REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

# SEGURANÇA CIBERNÉTICA INDUSTRIAL: EVOLUÇÃO E TENDÊNCIAS DAS AMEAÇAS VERSUS ESTRATÉGIAS DE PROTEÇÃO

## INDUSTRIAL CYBERSECURITY: EVOLUTION AND TRENDS OF THREATS VERSUS PROTECTION STRATEGIES

Engenharias • 29/09/2026

REGISTRO DOI: 10.70773/revistatopicos/790568368

Pericles Rezende Coelho[1]

**RESUMO**

Este artigo analisa a evolução das ameaças cibernéticas no contexto industrial e apresenta estratégias de proteção voltadas à preservação da continuidade operacional, da integridade dos dados e da segurança dos sistemas de controle industrial. A crescente adoção de tecnologias associadas à Indústria 4.0, como Internet Industrial das Coisas, computação em nuvem, inteligência artificial, automação e sistemas ciberfísicos, ampliou a integração entre os ambientes de tecnologia da informação e tecnologia operacional. Embora essa convergência tenha proporcionado ganhos de eficiência, produtividade e conectividade, também aumentou a superfície de ataque das organizações industriais. O estudo aborda ameaças como ransomware, phishing, malware sem arquivo, vulnerabilidades em softwares, ataques à cadeia de suprimentos e comprometimento de acessos remotos. Destacam-se, ainda, os impactos financeiros, operacionais, jurídicos e reputacionais provocados por incidentes de segurança, conforme demonstrado nos casos da Parker-Hannifin Corporation e da MKS Instruments. Como medidas de proteção, são discutidas a segmentação de redes, o monitoramento contínuo, a autenticação multifator, a realização de backups, a capacitação dos colaboradores, a gestão de riscos e a criação de planos de resposta a incidentes. Por fim, o artigo ressalta a importância da adoção de normas específicas, como a IEC 62443 e o NIST SP 800-82, bem como do uso responsável da inteligência artificial, para fortalecer a resiliência cibernética das organizações industriais.

**Palavras-chave:** Cibersegurança industrial; Indústria 4.0; Ransomware; Sistemas de controle industrial.

**ABSTRACT**

This article analyzes the evolution of cyber threats in the industrial

context and presents protection strategies aimed at preserving operational continuity, data integrity, and the security of industrial control systems. The growing adoption of Industry 4.0 technologies —such as the Industrial Internet of Things, cloud computing, artificial intelligence, automation, and cyber-physical systems—has expanded the integration between information technology and operational technology environments. While this convergence has yielded gains in efficiency, productivity, and connectivity, it has also increased the attack surface for industrial organizations. The study addresses threats such as ransomware, phishing, fileless malware, software vulnerabilities, supply chain attacks, and remote access compromise. It also highlights the financial, operational, legal, and reputational impacts caused by security incidents, as demonstrated by the cases of Parker-Hannifin Corporation and MKS Instruments. Protection measures discussed include network segmentation, continuous monitoring, multi-factor authentication, backups, employee training, risk management, and the creation of incident response plans. Finally, the article emphasizes the importance of adopting specific standards—such as IEC 62443 and NIST SP 800-82 —as well as the responsible use of artificial intelligence, to strengthen the cyber resilience of industrial organizations.
**Keywords:** Industrial cybersecurity; Industry 4.0; Ransomware; Industrial control systems.

## 1. INTRODUÇÃO

Com o desenvolvimento tecnológicos de suas oprações, as organizações industriais têm enfrentado novas ameaças cibernéticas que ipactam na convergência de seus sistemas de TI e ICS, na utiização da Internet das Coisas Industrial (IIoT) em seus

procesos fabris e, principalmente, em suas cadeias de suprimentos. (Merízio, 2023).

Em uma sociedade digital como a nossa nos dias de hoje, nenhum tipo de empreendimento está totalmente livre dos ataques efetuados por *hackers*. É importante destacar que mesmo o cenário atual apresente muitos desafios em relação às questões de defesa de seus projetos, o processo de investigação em termos ataques cibernéticos é funcamental o conhecimento amplo sobre cada tipo de ameaça (Outmarketing).

O surgimento da *internet* representou o ponto de partida para o atual nível de compartilhamento de informações. Esse marco histórico deu origem a uma dimensão intangível e abstrata que transformou o mundo onde foram criadas novas oportunidades para o desenvolvimento social, político e econômico, bem como novos desafios relacionados à privacidade, segurança e à divisão digital. Nesta dimensão, é crucial compreender a dinâmica do ciberespaço e desenvolver políticas e estratégias eficazes para aproveitar seu potencial e mitigar seus riscos (DA SILVA & NOGUEIRA, 2019).

## 2. METODOLOGIA

Este estudo caracteriza-se como uma pesquisa bibliográfica, de abordagem qualitativa, com objetivos exploratórios e descritivos. A pesquisa bibliográfica foi escolhida por possibilitar a análise de conhecimentos já publicados sobre segurança cibernética industrial, sistemas de controle industrial, tecnologia operacional, Internet Industrial das Coisas, ransomware, ameaças digitais e estratégias de proteção.

