness (2015) demonstram que ataques a sistemas elétricos, financeiros ou hospitalares podem ter impactos semelhantes aos de ações militares, reforçando a necessidade de estratégias nacionais de ciberdefesa integradas a políticas

internacionais de cooperação.

Por fim, conclui-se que a segurança cibernética contemporânea exige uma abordagem multidisciplinar, tecnológica e ética. O uso responsável e estratégico da inteligência artificial oferece novas possibilidades de defesa, desde que seja acompanhado de políticas públicas eficazes, marcos legais atualizados e investimento contínuo em pesquisa, educação e inovação. Como afirmam Russell e Norvig (2021, p. 993), “a IA não deve ser apenas poderosa, mas confiável, compreensível e alinhada com valores humanos fundamentais”. Assim, a construção de uma sociedade digital segura depende do equilíbrio entre avanço tecnológico, responsabilidade ética e governança sólida.

REFERÊNCIAS

- AMORIM, A. M.** Segurança da Informação e Cibersegurança: Conceitos e Desafios Contemporâneos. São Paulo: Atlas, 2020.
- ARAÚJO, R. S.; ALMEIDA, R. A.** Capacitação em Cibersegurança: Educação, Pesquisa e Prática. *Revista Brasileira de Computação Aplicada*, v. 12, n. 2, p. 77–92, 2020.
- AVEN, T.** Risk Analysis: Assessing Uncertainties Beyond Expected Values and Probabilities. Wiley, 2015.
- BISHOP, M.** Computer Security: Art and Science. 2nd ed. Boston: Addison-Wesley, 2018.
- BINNS, T.** The Ethics of Artificial Intelligence. Springer, 2018.
- BOECHAT, Gabriel Verleun.** Análise da aplicação da inteligência artificial no atual cenário de cibersegurança. 2022. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade de Brasília, Brasília, 2022. Disponível em: <https://repositorio.uniceub.br/jspui/bitstream/prefix/17278/1/21650430.pdf>.
- BRYSON, J.** The Ethics of Artificial Intelligence and Robotics. Springer, 2018.
- CALO, R.; HERMAN, G.; ZITTRAIN, J.** The Limits of the Law and the Promise of Regulation in AI. *Harvard Law Review*, 2019.
- CRUZ, M. A. et al.** Desafios da Segurança da Informação no Trabalho Remoto em Tempos de Pandemia. *Revista Gestão & Tecnologia*, v. 21, n. 1, p. 112–128, 2021.
- DIAKOPOULOS, N.** Algorithmic Transparency: Exploring the Role of Explainability. MIT Press, 2016.
- DONEDA, D.** Da Privacidade à Proteção de Dados Pessoais. 2. ed. Rio de Janeiro: Forense, 2021.
- FLORIDI, L.** Ethics of Artificial Intelligence: The Need for a New Regulatory Framework. Oxford University Press, 2019.
- GOLLMANN, D.** Computer Security. 3rd ed. Chichester: Wiley, 2011.
- GOMES, L. H.; SILVA, T. C.** A Cultura de Segurança da Informação nas Organizações. *Revista Tecnologia e Sociedade*, v. 15, n. 38, p. 121–135, 2019.
- MOSCHOVITIS, C.** Governança de Segurança da Informação: Estrutura e Prática. p. 56, 2019.
- (ISC).** The 2021 Cybersecurity Workforce Study. (ISC), 2021.
- LAUDON, K. C.; LAUDON, J. P.** Sistemas de Informação Gerenciais. 14. ed. São Paulo: Pearson, 2020.

LUGER, G. Artificial Intelligence: Structures and Strategies for Solving Complex Problems. Prentice Hall, 2019.

MITNICK, K. D.; SIMON, W. L. A Arte de Enganar: Contando Histórias de Hackers e Golpes de Engenharia Social. São Paulo: Campus, 2002.

MOURA, F. et al. Machine Learning Applied to Cybersecurity: Current Trends and Challenges. *Journal of Information Security and Applications*, v. 53, 2020.

OLIVEIRA, E.; VERONESE, G. Cibersegurança: Princípios e Práticas. Porto Alegre: Bookman, 2017.

O'NEIL, C. Weapons of Math Destruction. Crown Publishing Group, 2016.

PIRES, SOFIA FILIPA GONÇALVES. O impacto da inteligência artificial no setor bancário. 2020. Tese de Doutorado.

REZENDE, D. A. Governança de Tecnologia da Informação e Comunicação. São Paulo: Atlas, 2018.

RUSSELL, S.; NORVIG, P. Artificial Intelligence: A Modern Approach. Pearson, 2016.

RUSSELL, Stuart; NORVIG, Peter. Inteligência Artificial. 4. ed. São Paulo: Pearson, 2020.

SCHNEIER, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company, 2018.

SHARMA, A. Security in AI Systems: Risks and Challenges. Springer, 2020.

SIAU, K.; WANG, W. Artificial Intelligence and Ethics: Challenges and Solutions. *Information Systems Journal*, 2020.

SILVA, L. M. et al. Diplomacia Cibernética: Uma Nova Fronteira da Segurança Internacional. *Revista Brasileira de Estudos de Defesa*, v. 8, n. 2, p. 190–208, 2021.

SOUSA, A. S. S. et al. A Pesquisa Bibliográfica: Princípios e fundamentos. Cadernos da Fucamp. v.20, n.43, 2021.

STALLINGS, W. Segurança em Redes de Computadores: Princípios e Práticas. 6. ed. São Paulo: Pearson, 2019.

TANENBAUM, A.S.; BOS, H. Modern Operating Systems. 4a ed. Estados Unidos: Pearson Education, Inc., 2007.

VALERIANO, B.; MANESS, R. Cyber War versus Cyber Realities: Cyber Conflict in the International System. Oxford: Oxford University Press, 2015.

WHITMAN, M. E.; MATTORD, H. J. Principles of Information Security. 7th ed. Boston: Cengage Learning, 2021.