Research, Society and Development, v. 14, n. 6, e5714648937, 2025
(CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v14i6.48937

Ciberbiosegurança em ambientes biointeligentes: Integração de inteligência artificial, biologia sintética e automação em setores vitais

Cyberbiosecurity in biointelligent environments: Integrating artificial intelligence, synthetic biology and automation in vital sectors

Ciberbioseguridad en entornos biointeligentes: Integración de inteligencia artificial, biología sintética y automatización en sectores vitales

Recebido: 21/05/2025 | Revisado: 11/06/2025 | Aceitado: 12/06/2025 | Publicado: 15/06/2025

Enrico Jardim Clemente Santos
ORCID: https://orcid.org/0000-0003-0869-3342
Instituto de Pesquisas Energéticas e Nucleares, Brasil
Celltrotec, Brasil
E-mail: enrico@celltrotec.com.br
Angela Mazzeo
ORCID: https://orcid.org/0000-0001-8483-5002
Universidade de São Paulo, Brasil
Faculdade IBPTECH, Brasil
E-mail: angela.mazzeo@ibptech.edu.br

Resumo
O presente estudo visa analisar a importância da cibersegurança no contexto dos sistemas relacionados às ciências biológicas em diferentes setores da economia, a qual é denominada de ciberbiosegurança. Realizou-se uma pesquisa bibliográfica narrativa. A inovação tecnológica tornou-se um aspecto inerente à existência de nossa sociedade, uma vez que praticamente todos os itens relevantes para nossa vida diária possuem pelo menos um componente cibernético associado a ela. Dentre estes, podemos ressaltar os computadores pessoais, as redes de computadores, a tecnologia da informação e a realidade virtual. Agora, as ciências da vida vêm estabelecendo uma interface com a tecnologia da informação e a segurança cibernética. Esta convergência resultou em um crescimento significativo do setor de biotecnologia e suas aplicações na saúde, agricultura, manufatura, automação, inteligência artificial e biologia sintética. Com isso, fez-se necessário a criação de uma disciplina que englobasse a biossegurança e a segurança ciberfísica e cibersegurança, a qual foi denominada de ciberbiosegurança. Esta envolve a compreensão, proteção, mitigação, investigação e atribuição de vigilância indesejada, intrusões e atividades maliciosas e prejudiciais que podem ocorrer dentro ou nas interfaces das ciências médicas e da vida, que afetam a segurança, a competitividade e a resiliência.
Palavras-chave: Ciberbiosegurança; Biotecnologia; Segurança cibernética; Inteligência artificial; Biologia sintética.

Abstract
This study aims to analyze the importance of cybersecurity in the context of systems related to the biological sciences in different sectors of the economy, which is called cyberbiosecurity. A narrative bibliographic survey was carried out. Technological innovation has become an inherent aspect of our society's existence, since practically every item relevant to our daily lives has at least one cyber component associated with it. These include personal computers, computer networks, information technology and virtual reality. Life sciences are now interfacing with information technology and cyber security. This convergence has resulted in significant growth in the biotechnology sector and its applications in health, agriculture, manufacturing, automation, artificial intelligence and synthetic biology. This has necessitated the creation of a discipline that encompasses the scope of biosecurity and cyber-physical security and cyberbiosecurity which has been termed cyberbiosecurity which involves the understanding, protection, mitigation, investigation and attribution of unwanted surveillance, intrusions and malicious and damaging activities that may occur within or at the interfaces of the medical and life sciences, affecting security, competitiveness and resilience.
Keywords: Cyberbiosecurity; Biotechnology; Cyber security; Artificial intelligence; Synthetic biology.

Resumen
Este estudio pretende analizar la importancia de la ciberseguridad en el contexto de los sistemas relacionados con las ciencias biológicas en diferentes sectores de la economía, lo que se conoce como ciberbioseguridad. Se realizó un estudio bibliográfico narrativo. La innovación tecnológica se ha convertido en un aspecto inherente a la existencia de nuestra sociedad, ya que prácticamente todos los artículos relevantes para nuestra vida cotidiana tienen asociado al menos un componente cibernético. Entre ellos figuran los ordenadores personales, las redes informáticas, las

tecnologías de la información y la realidad virtual. Las ciencias de la vida están interactuando ahora con las tecnologías de la información y la ciberseguridad. Esta convergencia se ha traducido en un crecimiento significativo del sector de la biotecnología y sus aplicaciones en la salud, la agricultura, la fabricación, la automatización, la inteligencia artificial y la biología sintética. Esto ha hecho necesaria la creación de una disciplina que abarque el ámbito de la bioseguridad y la seguridad ciberfísica y la ciberbioseguridad que se ha denominado ciberbioseguridad que implica la comprensión, protección, mitigación, investigación y atribución de vigilancia no deseada, intrusiones y actividades maliciosas y perjudiciales que pueden ocurrir dentro o en las interfaces de las ciencias médicas y de la vida, afectando a la seguridad, la competitividad y la resiliencia.
Palabras chave: Ciberbioseguridad; Biotecnología; Ciberseguridad; Inteligencia artificial; Biología sintética.