Para a elaboração do trabalho, foram utilizadas fontes secundárias, tais como artigos científicos, livros, relatórios técnicos, documentos institucionais, normas de segurança, publicações especializadas e conteúdos produzidos por organizações relacionadas à área de cibersegurança. Foram considerados materiais que abordam a evolução dos ataques cibernéticos, os impactos da integração entre ambientes de TI e OT, os riscos associados à digitalização industrial e as práticas recomendadas para prevenção, detecção, resposta e recuperação de incidentes.

A pesquisa apresenta abordagem qualitativa porque busca compreender, interpretar e discutir informações presentes nas fontes consultadas, sem a realização de coleta de dados primários, questionários, entrevistas ou aplicação de métodos estatísticos. A análise concentrou-se nas características das principais ameaças enfrentadas pelas organizações industriais, como ransomware, phishing, malware sem arquivo, exploração de vulnerabilidades, ataques à cadeia de suprimentos e comprometimento de sistemas conectados.

Quanto aos objetivos, o estudo possui caráter exploratório, pois busca ampliar a compreensão sobre os riscos decorrentes da transformação digital e da convergência entre os ambientes de tecnologia da informação e tecnologia operacional. Também apresenta caráter descritivo, uma vez que descreve as principais ameaças cibernéticas, seus impactos sobre as organizações e as estratégias de proteção utilizadas para reduzir vulnerabilidades e fortalecer a resiliência operacional.

Além da revisão bibliográfica, foram utilizados estudos de caso relacionados às empresas Parker-Hannifin Corporation e MKS

Instruments. A análise desses casos permite demonstrar, de forma prática, como ataques cibernéticos podem causar interrupções na produção, perdas financeiras, exposição de dados pessoais, consequências jurídicas e danos à reputação corporativa. Assim, o estudo relaciona os conhecimentos teóricos apresentados na literatura aos impactos observados em organizações industriais.

## 3. REVISÃO DE LITERATURA

O estudo da segurança cibernética industrial tem avançado significativamente desde os primeiros registros de ataques a sistemas de supervisão, controle e aquisição de dados, conhecidos como sistemas SCADA. Com o aumento da conectividade e da digitalização das operações, os ataques deixaram de ser incidentes isolados e passaram a ocorrer de forma mais planejada, direcionada e sofisticada.

A literatura sobre o tema demonstra que a integração de dispositivos IIoT, sistemas ciberfísicos, soluções de computação em nuvem e equipamentos automatizados ampliou a quantidade de ativos conectados em ambientes industriais. Essa expansão favorece a coleta e o processamento de dados em tempo real, mas também cria novos pontos de vulnerabilidade. Equipamentos antigos, sistemas operacionais desatualizados, senhas fracas, conexões remotas mal configuradas e ausência de segmentação de redes são exemplos de fatores que podem facilitar a atuação de invasores.

Diversos estudos também destacam a importância da normatização para estruturar programas de segurança voltados ao setor industrial. Normas como a IEC 62443 e documentos como o NIST SP 800-82 oferecem orientações para a proteção de sistemas de controle

industrial, auxiliando as organizações na gestão de riscos, na definição de políticas de segurança, no controle de acessos e na proteção dos ativos críticos. Essas referências são importantes porque os ambientes industriais apresentam características próprias, como a necessidade de disponibilidade contínua, a presença de equipamentos legados e os riscos relacionados à segurança física das operações.

Dessa forma, a segurança cibernética industrial exige uma abordagem que considere não apenas a proteção de informações corporativas, mas também a integridade dos processos produtivos, a segurança dos trabalhadores, a disponibilidade de equipamentos e a continuidade das atividades da organização.

## 4. EVOLUÇÃO DAS AMEAÇAS CIBERNÉTICAS

As ameaças de ataques cibernéticos estão em constante evolução, tornando a sua detecção cada vez mais desafiadora. À medida que os sistmea segurança se sofisticam, os ataques também se tornam mais avançados. Já foi uma época em que os malwares benignos eram criados apenas para exibir mensagens *pop-up*. A motivação dos *hackers* era inicialmente impulsionada pela curiosidade em compreender o funcionamento das coisas. Hoje, os responsáveis por esses ataques são motivados principalmente por ganhos financeiros. Essa mudança de interesse tem transformado o cenário de segurança cibernética, exigindo constantes inovações e esforços para proteger sistemas e dados valiosos (Wright, 2023).

Com o desenvolvimento da Indústria 4.0 novas tecnologias disruptivas como Internet das Coisas (IoT), Big data, impressão 3D, inteligência artificial e novos sistemas ciber-físicos (CPS)

necessitaram de um gerenciamento de comunicações autônomas que permitissem arquiteturas de comunicação distribuída, em vez de depender apenas de arquiteturas centralizadas como a nuvem. A integração desses equipamentos heterogêneos no ambiente cibernético industrial obrigou as empresas a investir em cibersegurança na estratégia de *design* industrial para criar um ambiente de produção mais inteligente e seguro. No entanto, apesar das melhorias na eficiência de fabricação trazidas pela Indústria 4.0, falhas de segurança cibernética têm gerado impactos críticos nos modelos de negócios e na competitividade. (Mullet et al).