1. Introdução

As vulnerabilidades cibernéticas são uma realidade atualmente, as quais apresentam riscos significativos para indivíduos, organizações, governos e economias. Entretanto, os desafios associados às vulnerabilidades da cibersegurança não são intransponíveis, uma vez que exigem considerações cuidadosas por parte dos projetistas de equipamentos, desenvolvedores de *software* e sistemas de controle, além dos usuários finais. Porém, os riscos relacionados as ciências biológicas vêm sendo gerenciado por meio da implementação de práticas padrão de biossegurança (proteção do material biológico valioso contra uso indevido ou dano) e segurança cibernética (proteção de sistemas de computador contra roubo e danos ao seu hardware, software ou informações, bem como contra interrupção ou direcionamento incorreto dos serviços que prestam). Esta associação foi denominada de ciberbiosegurança, um esforço que visa salvaguardar a bioeconomia.

A ciberbiosegurança é um campo emergente e inovador que aborda as vulnerabilidades e ameaças que ocorrem por meio da interseção do ciberespaço e da biotecnologia, tendo como base três setores: segurança cibernética, biossegurança e segurança ciberfísica. A segurança cibernética visa à proteção dos sistemas de computador contra violação, perda e danos ao seu *hardware*, *software*, informações e dados, bem como a interrupção de aplicativos e demais serviços relacionados a estes. A biossegurança visa à redução de riscos relacionados ao uso indevido de ferramentas, dados e/ou conhecimentos relacionados ao material biológico. Já a segurança ciberfísica aborda os riscos relacionados à segurança de tecnologias como sistemas de controle e operação industrial, além dos sensores da Internet das Coisas, os quais interagem e afetam o mundo físico e a vida humana em tempo real.

Embora a segurança cibernética englobe a proteção de quaisquer dados eletrônicos, sistemas, redes, etc., a ciberbiosegurança é uma de suas aplicações mais importantes, pois tem como alvo a implementação de medidas corretivas, prevenção de intrusões ilegais e na proteção de dados, informações, processos, materiais valiosos e outros recursos online, pertencentes às ciências da vida, médicas, saúde humana, animal e ambiental, manufatura, agrícola, pecuária, e alimentar (Murch & DiEuliis, 2019).

Devido ao fato da ciberbiosegurança ser um conceito novo não há cursos de treinamento e certificação disponíveis, o que dificulta os processos de educação e desenvolvimento profissional contínuo dos funcionários nas organizações, assim como a criação de políticas relacionadas a mesma (Richardson, 2019).

As ameaças maliciosas, uso indevido ou exploração de informações, processos e materiais valiosos, na interface das ciências da vida e mundo digital, tendem a ser identificadas e mitigadas por meio de treinamentos e implementação de processos de segurança os quais tendem a ser periodicamente aprimorados. Dentre estes temos a implementação de um sistema de *Backups* de dados em um servidor separado e não conectado à internet; *Firewall* de segurança robusto e confiável; protocolos de segurança cibernética implementado caso ocorra a violação de dados; e implementação de auditorias regulares e verificações anti-malware.

O presente estudo visa analisar a importância da cibersegurança no contexto dos sistemas relacionados às ciências biológicas em diferentes setores da economia, a qual é denominada de ciberbiosegurança.

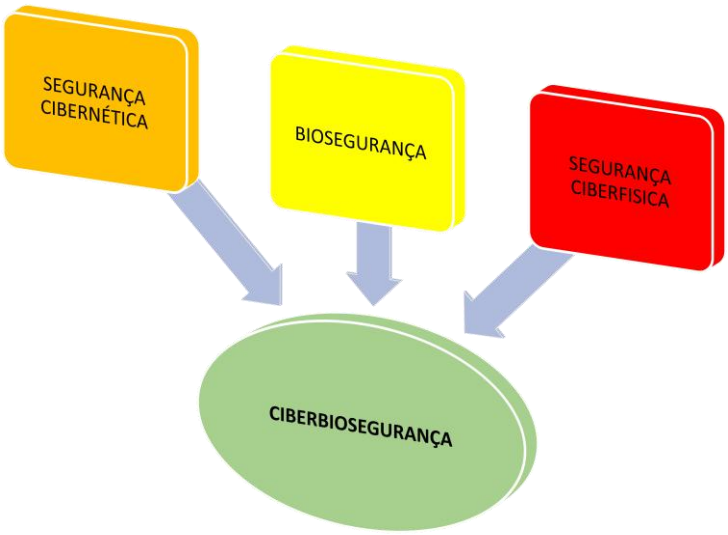
2. Metodologia

A metodologia científica é importante para que os artigos tenham reprodutividade nos resultados e que tenham aceitação pela comunidade acadêmica e científica (Pereira et al., 2018). O presente estudo teve como base, a pesquisa bibliográfica (Snyder, 2019; Sousa, 2021; Mattos, 2015) de cunho exploratório, descritivo e de natureza qualitativa e do tipo revisão de literatura narrativa (Rother, 2007; Mendes, 2022; Casarin, 2020) junto às bases de dados do Google Acadêmico, Scientific Electronic Library Online (Scielo), Literatura Latino-Americana do Caribe em Ciência da Saúde (LILACS), Researchgate e Medical Literature Analysis and Retrievel System Online (MEDLINE). Para a busca, foi realizado o recorte temporal de publicações entre os anos de 1943 e 2025, utilizando as seguintes palavras-chave: segurança cibernética; ciberbiosegurança; biossegurança; ataque cibernético; inteligência artificial; automação.