Do ponto de vista histórico, podemos considerar que o primeiro vírus da história foi lançado em 1980 por Elk Cloner como uma brincadeira direcionada aos usuários do computador Apple II. Sendo o conceito de antivírus surgido em 1983, quando Fred Cohen desenvolveu a primeira versão experimental e cunhou o termo "vírus". Essa aplicação tinha a habilidade de excluir malwares imediatamente, substituindo assim o trabalho de uma equipe de TI. O projeto se transformou em sua tese de doutorado, na qual ele investigou as formas de infecção e as técnicas para prevenir ataques de vírus e malwares (Merizio, 2023).

Em termos de evolução, podemos destacar que na década de 1990, com a expansão da internet, novas formas de ataques surgiram como *phishing* e ataques de negação de serviço (DoS) (Mansfield-Devine, 2020). Nos anos 2000, os atacantes se profissionalizaram com grupos que se organizaram criando *malwares* mais elaborados para obtenção de ganho financeiro (Singer & Friedman, 2014). Com a *ransomware,* a partir de 2020, aconteceu a proliferação de ataques em dispositivos em IoT (Greenberg, 2019).

Conforme uma pesquisa realizada em 2023 pela empresa Trend Micro, embora o número total de ataques de *ransomware* possa estar diminuindo, a gravidade e a precisão dos ataques estão aumentando com foco em alvos mais significativos e com métodos mais avançados. A referida pesquisa indica que os cibercriminosos estão adotando técnicas mais elaboradas, abandonando os tradicionais *e-mails* de *spam* em massa em favor de ataques altamente personalizados que visam indivíduos ou empresas específicas (ABES, 2024).

De acordo com Wright (2023), estas são algumas das ameaças e riscos de segurança mais comuns que as organizações enfrentam atualmente, conforme o quadro abaixo.

| Ameaça/Risco | Descrição Resumida |
|---|---|
| Cibercrime como Serviço (CaaS) | Gangues alugam malware e serviços (MaaS, RaaS, PhaaS) para criminosos menos habilidosos. |
| Malware Sem Arquivo (LOTL/Fileless) | Uso de ferramentas do sistema e *malware* na memória volátil para evitar detecção por antivírus. |
| Exploits de RPC | Abuso de MSRPC para escalada de privilégios e movimento lateral. |
| Phishing | Técnica de engenharia social para roubar credenciais ou induzir ações indesejadas |
| Comprometimento da Cadeia de Suprimentos | Ataques que comprometem *software* ou *hardware* de fornecedores, afetando muitos usuários. |
| Ransomware | *Malware* que criptografa dados e exige resgate, incluindo extorsão dupla e tripla. |

| | |
|---|---|
| Vulnerabilidades | Falhas no código exploradas para acesso inicial ou *ransomware*. |

Em seu relatório realizado em 2023, a empresa de consuloria PWC destaca que a indústria de manufatura tem enfrentado um número crescente de ataques cibernéticos, principalmente por ataques efetuados através do *ransomware*. Os ataques ocorrem principalmente devido a integração de ambientes de tecnologia operacional (OT) com sistemas conectados, aumentando a superfície de ataque, e com isso impactando substancialmente as cadeias de fornecimento da empresa, além da interrupção em outros departamentos (PwC, 2024).

É importante destacar que segundo o Relatório de Investigações de Violação de Dados da Verizon, o *ransomware* representou 15,5% dos incidentes de cibercrime em 2023. E na indústria manufatureira, foi responsável por 24% dos ataques bem-sucedidos. Esse fato, se deu principalmente pela fragilidade das cadeias de suprimento, e sistemas e tecnologias de IoT legados (Scimeca, 2023).

A recuperação de sistemas após um ataque cibernético pode ser cara e demorada. No entanto, não somente se deve a ataques de *ransomware* que as empresas enfrentam em termos de *malwares*, mas também, à infiltração em sistemas operacionais que resultam em roubo de dados financeiros e reputacionais (Gavejian et al, 2023).

## 5. ESTRATÉGIAS DE PROTEÇÃO

A convergência tecnológica nos sistemas de automação industrial que integra tecnologias como sensores, atuadores, redes de comunicação e sistemas de controle, aumentou a eficiência operacional, mas também criou vulnerabilidades que podem ser

exploradas por cibercriminosos. As principais falhas envolvem a Interconexão Excessiva, *Software* Desatualizado, Falta de Conscientização e Ameaças Internas (Teltex Tecnologia, 2023). é importante destacar a crescente dependência de tecnologias avançadas, como automação, inteligência artificial e *blockchain*, que torna os impactos de ataques cibernéticos na manufatura ainda mais severos (Gavejian et al, 2023).

É importante destacar que a convergência tecnológica nos sistemas de automação industrial que integra tecnologias como sensores, atuadores, redes de comunicação e sistemas de controle, aumentou a eficiência operacional, ao mesmo tempo, que houve um aumento exponencial das vulnerabilidades nos sistemas computacionas das empresas. As principais falhas envolvem a Interconexão Excessiva, *Software* Desatualizado, Falta de Conscientização e Ameaças Internas (Teltex Tecnologia, 2023). Incluindo a crescente dependência de tecnologias avançadas como a automação, inteligência artificial e *blockchain*, (Gavejian et al, 2023).