3. Resultados e Discussão

O primeiro artigo relacionado ciberbiosegurança foi publicado por Peccoud e colaboradores em 2018. O artigo enfocava principalmente questões relacionadas à segurança da interface biotecnológica com o ciberespaço e à necessidade de se conscientizar o usuário acerca dos riscos envolvidos. O artigo em questão contribuiu significativamente para o futuro escopo da ciberbiosegurança (Peccoud, 2018). Já o termo ciberbiosegurança foi estabelecido por Murch e colaboradores que descreveram as vulnerabilidades existentes entre a segurança cibernética, segurança ciberfísica e biossegurança (Figura 1) (Murch, 2018). Segundo Murcha a ciberbiosegurança pode ser definida como o "desenvolvimento da compreensão das vulnerabilidades à vigilância indesejada, intrusões, atividades maliciosas e prejudiciais que podem ocorrer dentro ou nas interfaces dos próximos sistemas de ciências da vida, cibernéticas, ciberfísicas, cadeia de suprimentos e infraestrutura, e desenvolver e instituir medidas para prevenir, proteger, mitigar, investigar e atribuir tais ameaças no que se refere à segurança, competitividade e resiliência" (Murch, 2018)(Figura 1).

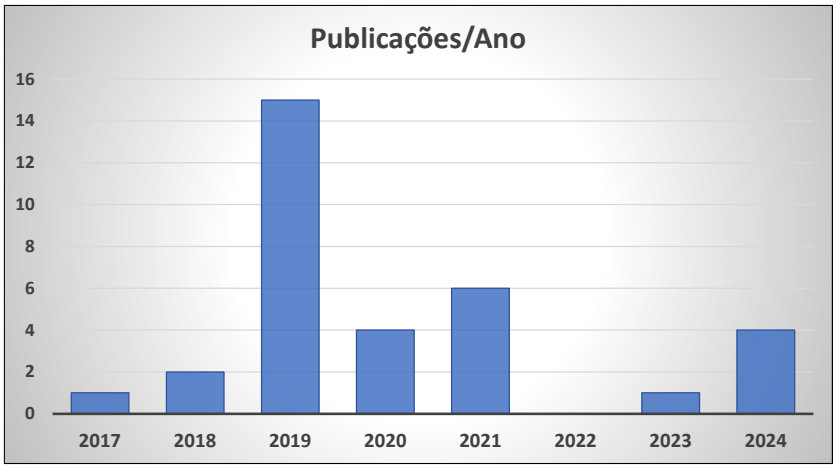
Figura 1 - A ciberbiosegurança é a integração das disciplinas de biossegurança, segurança ciberfísica e cibersegurança que envolve a compreensão, proteção, mitigação, investigação e atribuição de vigilância indesejada, intrusões e atividades maliciosas e prejudiciais que podem ocorrer dentro ou nas interfaces das ciências médicas e da vida, que afetam a segurança, a competitividade e a resiliência.



Fonte: Autoria Própria.

A ciberbiossegurança é uma disciplina que tem um impacto significativo nas operações digitais de empresas de diferentes setores, incluindo agropecuário e de saúde. Dados obtidos por meio de levantamento bibliográfico realizado no Medical Literature Analysis and Retrievel System Online (MEDLINE), tendo como base o período entre janeiro de 2017 a outubro de 2024, e utilizando o termo *cyberbiosecurity*, resultaram em 31 publicações científicas (Figura 2). Neste período, o ano de 2019 apresentou o maior número de publicações (15 ao todo), ao passo que no ano de 2022 não foi identificada nenhuma publicação. Estes dados comprovam ser a cibersegurança uma área extremamente nova.

Figura 2 - Taxa de publicações anuais relativas ao tópico ciberbiossegurança no MEDLINE.



Fonte: Autoria Própria.

Avanços científicos, matemáticos, computacionais e de engenharia integrados com a biologia regenerativa, genética e tecnologias de reprodução, vacinas derivadas de plantas e terapias animais, design biológico e automação de testes e outras atividades estão resultando no rápido desenvolvimento de aplicações biotecnológicas e agropecuárias de relevância. Devido à sua vulnerabilidade no setor de segurança cibernética, áreas como saúde, agropecuária e manufatureiro vêm enfrentando desafios significativos, uma vez que vêm sendo alvo de diversos tipos de ataques cibernéticos, como os realizados por meio de aplicativos e plataformas online, por exemplo.

Cibersbiossegurança na agropecuária

Devido a rápida expansão da população mundial, proteger a agropecuária e a cadeia de abastecimento alimentar quanto a ataques cibernéticos é um fator de alta prioridade, uma vez que dados corrompidos pode resultar em perdas significativas para a bioeconomia devido a tomada de decisões equivocadas (Duncan, 2019).

A implementação de alguns procedimentos de cibersegurança como auditorias no sistema de rede e equipamentos visando a identificação de possíveis vulnerabilidades, instalação de firewalls e outros softwares que ajudem a mitigar as ameaças de invasão cibernética, utilização de algoritmos baseados em inteligência artificial visando, por exemplo, verificar se um usuário malicioso está acessando o sistema e alterando os dados referentes ao processo de irrigação das plantações e educar os colaboradores acerca de possíveis ameaças cibernéticas que podem expor ativos digitais de extrema relevância.