A proteção em segurança cibernética Industrial, exige inovação, valor agregado e competitividade no ecossistema de negócios. A conquista da confiança, a promoção da resiliência, a simplificação da segurança e seu gerenciamento torna-se obrigatório quanto ao preparo para crises, a proteção de ativos essenciais e ao aumento da competitividade nos negócios (Cordeiro, 2023). Uma estratégia eficaz de segurança cibernética deve ser adaptada às necessidades específicas da organização. Isso envolve a identificação das ameaças mais prováveis e o desenvolvimento de medidas preventivas adequadas (Teletex, 2023). A criação de um plano que inclua diretrizes, políticas e procedimentos é fundamental para garantir a

integridade, confidencialidade e disponibilidade dos sistemas de informação da empresa (Check Point, 2023).

Os funcionários desempenham um papel crítico na segurança cibernética. Programas de treinamento regulares sobre práticas recomendadas de segurança, como identificação de e-mails suspeitos e proteção de informações sensíveis, são essenciais para reduzir o risco de ataques bem-sucedidos (AWS, 2023). A conscientização pode ajudar a prevenir incidentes causados por erro humano, que é uma das principais causas de violações de segurança (Gatefy, 2023).

A adoção de tecnologias avançadas é vital para proteger a infraestrutura da organização. Isso inclui o uso de firewalls, software antivírus, sistemas de detecção de intrusão e soluções baseadas em inteligência artificial para monitorar atividades suspeitas (AWS, 2023) . Essas ferramentas ajudam a identificar e neutralizar ameaças antes que possam causar danos significativos (Teletex, 2023).

A criação de um plano de gestão de riscos é crucial para identificar, avaliar e mitigar os riscos cibernéticos específicos enfrentados pela organização (Teletex, 2023). Isso envolve a classificação dos riscos com base em sua probabilidade e impacto, permitindo que a empresa desenvolva estratégias eficazes para enfrentá-los (Check Point, 2023).

Estabelecer políticas robustas para backup e recuperação de dados é fundamental para garantir que a organização possa se recuperar rapidamente após um ataque cibernético. Testes regulares dos processos de backup ajudam a assegurar que os dados possam ser

restaurados sem perda significativa (ALTI Tecnologia, 2023; Check Point, 2023).

A implementação de um sistema eficaz para monitoramento contínuo permite à organização detectar atividades anômalas em tempo real (ALTI Tecnologia, 2023). Além disso, deve haver um plano claro para resposta a incidentes que detalhe as etapas a serem seguidas em caso de violação da segurança (AWS, 2023).

## 6. ESTUDOS DE CASO

### 6.1. Parker-Hannifin Corporation

Em fevereiro de 2022 ocorreu um ataque cibernético à Parker-Hannifin Corporation, uma empresa global de tecnologia de controle e movimento, na qual causou sérios impactos à empresa. O incidente foi causado por um grupo de *hackers* conhecidos como *Conti*, que conseguiu acessar os sistemas da empresa sem permissão por alguns dias em março. Onde foram vazadas informações sensíveis relacionadas à identificação pessoal dos funcionários atuais e antigos da empresa juntamente com dados dos seus dependentes. Os dados continham nomes completos de pessoas juntamente com números de identidade social, seus endereços residenciais, entre outras informações (CisoAdvisor, 2022).

Os impactos do ataque foram significativos. A Parker-Hannifin enfrentou uma interrupção significativa em suas operações, o que afetou sua capacidade de processar pedidos e manter a produção. Essa paralisação não apenas resultou em perdas financeiras diretas, mas também comprometeu a confiança dos clientes e parceiros comerciais na empresa. Estima-se que o custo total do ataque tenha

superado US$200 milhões, considerando as perdas operacionais e os gastos com remediação (Pwc, 2024).

Além das consequências financeiras e operacionais, a exposição de dados sensíveis levantou preocupações legais para a Parker-Hannifin. Na qual a empresa teve que lidar com as implicações da violação de dados e as possíveis ações judiciais decorrentes da exposição das informações pessoais dos funcionários. Para mitigar os danos causados pelo ataque, a Parker-Hannifin iniciou protocolos de resposta a incidentes imediatamente após descobrir a violação. Isso incluiu o desligamento de sistemas afetados e a colaboração com especialistas em segurança cibernética para investigar o incidente (Ciso Advisor, 2022).

A empresa também implementou medidas corretivas, como o envio de notificações aos indivíduos cujas informações foram comprometidas e ofereceu monitoramento gratuito por dois anos através do Experian's IdentityWorks para ajudar a proteger os afetados contra possíveis fraudes (Ciso Advisor, 2022). Essas ações refletem um esforço para restaurar a confiança e reforçar a segurança cibernética da organização diante das ameaças em evolução no ambiente digital (PwC, 2024).

### 6.2. MKS Instruments

Em fevereiro de 2023, a MKS Instruments, uma empresa americana especializada em equipamentos para a indústria de semicondutores, foi vítima de um ataque de ransomware que teve impactos significativos em suas operações e finanças. O ataque ocorreu no dia 3 de fevereiro de 2023 e afetou os sistemas de produção da empresa,

levando à suspensão temporária das operações em algumas instalações (CSO Online, 2023; MKS Instruments, 2023).

O ataque foi identificado como um evento de ransomware, onde os hackers conseguiram criptografar os sistemas de negócios e fabricação da MKS Instruments, tornando-os indisponíveis. Além disso, houve indícios de que dados pessoais dos funcionários também teriam sido exfiltrados durante o incidente. A empresa imediatamente ativou seus protocolos de resposta a incidentes e notificou as autoridades legais sobre o ocorrido (BankInfoSecurity, 2023; Cybersecurity Dive, 2023).

Os efeitos financeiros do ataque foram substanciais. A MKS Instruments estimou uma perda de receita de aproximadamente **US$200 milhões** no primeiro trimestre de 2023 devido à interrupção das operações e à incapacidade de processar pedidos e enviar produtos. Antes do ataque, a empresa esperava reportar cerca de **US$1 bilhão** em receita para o trimestre (Optics.org, 2023; Cybersecurity Dive, 2023). O CEO da empresa, John Lee, afirmou que o incidente teve um impacto material nas operações das divisões de soluções ópticas e soluções a vácuo da MKS (CSO Online, 2023).

Após o ataque, a MKS Instruments começou a restaurar seus sistemas assim que foi considerado seguro fazê-lo. A empresa também contratou especialistas em resposta a incidentes para ajudar na investigação do ataque e na recuperação dos sistemas afetados (BankInfoSecurity, 2023). Além disso, a MKS enviou notificações aos indivíduos cujos dados pessoais poderiam ter sido comprometidos, embora não houvesse confirmação definitiva sobre a exfiltração desses dados (My Injury Attorney, 2023).

A situação também resultou em repercussões legais para a MKS Instruments. Em março de 2023, um ex-funcionário processou a empresa por supostas falhas na proteção das informações pessoais e médicas dos empregados. A ação alegava que a MKS não implementou controles adequados para evitar acessos não autorizados aos seus sistemas financeiros (BankInfoSecurity, 2023).

O ataque cibernético à MKS Instruments exemplifica os desafios crescentes que as empresas enfrentam em relação à segurança cibernética. Com o aumento das ameaças de ransomware na indústria, é crucial que as organizações adotem medidas proativas para proteger suas operações e dados sensíveis. A MKS está atualmente focada na recuperação e na implementação de melhorias em suas práticas de segurança cibernética para prevenir futuros incidentes.

## 7. TENDÊNCIAS FUTURAS E RECOMENDAÇÕES

A segurança cibernética industrial tende a assumir um papel cada vez mais estratégico diante da expansão da Indústria 4.0, da Internet Industrial das Coisas (IIoT), da computação em nuvem, da automação e da integração crescente entre os ambientes de tecnologia da informação (TI) e tecnologia operacional (OT). Os sistemas de OT envolvem dispositivos e tecnologias programáveis que interagem diretamente com processos físicos, incluindo sistemas de controle industrial, equipamentos de automação, sensores, atuadores e sistemas de monitoramento. Por essa razão, sua proteção exige atenção não apenas à confidencialidade dos dados, mas também à disponibilidade, à confiabilidade e à segurança das operações produtivas (NIST, 2023).

Uma das principais tendências é a utilização de inteligência artificial e aprendizado de máquina para auxiliar na identificação de ameaças, na análise de comportamentos anômalos e no monitoramento contínuo de redes industriais. A aplicação dessas tecnologias pode ampliar a capacidade das organizações de analisar grandes quantidades de dados provenientes de equipamentos conectados, registros de eventos e comunicações entre sistemas. No entanto, mecanismos de inteligência artificial também podem ser vulneráveis a manipulações e ataques adversariais, o que demonstra a necessidade de validação, monitoramento e supervisão humana durante sua utilização em ambientes críticos (NIST, 2025).

O modelo de confiança zero, denominado *Zero Trust*, constitui outra tendência relevante para a proteção de infraestruturas industriais. Esse modelo pressupõe que usuários, dispositivos, redes, aplicações e dados devem ser verificados continuamente, sem que a posição interna na rede seja suficiente para garantir confiança. A adoção de controles de identidade, autenticação multifator, visibilidade de ativos, monitoramento de dispositivos, gestão de redes e governança de dados contribui para reduzir os riscos de acessos indevidos e movimentação lateral de invasores (CISA, 2023).

A segmentação e o isolamento de redes permanecem medidas indispensáveis para a proteção de ambientes industriais. A separação entre redes corporativas, sistemas administrativos, redes de produção, dispositivos de controle e equipamentos críticos reduz a possibilidade de propagação de códigos maliciosos e limita o alcance de um incidente. O NIST ressalta que a segurança de sistemas de OT deve considerar ameaças, vulnerabilidades e contramedidas adequadas às particularidades de desempenho, confiabilidade e segurança existentes nesses ambientes (NIST, 2023).

A adoção da série de normas IEC 62443 representa uma tendência importante para a organização da segurança em sistemas de automação e controle industrial. Essa série propõe, entre outros princípios, a divisão da infraestrutura em zonas e conduítes, permitindo agrupar ativos com requisitos semelhantes de segurança e controlar as comunicações entre diferentes partes da rede. Dessa forma, a organização pode estabelecer controles específicos, reduzir conexões desnecessárias e limitar a propagação de ameaças entre sistemas corporativos e operacionais (CISCO, 2024).