Embora os riscos associados ao ciberataques (tentativa de obter acesso não autorizado aos sistemas informáticos visando roubar, modificar ou destruir dados) sejam de conhecimento público, é incomum que as fazendas, principalmente as pequenas, tenham planos de contingência visando prevenir ataques cibernéticos (van der Linden, 2020). A interconectividade entre fazendas e instalação de produção com os fornecedores e vendedores propicia a troca dados que criando assim redes de

informações normalmente não supervisionadas. A aplicação de tecnologias voltadas agricultura de precisão e sistemas autônomos assim como processamentos e registros bioautomatizados, produzem um volume significativo de dados referentes a informações econômicas e biológicas para agronegócios (Sykuta, 2016). Portanto, a proteção do setor agropecuário inclui a implementação de processos de cibersegurança e biossegurança de forma proteger a bioeconomia (Santos, 2017).

O processamento de alto rendimento, gerenciamento e integração de dados, bioautomação e outros gerenciamento de dados biológicos são de fundamental relevância para o setor de agronegócio. O acesso aos dados propicia um aumento na segurança e eficácia dos processos de decisão e produção dentro do sistema alimentar e agrícola. No entanto, essas informações são suscetíveis a ataques cibernéticos, pois os usuários podem não estar alertas para possíveis vulnerabilidades nem serem treinados em proteções eficazes e estratégias de segurança (Sykuta, 2016). Dentre alguns exemplos de alimentos e produtos agrícolas de alto valor, suscetíveis a ameaças cibernéticas, temos as culturas agrícolas especializadas e de alto rendimento, gado de alto desempenho, banco de germoplasma vegetal e animal, sistemas biocontrolados como estufas, rede de diagnóstico contendo dados referentes a animais e vegetais doentes, parâmetros de controle do processamento térmico e sistemas de tratamento e abastecimento de água. Sendo assim, proteger o setor agropecuário de ataques cibernéticos resulta na tomada de boas decisões no que tanges a segurança e eficácia da produção (Duncan, 2019; van der Linden, 2020).

Atualmente não existem cursos, treinamento e certificações para indivíduos interessados em se tornarem especialistas ciberbiossegurança no setor agropecuário, o que pode levar a práticas de segurança inadequadas em qualquer parte da cadeia de suprimentos. Nos dias atuais o candidato provavelmente ideal deveria graduado em agronomia ou medicina veterinária, com conhecimento em segurança cibernética e biossegurança (Richardson, 2019). Cursos voltados a ciberbiosegurança precisam ser criados para preparar profissionais para os dias atuais e vindouros (Geil et al., 2018).

Ciberbiosegurança na saúde

Com o início da pandemia de COVID-19, no início de 2020, milhões de pessoas começaram a trabalhar em suas residências em um sistema de *home office*, tornando as videoconferências uma realidade na vida das pessoas. No que se refere à saúde das pessoas, as consultas on-line, a reabilitação assistida por computador e o monitoramento remoto surgiram como recursos extremamente interessantes para o sistema de saúde. Tal fato se deu, na maioria, à inacessibilidade dos serviços de atendimento tradicionais, em função dos altos riscos de exposição das consultas de saúde presenciais. (Jalali, 2021). Entretanto, barreiras como pessoal capacitado, custos elevados, acesso à banda larga e alfabetização digital dos pacientes mostraram ser uma realidade no dia a dia da população mundial.

A crescente utilização de dispositivos médicos conectados, via Internet, como ventiladores, bombas de infusão, equipamentos de imagem radiológica, equipamentos de monitoramento a dispositivos implantáveis e suporte de órgãos específicos, vem apresentando riscos significativos. A interrupção ou invasão de qualquer um desses dispositivos pode atrasar, ou alterar o protocolo de atendimento, podendo causar danos irreparáveis a um paciente, assim como manchar a reputação da instituição, infligindo perdas financeiras significativas (Mazzeo, 2025a). Além disso, questões relacionadas a privacidade dos dados clínicos e financeiros dos pacientes, integridade dos dados de testes de diagnóstico, integridade dos bancos de dados biológicos, assim como a segurança nos avanços da engenharia biológica, que possam dar origem a patentes, são questões extremamente relevantes (You, 2015; Khera, 2017). Instituições de saúde têm sido alvos de *biohackers* (*hackers* que atuam especificamente no setor das ciências da vida) que têm obtido milhares de dólares em resgates devido à natureza crítica das informações (*ransomware*) (Osborne, 2018).

Ataques cibernéticos podem resultar em consequências significativas ao sistema de saúde uma vez que dados valiosos e confidenciais usados para criar medicamentos, tratamentos, etc., que podem ser acessados por agentes mal-intencionados se

armazenados em um sistema operacional não seguro (vulnerabilidades dos sistemas)(Mazzeo, 2025a). Tal fato levou ao surgimento de um novo campo de atuação denominado de ciberbiosegurança.

Em particular, os desafios a serem considerados são a privacidade e integridade dos bancos, de dados médicos, pacientes e instituições de saúde, defesa contra-ataques cibernéticos e automação laboratorial e hospitalar. A integridade dos bancos de dados públicos de bioinformática, como, por exemplo, os mantidos pelo NCBI (The *National Center for Biotechnology Information),* e a proteção da propriedade intelectual são de fundamental importância.