A proteção da cadeia de suprimentos também tende a receber maior atenção das organizações industriais. A dependência de fornecedores de softwares, fabricantes de equipamentos, empresas de manutenção, plataformas em nuvem e prestadores de acesso remoto amplia os riscos relacionados a terceiros. A gestão da cadeia de suprimentos deve incluir o acompanhamento de ativos físicos e virtuais, a definição de políticas de segurança, o estabelecimento de controles mínimos e a avaliação contínua dos riscos associados à aquisição de dispositivos e serviços (CISA, 2023).

Outro aspecto essencial é o aperfeiçoamento de planos de resposta a incidentes e recuperação de desastres. A preparação para incidentes deve contemplar ações de detecção, análise, contenção, erradicação, recuperação e avaliação posterior ao ataque. No ambiente industrial, essas ações precisam ser adaptadas para preservar a continuidade da produção, a segurança dos trabalhadores, a disponibilidade dos sistemas de controle e a integridade dos equipamentos críticos (NIST, 2023).

Diante dessas tendências, recomenda-se que as organizações industriais realizem inventários completos e atualizados de ativos de TI e OT. Esse levantamento deve abranger sistemas de controle, servidores, controladores lógicos programáveis, estações de engenharia, dispositivos IIoT, equipamentos legados, softwares, conexões remotas e acessos concedidos a fornecedores. A identificação dos ativos permite compreender a superfície de ataque da organização e estabelecer prioridades para a aplicação de controles de segurança (CISA, 2023; NIST, 2023).

Também se recomenda classificar os ativos de acordo com sua criticidade para a produção, a segurança das pessoas, a proteção ambiental, a qualidade dos produtos e a continuidade do negócio. Essa classificação contribui para que os investimentos e controles de segurança sejam direcionados inicialmente aos sistemas cujo comprometimento possa gerar maiores impactos operacionais, financeiros ou físicos. A gestão de riscos voltada aos ambientes de OT deve considerar as particularidades e os efeitos de falhas sobre processos físicos e operacionais (NIST, 2023).

As empresas devem implementar segmentação de rede, criando zonas de segurança e estabelecendo canais de comunicação controlados entre ambientes corporativos e operacionais. Essa medida deve ser acompanhada pelo uso de firewalls industriais, regras restritivas de comunicação, registros de eventos, monitoramento contínuo e mecanismos de isolamento. A utilização de zonas e conduítes permite organizar os ativos conforme suas necessidades de segurança e controlar a circulação de dados entre diferentes setores da infraestrutura (CISCO, 2024; NIST, 2023).

Recomenda-se ainda a adoção de autenticação multifator, políticas de senhas seguras e o princípio do menor privilégio. Os acessos administrativos, remotos e de fornecedores devem ser concedidos apenas quando necessários, monitorados e revisados periodicamente. Tais medidas estão alinhadas aos pilares de identidade, dispositivos, redes, aplicações e dados previstos no modelo de maturidade de confiança zero, que propõe a evolução gradual dos controles de segurança nas organizações (CISA, 2023).

A atualização de sistemas, softwares e dispositivos deve ocorrer de forma planejada e controlada. Em ambientes industriais, atualizações precisam ser avaliadas antes da implantação, pois alterações inadequadas podem provocar incompatibilidades ou indisponibilidade de sistemas essenciais à produção. Assim, a gestão de vulnerabilidades deve conciliar a redução dos riscos cibernéticos com os requisitos de desempenho, disponibilidade, confiabilidade e segurança física dos ambientes de OT (NIST, 2023).

A manutenção de backups atualizados, protegidos e submetidos a testes de restauração é igualmente fundamental. A capacidade de recuperar dados, configurações e sistemas após um incidente pode reduzir o tempo de paralisação e os prejuízos gerados por ataques como ransomware. Os procedimentos de backup e recuperação devem estar integrados ao plano de resposta a incidentes, contemplando etapas de contenção, restauração e análise posterior ao evento (NIST, 2023). Por fim, recomenda-se a realização de treinamentos contínuos para funcionários, operadores, gestores e prestadores de serviço. A capacitação deve abordar o reconhecimento de mensagens suspeitas, a proteção de credenciais, o uso seguro de dispositivos, a identificação de comportamentos anômalos e a comunicação imediata de possíveis

incidentes. A combinação entre pessoas capacitadas, processos de segurança bem definidos e controles tecnológicos compatíveis com a realidade industrial é indispensável para fortalecer a resiliência cibernética das organizações (NIST, 2023; CISA, 2023).

## 8. CONCLUSÃO

A segurança cibernética industrial tornou-se um elemento essencial para a continuidade, a confiabilidade e a competitividade das organizações. A evolução da Indústria 4.0, marcada pela integração entre sistemas de tecnologia da informação, sistemas de controle industrial, dispositivos IIoT, computação em nuvem e tecnologias de automação, ampliou significativamente a eficiência dos processos produtivos. Contudo, essa integração também aumentou a superfície de ataque e criou novas possibilidades de exploração por parte de criminosos cibernéticos.