Ciberbiosegurança na indústria manufatureira

Manter a segurança cibernética na economia moderna, onde tecnologias avançadas de fabricação e estratégias digitais estão se tornando a norma, é um desafio significativo. As organizações dependentes de ciência e tecnologia estão se tornando mais complexas e conectadas por meio de uma rede em instalações, cadeias de suprimentos, logística e mecanismos de transporte. A manufatura distribuída emprega redes de produção descentralizadas ligadas pela tecnologia da informação. À medida que mais conexões entre sistemas tradicionalmente isolados são desenvolvidas, mais controles de segurança devem ser considerados para mitigar riscos e reduzir vulnerabilidades. Para isso, o primeiro passo para essas organizações é mapear os riscos.

Os processos de fabricação, requisitos regulatórios, propriedade intelectual e os sistemas ciberfísicos envolvidos na produção de terapias biológicas podem ser vulneráveis principalmente a três formas de ataques cibernéticos: sabotagem (atos deliberados e maliciosos que danificam a infraestrutura digital ou física), espionagem corporativa (um ataque avançado e persistente pode permitir que rivais corporativos roubem comunicações internas, IP relacionados ao produto ou processo e dados de monitoramento de instalações para obter uma vantagem competitiva) e crime/extorsão (criptografar arquivos com uma nota de resgate solicitando remuneração por seu retorno) (Morag, 2014; Carman, 2014).

As empresas biofarmacêuticas são consideradas indústrias de alto valor agregado, tornando-se um alvo atraente para os *biohackers*. O modelo de produção em lotes de grande escala para terapias biológicas, vacinas e proteínas recombinantes é um setor vulnerável, pois qualquer interrupção na cadeia de produção pode prejudicar de forma significativa a produção anual da empresa e, por consequência, seu faturamento.

As empresas biofarmacêuticas (empresa que fabricam e comercializam biofármacos ou medicamentos produzidos com recurso biotecnológicos) empregam sistemas ciberfísicos com uma variedade de funções como: fornecimento de matérias-primas, desenvolvimento e otimização de linhagens celulares, desenvolvimento de processos *upstream* e *downstream*, fabricação, estudos de validação, ensaios clínicos, gerenciamento da cadeia de suprimentos de produtos, monitoramento de segurança de medicamentos pós-comercialização e interface com provedores de saúde. Como parte das abordagens avançadas de fabricação, várias ferramentas, como a inteligência artificial e a internet das coisas, estão permitindo um controle mais responsivo visando otimizar a reprodutibilidade, qualidade, segurança e fornecimento da produção (Helu, 2015; Zhong, 2017).

As empresas farmacêuticas mantêm em suas redes corporativas dados de pacientes relacionados a ensaios clínicos e gerenciamento de doenças. Como os dados são informações pessoais altamente confidenciais e regulamentadas, violações podem incorrer em grandes multas e prejudicar a reputação de uma empresa. Avaliar os riscos emergentes acerca da segurança cibernética é especialmente importante em toda a indústria biofarmacêutica, pois muitas empresas trabalham visando estabelecer estratégias digitais relacionadas a desenvolvimento de medicamentos, design de processos, fabricação, controle de qualidade e ensaios clínicos.

Ciberbiossegurança na biologia sintética

O termo "biologia sintética" vêm sendo amplamente utilizado para descrever atividades relacionadas a diversas *disciplinas* como bioengenharia, química, bioquímica e ciência dos materiais até biologia celular e molecular (Purnick, 2009) que tem por objetivo final redesenhar organismos vivos de forma que adquiram novas habilidades. Em 2010, John *Craig Venter* e colaboradores criaram, em laboratório, uma célula bacteriana (*Mycoplasma mycoides*) controlada por um genoma completamente artificial, inteiramente sintetizado quimicamente (Gibson, 2010). Desde então, diversas aplicações vêm sendo estabelecidas, como a criação de circuitos genéticos, novas moléculas e commodities como combustíveis, eletricidade, ração, materiais renováveis, biossensores e exploração espacial (Rollin et al., 2013; Kiss et al., 2014; Verseux, 2016).

À medida que as técnicas de automação laboratorial se tornem mais difundidas e o custo de produção seja reduzido, a biologia sintética terá um impacto significativo no setor de ciberbiossegurança. A convergência da robótica, microfluídica, design de sistemas livres de células e engenharia metabólica tendem a criar riscos relacionados à ciberbiossegurança. (Nielsen, 2011; Murch, 2018; Peccoud, 2018). À medida que esses campos se desenvolvem e convergem entre si, as vulnerabilidades reveladas oferecerão novas oportunidades de exploração por parte dos *biohackers*.

Ciberbiossegurança na inteligência artificial

A ideia de uma máquina que possa realizar tarefas de forma inteligente é algo que permeia a humanidade há bastante tempo. Porém, foi em 1943 que Warren McCulloch e Walter Pitts publicaram um artigo que abordava pela primeira vez as redes neurais e estruturas de raciocínio artificiais em forma de modelo matemático, para simular o sistema nervoso (McCulloch, 1943). Em 1950, Claude Shannon publicou um artigo científico acerca do processo de programar uma máquina para jogar xadrez com cálculos de posição simples e eficazes (Shannon, 1950). No mesmo ano, Alan Turing desenvolveu o teste de Turing, originalmente conhecido como o Jogo da Imitação, o qual tinha por objetivo avaliar se uma máquina consegue atuar de forma equivalente a um humano durante uma conversa por escrito (Turing, 1950). No ano seguinte Marvin Minsky e Dean Edmunds constroem a SNARC (*Stochastic Neural Analog Reinforcement Calculator*) uma calculadora de reforço analógico neural estocástico que realiza operações matemáticas simulando sinapses, ou seja, a primeira rede neural artificial constituída por uma rede de 40 neurônios. Em 1952, Arthur Lee Samuel desenvolveu o primeiro software que joga damas e aprende por conta própria, ou seja, autodidata. Porém, o marco-zero da inteligência artificial foi estabelecido na Conferência de Dartmouth realizada em 1956 quando a mesma foi batizada por John McCarthy tendo sua máxima definida da seguinte forma: cada aspecto de aprendizado ou outra forma de inteligência pode ser descrita de forma tão precisa que uma máquina pode ser criada para simular isso (Toosi, 2021).