A análise apresentada demonstrou que as ameaças deixaram de ser ataques simples e isolados para assumir formas mais sofisticadas, direcionadas e financeiramente motivadas. Ransomware, phishing, malware sem arquivo, exploração de vulnerabilidades, comprometimento da cadeia de suprimentos e ataques realizados como serviço estão entre os principais riscos enfrentados pelo setor industrial. Os casos da Parker-Hannifin Corporation e da MKS Instruments evidenciam que um incidente cibernético pode provocar paralisações operacionais, perdas financeiras expressivas, exposição de dados pessoais, consequências jurídicas e danos à reputação empresarial.

Diante desse cenário, a proteção da infraestrutura industrial não deve depender de uma única ferramenta ou ação isolada. É

necessário adotar uma abordagem integrada, baseada na identificação e avaliação de riscos, na segmentação das redes, na atualização dos sistemas, no controle de acessos, no monitoramento contínuo e no uso de sistemas de detecção e resposta a incidentes. Da mesma forma, a realização de backups testados, a elaboração de planos de continuidade e recuperação e a capacitação constante dos funcionários são medidas indispensáveis para reduzir a probabilidade e o impacto dos ataques.

Também se destaca a importância da adoção de normas e boas práticas específicas para ambientes industriais, como a IEC 62443 e o NIST SP 800-82. Essas referências contribuem para estruturar políticas de segurança, orientar a gestão de riscos e estabelecer responsabilidades entre fabricantes, fornecedores e operadores. No futuro, recursos baseados em inteligência artificial poderão ampliar a capacidade de identificar comportamentos anômalos e responder rapidamente às ameaças, embora sua utilização também exija controles, validação humana e avaliação permanente dos riscos.

Portanto, a segurança cibernética industrial deve ser compreendida como um processo contínuo, estratégico e compartilhado por toda a organização. Mais do que reagir aos incidentes depois que eles ocorrem, as empresas precisam desenvolver uma cultura de prevenção, resiliência e melhoria constante. Somente por meio da combinação entre tecnologia, normas, capacitação profissional, governança e preparação para crises será possível proteger os sistemas de controle industrial e garantir a continuidade segura das operações em um ambiente tecnológico em permanente transformação.

**REFERÊNCIAS BIBLIOGRÁFICAS**

ABES. **2023 fecha com 161 bilhões de ataques cibernéticos em mais um recorde, segundo relatório da Trend Micro.** 2024. Disponível em: https://abes.com.br/2023-fecha-com-161-bilhoes-de-ataques-ciberneticos-em-mais-um-recorde-segundo-relatorio-da-trend-micro/. Acesso em: 10 set. 2026.

AMAZON WEB SERVICES. **Cybersecurity: práticas recomendadas para proteção de dados e sistemas.** 2023.

BANKINFOSECURITY. **MKS Instruments ransomware attack results in $200M sales hit.** 2023. Disponível em: https://www.bankinfosecurity.com/mks-instruments-ransomware-attack-results-in-200m-sales-hit-a-21442. Acesso em: 10 set. 2026.

CANONGIA, Claudia; MANDARINO JUNIOR, Raphael. **Segurança cibernética: o desafio da nova sociedade da informação.** [S. l.: s. n.], [s. d.]. Disponível em: https://cdi.mecon.gob.ar/bases/doc/parceriasest/29.pdf. Acesso em: 10 set. 2026.

CHECK POINT. **Estratégias de segurança cibernética para organizações.** 2023.

CHEMINOD, Marco; et al. **Cybersecurity in industrial control systems.** 2020.

CISCO. **ISA/IEC 62443-3-3: what is it and how to comply?** Cisco, 16 ago. 2024. Disponível em: https://www.cisco.com/c/en/us/products/collateral/security/isaiec-62443-3-3-wp.html. Acesso em: 10 set. 2026.

CISO ADVISOR. **Parker-Hannifin data breach and Conti ransomware incident.** 2022.

CORDEIRO, A. **Megatendências mundiais 2040: contribuição para um debate de longo prazo para o Brasil.** Capítulo 12. [S. l.]: Escola Superior de Guerra, 2023. Disponível em: https://repositorio.esg.br/bitstream/123456789/1665/1/Megatendencias__Mundiais_2040.pdf. Acesso em: 10 set. 2026.

CSO ONLINE. **MKS Instruments cyberattack disrupts manufacturing operations.** 2023.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. **Zero Trust Maturity Model: version 2.0.** Washington, DC: CISA, abr. 2023. Disponível em: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf. Acesso em: 10 set. 2026.

CYBERSECURITY DIVE. **MKS Instruments says February ransomware attack will clip revenue by $200 million.** 2 mar. 2023. Disponível em: https://www.cybersecuritydive.com/news/mks-ransomware-200-million-revenue/644000/. Acesso em: 10 set. 2026.

DA SILVA, Washington Rodrigues; NOGUEIRA, Jorge Madeira. Ataques cibernéticos e medidas governamentais para combatê-los. **O Comunicante,** v. 9, n. 1, p. 42-57, 2019.