A aplicação crescente da inteligência artificial nos processos biotecnológicos e bioindustriais, que vão desde dados moleculares até a automação de laboratórios de biologia sintética, é uma realidade no mundo atual (Chakravarthi, 2024). Entretanto, a integração entre biotecnologia, tecnologias digitais e automação acarreta desafios robustos no que se refere ao acesso, controle e integridade dos dados relacionados à proteção das infraestruturas biológicas. Estas podem estar suscetíveis a ameaças cibernéticas, que podem comprometer dados, equipamentos, modelos preditivos e sistemas de controle automatizados (Pinkham, 2021).

A inteligência artificial vem sendo utilizada de diferentes formas no campo da biotecnologia, como na otimização de rotas metabólicas, desenvolvimento de fármacos, criação de modelos preditivos de doenças e otimização de decisões clínicas (Mazzeo, 2025b). Porém, diferentes ameaças vêm emergindo por meio de ataques cibernéticos como, ocasionar danos a integridade dos dados genéticos armazenados ou comprometer a privacidade genética de indivíduos ou populações, manipular dados produzindo resultados falsos negativos ou positivos com graves consequências clínicas, modificar de forma não

autorizada sistemas dos laboratórios automatizados, alterar protocolos automatizados referentes a projeção e produção de patógenos sintéticos que apresentem uma maior virulência ou resistência a tratamentos, acesso remoto a dispositivos IoT biomédicos e laboratoriais, vazamento de organismos modificados geneticamente, sabotagem de biofábricas automatizadas para produzir toxinas ou falhar em produção e manipulação de resultados de diagnósticos baseados em automação laboratorial (Arshad, 2021).

Dentre as áreas críticas que dependem do sistema de automação estão as plataformas de síntese genética, fermentadores industriais inteligentes para produção de biofármacos, laboratórios de biossegurança com controle remoto, sistemas robóticos de manipulação de patógenos e dispositivos IoT de biossensoriamento ambiental ou clínico. Esses sistemas operam frequentemente conectados a redes corporativas ou em nuvem, o que os torna mais suscetíveis aos ataques cibernéticos (Arshad, 2021; Nayak, 2022).

Visando mitigar possíveis consequências, estratégias vêm sendo implementadas como: 1 - Implementação de uma criptografia robusta; 2 - Autenticação multifator para sistemas de controle; 3 - Redes segmentadas; 4 - Autenticação multifatorial; 5 - Protocolos de resposta a incidentes em infraestruturas que tratam dados biológicos sensíveis; 6 - Implementação de um sistema de confiança zero; 7 – Implementação de modelos de inteligência artificial auditáveis, explicáveis e rastreáveis; 8 - Auditorias periódicas de software embarcado em robôs e sensores biológicos são fundamentais para garantir a confiabilidade dos sistemas; 9 - Capacitação de equipes multidisciplinares em segurança digital e biossegurança; 10 - Protocolos de resposta a incidentes que envolvam dados ou materiais biológicos e11 – Implementação de uma regulamentação e limites éticos e sociais no que se refere a utilização da inteligência artificial (Cuningkin, 2021; Wang, 2022).

A convergência entre biotecnologia, tecnologias digitais e automação exige uma abordagem integrada, proativa e robusta frente aos desafios da ciberbiosegurança. A prevenção de incidentes ciberbiológicos deve ser tratada como prioridade estratégica em instituições de pesquisa, empresas bioindustriais e governos. Assim sendo, o desenvolvimento e fortalecimento de políticas públicas e interdisciplinares, formação de profissionais híbridos, desenvolvimento de normas técnicas, combinando ciência da computação e biológica, são passos fundamentais para garantir a segurança e a ética biotecnológica.

4. Considerações Finais

À medida que as biotecnologias continuam avançando e evoluindo, a ciberbiosegurança será uma consideração fundamental na infraestrutura crítica existente relacionada a todas essas arenas. A ciberbiosegurança pode ser vista como uma abordagem que visa compreender as vulnerabilidades que podem afetar instituições médicas, biotecnológicas, agropecuárias, logísticas e infraestruturas por meio de intrusões, atividades maliciosas e prejudiciais além de desenvolver e instituir medidas para prevenir, proteger, mitigar e investigar tais ameaças no que se refere à segurança, competitividade e resiliência. Além disso, novos componentes de infraestrutura crítica podem surgir e ser definidos por meio de avanços na indústria de biologia sintética, e a segurança cibernética precisará ser avaliada para esses novos componentes. Em nossa opinião, a conscientização e a identificação de vulnerabilidades é um primeiro passo importante para o lançamento do campo, seguido pelo desenvolvimento e implementação de mitigações e soluções. Eventualmente, os profissionais neste campo em crescimento serão responsáveis pelo desenvolvimento de diretrizes e padrões de governança, o que exigirá adesão e compatibilidade com as estratégias defensivas nacionais existentes.

Referências

Arshad, S., Arshad, J., Khan, M. M., & Parkinson, S. (2021). Analysis of security and privacy challenges for DNA-genomics applications and databases. *Journal of biomedical informatics*, *119*, 103815. https://doi.org/10.1016/j.jbi.2021.103815

Carman, A. (2014). Dragonfly Malware was Designed to Target Pharmaceutical Companies. *SC Magazine. Available online at:* https://www.scmagazine.com/home/security-news/dragonfly-malware-was-designed-to-target-pharmaceutical-companies/ *(accessed August 11, 2019).*

Casarin, S. T. et al. (2020). Tipos de revisão de literatura: considerações das editoras do Journal of Nursing and Health/Types of literature review: considerations of the editors of the Journal of Nursing and Health. Journal of Nursing and Health,10(5). DOI: https://doi.org/10.15210/jonah.v10i5.19924. https://periodicos.ufpel.edu.br/index.php/enfermagem/article/view/19924.

Chakravarthi, P. G.; Rambabu V; Ramamurty DSVNM; Rahul G. & Prasad SVGVA. AI and Machine Learning in Biotechnology: A Paradigm Shift in Biochemical Innovation. International Journal of Plant, Animal and Environmental Sciences. 14(2024), 70-80. DOI: 10.26502/ijpaes.4490166

Chi, H., Welch, S., Vasserman, E., & Kalaimannan, E. (2017). "A Framework of Cybersecurity Approaches in Precision Agriculture. in" proceedings of the ICMLG2017 5th International Conference on Management Leadership and Governance, Dayton, USA, 2–3 March, 2017. Reading, UK: Academic Conferences and Publishing Limited, 90–95.

Cuningkin, V., Riley, E., & Rainey, L. (2021). Preventing Medjacking. *The American journal of nursing*, *121*(10), 46–50. https://doi.org/10.1097/01.NAJ.0000794252.99183.5e

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K. & Dudek, N., Mostaghimi, S., Colbert, E., & Murch, R. (2019). Ciberbiossegurança: uma nova perspectiva sobre a proteção do sistema alimentar e agrícola dos EUA. *Fronteiras em bioengenharia e biotecnologia*, *7*, 63. https://doi.org/10.3389/fbioe.2019.00063

Emergen Research (2020). Smart Farming Market by Farming Type (Livestock Monitoring, Precision Farming, Others), by Offerings (Software, Hardware, Others), and by Application (Livestock Monitoring Application, Precision Farming Application, Others), Forecasts to 2027. Available at: https://www.emergenresearch.com/industry-report/smart-farming-market

Geil A., Sagers G., Spaulding A. D., & Wolf J. R. (2018). Cyber Security on the Farm: an Assessment of Cyber Security Practices in the United States Agriculture Industry. *Int. Food Agribusiness Manage. Rev.* 21 (1030-2018-1811), 317–334. 10.22434/ifamr2017.0045

Gibson, D. G., Glass, J. I., Lartigue, C., Noskov, V. N., Chuang, R. Y., Algire, M. A., Benders, G. A., Montague, M. G., Ma, L., Moodie, M. M., Merryman, C., Vashee, S., Krishnakumar, R., Assad-Garcia, N., Andrews-Pfannkoch, C., Denisova, E. A., Young, L., Qi, Z. Q., Segall-Shapiro, T. H., Calvey, C. H. & Venter, J. C. (2010). Creation of a bacterial cell controlled by a chemically synthesized genome. *Science (New York, N.Y.)*, *329*(5987), 52–56. https://doi.org/10.1126/science.1190719

Helu, M., & Hedberg, T., Jr (2015). Enabling Smart Manufacturing Research and Development using a Product Lifecycle Test Bed. *Procedia manufacturing*, *1*, 86–97. https://doi.org/10.1016/j.promfg.2015.09.066

Jalali, M. S., Landman, A., & Gordon, W. J. (2021). Telemedicine, privacy, and information security in the age of COVID-19. *Journal of the American Medical Informatics Association: JAMIA*, *28*(3), 671–672. https://doi.org/10.1093/jamia/ocaa310

Khera, M. (2017). Think Like a Biohacker. *Journal of diabetes science and technology*, *11*(2), 207–212. https://doi.org/10.1177/1932296816677576

Kiss, A. A., Grievink, J. & Rito-Palomares, M. (2014). A systems engineering perspective on process integration in industrial biotechnology. *J. Chem. Tech. Biotech.* 90, 349–355. 10.1002/jctb.4584

Mazzeo, A & Santos, E J C. (2025a). Integrating Cybersecurity into Veterinary Medicine: Protecting Animal Health Data and Systems. *Research, Society and Development*, *14*(5), e7414547190. https://doi.org/10.33448/rsd-v14i5.47190

Mazzeo, A & Santos, E J C. (2025b). Integration of biomedical devices and the internet of bodies revolution. *Research, Society and Development*, *14*(5), e11814548921. https://doi.org/10.33448/rsd-v14i5.48921

McCulloch, W.S. & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics* 5, 115–133 (1943). https://doi.org/10.1007/BF02478259