EMNIFY. **Segurança IoT.** [S. l., s. d.]. Disponível em: https://www.emnify.com/pt-br/glossario-iot/seguranca-iot. Acesso em: 10 set. 2026.

FERNANDES, et al. **Cibersegurança industrial e desafios da Internet Industrial das Coisas.** 2023.

GATEFY. **Conscientização em segurança cibernética e prevenção de incidentes.** 2023.

GAVEJIAN, K.; KINGHORN, C.; MCGRATH, T. **Dealing with the growing threat of cyberattacks in the manufacturing sector: what employers need to know.** [S. l.]: Jackson Lewis, 2023. Disponível em: https://www.jacksonlewis.com/insights/dealing-growing-threat-cyberattacks-manufacturing-sector-what-employers-need-kn. Acesso em: 10 set. 2026.

GREENBERG, Andy. **Sandworm: a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers.** New York: Doubleday, 2019.

INTERNATIONAL ELECTROTECHNICAL COMMISSION. **IEC 62443: industrial communication networks – network and system security.** Geneva: IEC, [s. d.].

KASPERSKY. **What is IoT?** [S. l., s. d.]. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-iot. Acesso em: 10 set. 2026.

KUSHNER, David. The real story of Stuxnet. **IEEE Spectrum,** 26 fev. 2013. Disponível em: https://spectrum.ieee.org/the-real-story-of-stuxnet. Acesso em: 10 set. 2026.

MANSFIELD-DEVINE, Steve. The evolution of cyber threats. **Computer Fraud & Security,** [S. l.], 2020.

MKS INSTRUMENTS. **Annual report 2023.** Andover, MA: MKS Instruments, 2024. Disponível em: https://investor.mks.com/static-

files/74b247f8-c558-41c5-a521-873dbb761666. Acesso em: 10 set. 2026.

MKS INSTRUMENTS. **MKS Instruments reports fourth quarter and full-year 2022 results.** Andover, MA, 27 fev. 2023. Disponível em: https://investor.mks.com/node/21546/pdf. Acesso em: 10 set. 2026.

MULLET, Victor; et al. **Cybersecurity challenges in Industry 4.0 and industrial cyber-physical systems.** [S. l.: s. n.], [s. d.].

NATIONAL CYBER SECURITY CENTRE. **Common cyber-attacks: reducing the impact.** Cyber Attacks White Paper, jan. 2016. Disponível em: https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact. Acesso em: 10 set. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Adversarial Machine Learning: a taxonomy and terminology of attacks and mitigations.** NIST AI 100-2e2025. Gaithersburg, MD: National Institute of Standards and Technology, 2025. Disponível em: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2025.pdf. Acesso em: 10 set. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Guide to Operational Technology (OT) Security.** NIST Special Publication 800-82, Revision 3. Gaithersburg, MD: National Institute of Standards and Technology, 2023. Disponível em: https://csrc.nist.gov/pubs/sp/800/82/r3/final. Acesso em: 10 set. 2026.

OUTMARKETING, Annielly. **Tipos de ataques cibernéticos.** 2023. Disponível em: https://www.interop.com.br/tipos-de-ataques-ciberneticos/. Acesso em: 10 set. 2026.

PRODUZA. **IoT na manufatura: aplicações e impactos na indústria.** [S. l., s. d.]. Disponível em: https://produza.ind.br/tecnologia/iot-na-manufatura/. Acesso em: 10 set. 2026.

PwC. **Cybersecurity risks and ransomware threats in the manufacturing sector.** 2024.

SAP. **What is cybersecurity?** [S. l., s. d.]. Disponível em: https://www.sap.com/brazil/products/financial-management/what-is-cybersecurity.html. Acesso em: 10 set. 2026.

SINGER, P. W.; FRIEDMAN, Allan. **Cybersecurity and cyberwar: what everyone needs to know.** New York: Oxford University Press, 2014.

TELTEX TECNOLOGIA. **Os desafios da cibersegurança em sistemas de automação industrial.** 2023. Disponível em: https://teltex.com.br/os-desafios-da-ciberseguranca-em-sistemas-de-automacao-industrial/. Acesso em: 10 set. 2026.

THRIVEDX. **The evolution of cyber threats.** [S. l., s. d.]. Disponível em: https://thrivedx.com/resources/article/top-cybersecurity-challenges-for-cisos-in-2024. Acesso em: 10 set. 2026.

TREND MICRO. **2023 fecha com 161 bilhões de ataques cibernéticos em mais um recorde, segundo relatório da Trend Micro.** 2024. Disponível em: https://abes.com.br/2023-fecha-com-161-bilhoes-de-ataques-ciberneticos-em-mais-um-recorde-segundo-relatorio-da-trend-micro/. Acesso em: 10 set. 2026.

VERIZON. **2024 Data Breach Investigations Report: manufacturing snapshot.** 2024. Disponível em:

https://www.verizon.com/business/resources/Tb04/infographics/2024-dbir-manufacturing-snapshot.pdf. Acesso em: 10 set. 2026.

WRIGHT, Dean. **The evolution of cyber threats.** ThriveDX, 2023.

---

[1] Mestre em Engenharia Industrial pela Universidade do Minho, Portugal. ORCID https://orcid.org/0009-0009-8392-7939.