Mendes, C. (2022). O que é uma revisão narrativa de literatura: exemplos e considerações da metodologia. https://www.youtube.com/watch?v=YlBWSVsxvRM

Morag, N. (2014). Cybercrime, Cyberespionage, and Cybersabotage: Understanding Emerging Threats. Colorado Technical University: College of Security Studies. *Available online at:* https://www.coloradotech.edu/media/default/CTU/documents/resources/cybercrime-white-paper.pdf *(accessed August 11, 2019).*

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy. *Frontiers in bioengineering and biotechnology*, *6*, 39. https://doi.org/10.3389/fbioe.2018.00039

Murch, R., & DiEuliis, D. (2019). Editorial: Mapping the Cyberbiosecurity Enterprise. *Frontiers in bioengineering and biotechnology*, *7*, 235. https://doi.org/10.3389/fbioe.2019.00235

Nayak, J., Meher, S. K., Souri, A., Naik, B., & Vimal, S. (2022). Extreme learning machine and bayesian optimization-driven intelligent framework for IoMT cyber-attack detection. *The Journal of supercomputing*, *78*(13), 14866–14891. https://doi.org/10.1007/s11227-022-04453-z

Nielsen, J., & Keasling, J. D. (2011). Synergies between synthetic biology and metabolic engineering. *Nature biotechnology*, *29*(8), 693–695. https://doi.org/10.1038/nbt.1937

Osborne, C. (2018). US Hospital Pays $55,000 to Biohackers After Ransomware Attack. ZDNet. *Available online at:* https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/ *(accessed August 11, 2019).*

Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: From Naive Trust to Risk Awareness. *Trends in biotechnology*, *36*(1), 4–7. https://doi.org/10.1016/j.tibtech.2017.10.012

Pereira, A. S. et al. (2018). Metodologia da pesquisa científica. [free ebook]. Santa Maria: Ed. UFSM.

Pinkham, D. W., Sala, I. M., Soisson, E. T., Wang, B., & Deeley, M. A. (2021). Are you ready for a cyberattack?. *Journal of applied clinical medical physics*, *22*(10), 4–7. https://doi.org/10.1002/acm2.13422

Purnick, P. E., & Weiss, R. (2009). The second wave of synthetic biology: from modules to systems. *Nature reviews. Molecular cell biology*, *10*(6), 410–422. https://doi.org/10.1038/nrm2698

Richardson, L. C., Lewis, S. M., & Burnette, R. N. (2019). Building Capacity for Cyberbiosecurity Training. *Frontiers in bioengineering and biotechnology*, *7*, 112. https://doi.org/10.3389/fbioe.2019.00112

Rollin, J. A., Tam, T. K. & Zhang, Y. H. P. (2013). New biotechnology paradigm: cell-free biosystems for biomanufacturing. Green Chem. 15, 1708–1719. 10.1039/c3gc40625c

Rother, E. T. (2007). Revisão sistemática x revisão narrativa. Acta paul. enferm. 20 (2). https://doi.org/10.1590/S0103-21002007000200001.

Shannon, C. E. (1950). A Chess-Playing Machine. *Scientific American*, *182*(2), 48–51. DOI:10.1007/978-1-4613-8716-9_6

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of business research, 104, 333-339.

Sousa, A. S.; Oliveira, G. S.; & Alves, L. H (2021). A pesquisa bibliográfica: princípios e fundamentos. Cadernos da Fucamp, 20(43). https://revistas.fucamp.edu.br/index.php/cadernos/article/view/2336

Sykuta, M. E. (2016). Big data in agriculture: property rights, privacy and competition in ag data services. *Internat. Food Agribusiness Manage. Rev. 19, 57–74.*

Toosi, A., Bottino, A., Saboury, B. & Rahmim, A. (2021) A brief history ofAI: how to prevent another winter (a critical review). PET Clin.https://doi.org/10.1016/j.cpet.2021.07.001

Van der Linden, D., Michalec, O. A. & Zamansky, A. (2020). Cybersecurity for Smart Farming: Socio-Cultural Context Matters. *IEEE Technol. Soc. Mag.* 39 (4), 28–35. 10.1109/mts.2020.3031844

Verseux, C. N., Paulino-Lima, I. G., Baqué, M., Billi, D. & Rothschild, L. J. (2016). Synthetic Biology for Space Exploration: Promises and Societal Implications. In: Hagen, K., Engelhard, M., Toepfer, G. (eds) Ambivalences of Creating Life. Ethics of Science and Technology Assessment, vol 45. Springer, Cham. https://doi.org/10.1007/978-3-319-21088-9_4

Wang, T., Tu, M., Lyu, H., Li, Y., Orfila, O., Zou, G., & Gruyer, D. (2022). Impact Evaluation of Cyberattacks on Connected and Automated Vehicles in Mixed Traffic Flow and Its Resilient and Robust Control Strategy. *Sensors (Basel, Switzerland)*, *23*(1), 74. https://doi.org/10.3390/s23010074

You, E., & Kozminski, K. G. (2015). Biosecurity in the age of Big Data: a conversation with the FBI. *Molecular biology of the cell*, *26*(22), 3894–3897. https://doi.org/10.1091/mbc.E14-01-0027

Zhong, R. Y., Xu, X., Klotz, E. & Newman, S. T. (2017). Intelligent manufacturing in the context of industry 4.0: A review. Engineering 3, 616–630. 10.1016/J.ENG.2017.05.015